Understanding Information Security
Strategy in Organisations

Craig A. Horne

BSc, La Trobe University, 1992
MBA, La Trobe University, 2002
ORCID ID: 0000-0001-7395-4348

Submitted in total fulfilment of the requirements of the
degree of Doctor of Philosophy

December 2018

Department of Computing and Information Systems
The University of Melbourne
Abstract

The research topic under investigation in this thesis is information security strategy in organisations and I propose a substantive theory for understanding this phenomenon under varying environmental and internal conditions. My original contribution to knowledge includes a definition for information security strategy, criteria for organisational environment and information assessment, a conceptual model of information security strategy, a substantive theory on information security strategy, and a descriptive set of benefits that can be adopted after strategy selection and approval.

Organisations are progressively undertaking digital transformation of their products and services to reduce costs, improve customer relationships, and consolidate operations. Information is the “lifeblood” of any organisation and is increasingly being used to support this digital transformation across the entire organisation. Yet, the boundaries of information, its value, and importance in supporting organisational goals are frequently overlooked, creating security exposures and vulnerabilities. One reason for this is a lack of attention paid to cataloguing and controlling valuable information being used as a business resource. Others are that usage of emerging disruptive technology such as cloud-based applications can create porous network borders, that security controls used to protect information can be expensive and complex, and that organisational leaders may resist the implementation of security controls due to a perception that they impede productivity. This then leads to increased risk to information, affecting organisational leaders in the governing body, who currently have no consistent guidance available to help them in selecting a strategy or setting a strategic direction for information security.

To address this problem, I examine a range of concepts when adopting an approach to securing information, by interviewing security leaders in larger organisations. In a qualitative study, I interviewed twenty-five participants and took a phenomenological
approach to understanding their lived experiences with developing and using an information security strategy. I used grounded theory methodology and techniques to analyse the interview transcripts and their organisation’s information security strategy documents when permitted, to understand significant information security concepts and their relationships in an organisational context. The results show that organisational leaders choose from four main strategies when making decisions to secure their organisation’s information, which are Fortification, Devaluation, Outsourcing and Minimisation. Their selection depends on consideration of organisational factors including constraints on outsourcing decisions and the value of information held within the organisation. This facilitated the development of a conceptual model of information security strategy and a substantive theory on information security strategy. The implications of this are that organisations can continue business operations towards the achievement of strategic goals using information as a resource, and that the selection of an information security strategy can lead to a more complete understanding of the comprehensive strategic plans required to implement operational security controls throughout an organisation, making them more applicable and cost effective.
Declaration

This is to certify that:

i. the thesis comprises only my original work towards the PhD except where indicated in the Preface,

ii. due acknowledgement has been made in the text to all other material used,

iii. the thesis is fewer than 100 000 words in length, exclusive of tables, maps, bibliographies and appendices.

Signature:

Name: Craig A. Horne

Date: 14 December 2018
Preface

Statements from the student researcher on the preparation of this thesis:

• Some passages in this thesis have been quoted verbatim from published papers where I was the primary author, with permission from the co-authors and publishers. It is noted at the beginning of the relevant chapters where this has occurred.

• Although the supervisors have contributed minor editing and proof-reading suggestions for this thesis and associated conference and journal articles, the work output is entirely an original effort from the student researcher.

• There has been no work submitted for other qualifications or work carried out prior to PhD candidature enrolment.

• There has been no third-party editorial assistance, either paid or voluntary.

• The services of a freelance transcriber were used to convert some audio recordings of interviews into ‘raw’ written transcription documents. These raw transcriptions were then converted into ‘clean’ transcriptions by the student researcher, who personally checked every word. The transition from raw to clean transcription involved listening to the audio again and removing umms and ahhs, replacing unintelligible sections with the correct words, removing profane words, and removing accidental self-disclosures. Only clean written transcriptions were then analysed as part of the Findings chapter.

• This research received funding support from an Australian Government Research Training Program Scholarship.
Preface – Publications

The following is a list of academic journal articles, poster sessions, workshops, outlets and conferences that publishes research and findings from this thesis. Elements of these articles are included in this thesis. The publication of articles is also highlighted at the beginning of relevant chapters in this thesis.

Peer-reviewed journal articles:

Peer-reviewed conference proceedings:

Doctoral colloquiums at educational institution:

Popular media outlets:
Preface – Acknowledgements

I would like to thank and acknowledge the efforts of my supervisor Dr. Sean Maynard who was a practical source of truth in a complex assortment of literature. He patiently waded into the deep end with me, taking the time to explore and comprehend subtle nuances in key areas. I was especially grateful for his open-door policy and motivational support. Thanks also to my supervisor Dr. Atif Ahmad, who readily engaged with me at an intellectual level to robustly discuss concepts, possessed the self-control to extend patience when I needed it and provided considered guidance on the overall research direction.

I am grateful for mentorship along the way from senior scholars who have given their time so generously. Many thanks to Leon Stirling, Rod Dilnutt, Richard Baskerville, Justin Zobel, Graeme Shanks, Deborah Bunker, Axel Korthaus, John Lamp, Ella Hafermalz, Henry Linger, and Julie Fisher for their guidance. Dr. Steve Versteeg deserves credit as without him, I would not have commenced doctoral research in the first place. Dr. Jeb Webb, Dr. Piya Shedden and Dr. Jay Jeong were always available for coffee to discuss any aspect of my thesis.

I would like to thank my parents Donald and Patricia for raising me to believe in lifelong learning and always encouraging me to be the best I can. My sisters Nicole and Sharon deserve credit for their excitement on this seemingly endless journey whenever I gave them an update. Most importantly, my beautiful wife Dr. Michelle Horne and sons Daniel and Edmund who have provided boundless love and support throughout the many years it took to complete this research program. I thank them for this opportunity to indulge my intellectual curiosity and hope they find as much enjoyment in lifelong learning as I have.
# Table of Contents

Abstract................................................................................................................................................... iii

Declaration................................................................................................................................................ vi

Preface....................................................................................................................................................... vii

Preface – Publications............................................................................................................................... viii

Preface – Acknowledgements .................................................................................................................. ix

Glossary....................................................................................................................................................... xi

List of Tables............................................................................................................................................... xiv

List of Figures............................................................................................................................................. xv

Chapter 1: Introduction ............................................................................................................................. 16

1.1 Context of the Study............................................................................................................................ 16

1.2 Statement of the Problem.................................................................................................................... 24

1.3 Aim and Scope..................................................................................................................................... 29

1.4 Significance.......................................................................................................................................... 30

1.5 Contributions to Knowledge ............................................................................................................. 31

1.6 Overview............................................................................................................................................ 33

Chapter 2: Research Background .......................................................................................................... 36

2.1 Chapter Aim......................................................................................................................................... 36

2.2 Defining Information Security Strategy............................................................................................ 38

2.3 Information Security Strategy in Information Systems .................................................................... 41

2.4 Theoretical Background..................................................................................................................... 69

2.5 Proposed Definition of Information Security Strategy....................................................................... 72

2.6 Chapter Summary............................................................................................................................... 72

Chapter 3: Research Approach ................................................................................................................. 73
Appendix E:  Example Transcript from an Interview................................. 326
Appendix F:  Descriptions of Concepts and Relationships.......................... 340
Appendix G:  Data Structure .................................................................... 346
## Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>APRA</td>
<td>Australian Prudential Regulation Authority</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced persistent threats</td>
</tr>
<tr>
<td>ASD</td>
<td>Australian Signals Directorate</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring your own device</td>
</tr>
<tr>
<td>CapEx</td>
<td>Capital expenditure</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud access security broker</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, integrity, availability</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CPS</td>
<td>Cross-industry prudential standard</td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>GTM</td>
<td>Grounded theory methodology</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communications technology</td>
</tr>
<tr>
<td>InfoSec</td>
<td>Information security</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual property</td>
</tr>
<tr>
<td>IS</td>
<td>Information systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>OpEx</td>
<td>Operational expenditure</td>
</tr>
<tr>
<td>OrgISS</td>
<td>Organisational information security strategy</td>
</tr>
<tr>
<td>SETA</td>
<td>Security education, training and awareness</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
</tbody>
</table>
List of Tables

Table 2.1. Information Security Strategy Conceptualisations and Role in Information Systems Research ................................................................. 45
Table 2.2. Information Security Strategy Conceptualisations and Levels of Analysis 46
Table 2.3. Thematic Map of Results from Literature Review of OrgISS .................. 68
Table 2.4. Information Systems Theories and Information Security Strategy .......... 71
Table 4.1. Data Collection Phase Sample – Organisation Demographics .......... 120
Table 7.1. Open (Level 1) Codes Mapped to Category (Level 2) Codes ............... 261
Table 7.2. Common Constraining Antecedents for Outsourcing ....................... 274
Table B.1. Information Systems Theories and Information Security Strategy ....... 310
Table F.1. Descriptions of Concepts ................................................................. 340
Table F.2. Descriptions of Concept Relationships ........................................... 343
List of Figures

Figure 2.1: Thematic Map of Information Security Strategy in Organisations in IS Research............................................................................................................................................. 49
Figure 3.1. Overall Research Process Flow Chart................................................................................................................. 75
Figure 3.2. Sociological Paradigms (Burrell and Morgan 1979) ................................................................. 85
Figure 4.1. Summary of Common Platforms Used for Storing Information............. 150
Figure 5.1. Conceptual Model of Core Organisational Concepts .................. 219
Figure 7.1. Generic Information Security Strategies ................................................................. 260
Figure 7.2. Conceptual Model of Organisational Information Security Strategy ..... 266
Chapter 1: Introduction

Organisational information security strategy (OrgISS) is an area within the information systems (IS) discipline that examines the security of information at an organisational level for strategic purposes. This introductory chapter opens by expanding on key terms used throughout the thesis, giving some context to the topic in order to categorise established lines of inquiry, identifying the problem with efforts made in the area to date, establishing a singular aim of this research effort and the scope of the study based on the limited resources available, explaining the significance of the study in both theoretical and practical terms, and finally offering a descriptive overview of the thesis structure.

1.1 Context of the Study

There is an increasing global trend towards the digitisation of organisational products and services in order to lower expenses, increase performance, increase dynamism in a fluctuating market, expand the target market to include a global focus, and increase delivery speed (Bharadwaj, El Sawy, Pavlou, & Venkatraman, 2013a). This digitisation depends on an increased use of information that resides on, and is therefore exposed to, a greater interconnection of networks and systems (Bharadwaj et al., 2013a). This exponential increase in the number of networks and systems that information is stored and transmitted on comes with an associated risk to that

---

1 Elements of this chapter are published in the following peer-reviewed articles:


information, especially given many supporting networks terminate or route overseas, beyond the control of the information owner. Often, the value and importance of information are frequently overlooked, creating security exposures.

Against the backdrop of an increasing need for information, there has been a concurrent global increase in the complexity and prevalence of security threats to information (ACS, 2016; Ahmad, Webb, Desouza, & Boorman, 2019; Gupta & Sharman, 2012). Information security threats for organisations are predicted to rise annually in number and scale (ACS, 2016). Once a threat eventuates into a security incident, organisational leaders often face hefty clean-up costs to restore their organisation’s digital systems’ operations or information integrity. Of concern to organisations, global clean-up costs from information security attacks on organisations are currently estimated to total as much as $500 billion per annum (ACS, 2016). Given the significance of these impacts, governments around the world are increasingly looking to pass legislation and impose significant penalties on people and organisations to hold them accountable for securing their organisation’s information. These factors mean that organisations should set an information security strategy to guide their security efforts (Wu & Guo, 2016).

In this study, the unit of analysis is the entity known as an organisational information security strategy. The units of observation are (1) an individual research participant, (2) organisations that engage in information security at the strategic level, and (3) a document that purports to contain an information security strategy. Together, the unit of analysis and the unit of observation form the population of the research enterprise.

1.1.1 Understanding Key Terms

The following is a description of some key terms that together are used throughout this thesis. The focus in this thesis is on information security strategy, so each of
these words are individually described in turn, as they are later combined for the keyword search during the literature review in the next chapter.

1.1.1.1 Information

Information has been characterised as amorphous and intangible, which may be stored on various platforms such as paper, computer databases and even cognitive media (people’s minds) (Ahmad, Ruighaver, & Teo, 2005; VonSolms & Van Niekerk, 2013). Organisations protect their information because it is used broadly for daily operations and, depending on its sensitivity and utility, may even form the basis for competitive advantage (Ahmad, Maynard, & Park, 2014b; Park, Ruighaver, Maynard, & Ahmad, 2011; Porter & Millar, 1985). Information may have varying levels of value, from very little to high, and should be classified accordingly. Classifications may then be used as the basis for assigning access rights to employees (Ahmad, Bosua, & Scheepers, 2014a). Classification labels then direct the type of security controls that are assigned to protect the information, which includes technical controls which are technology-based, formal controls such as defined rules and procedures, and informal controls such security education, training and awareness programs and the ensuing security culture that is developed as a result (Backhouse & Dhillon, 1996; Beebe & Rao, 2010).

Information is not data, as data are considered to be raw facts and numbers. For example, the binary number ‘00110101’ is data whereas information is considered to be data that has been processed to become meaningful, for example the map latitude and longitude for a city (McKinney Jr & Yoos, 2010). For the purposes of this thesis however, the word data is often used interchangeably with the word information, because the research participants who provided the research data use the words interchangeably. Information has a lifecycle, in that it is created, stored, used, and eventually deleted (Tallon & Scannell, 2007). The lifecycle of information is
not enough however to explain decisions made to secure it, as it lacks the strategic perspective.

Information can have different sensitivities and therefore classifications, yet be difficult to control which can lead to information leakage of highly classified information (Ahmad et al., 2005). Where the information is stored, for example internally on privately owned IT infrastructure or externally on public cloud-based storage, changes the benefits and the risks from specific threats (Loh & Venkatraman, 1995). Information is also distinct from knowledge, as knowledge is considered to be an inherently human trait; an amalgamation of information existing in the conscious brain (Dulipovici & Baskerville, 2007). Research subjects sometimes used the word knowledge interchangeably with information, so for the purposes of this thesis, where the term knowledge is used, the word information should be inferred. Knowledge or information then affects organisational structure, which can include the type and location of IT infrastructure used to store it (Teece, 2000). This relationship where information drives decision-making about the selection of IT assets is foundational and the primary perspective taken throughout this entire thesis.

1.1.1.2 Security

Security threats originate from a variety of areas, including business organisations and military departments, government and law enforcement agencies, even diminished privacy and freedoms from online engagement (Schneier, 2003). Information security has been defined as “preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved” (ISO/IEC, 2018, pp. 4). Historically most organisations have adopted a preventative approach to information security, achieving a perceived secure state using risk management for a
planned implementation of technological controls (Da Veiga & Eloff, 2007; Webb, Ahmad, Maynard, & Shanks, 2014, 2016). Taking a management practice perspective, information security has then advanced through a period that favoured integrating information security into the organisational hierarchy, followed by an era that incorporated information security into employee duties to inculcate an effective security culture, and then an age that advocated governance to counter fraud and social engineering attacks (Da Veiga & Eloff, 2007). These advancements resulted in a greater focus on strategic-level protection of information but have not directly tackled the problem of where to begin a coordinated focus on the security of information.

1.1.1.3 Strategy

Strategy is a concept that has been developed over centuries in the military and business disciplines (Grattan, 2002). The word strategy originally came from the Greek ‘strategos’, meaning military general. Military strategy is a set of ideas implemented by military organisations to pursue desired strategic goals. Military strategy deals with the planning and conduct of campaigns, and the movement and disposition of national forces. Strategy is the art of distributing and applying military means, such as armed forces and supplies, to fulfil the ends of policy. In military literature, strategy is the highest level of planning, with the next level lower down termed operational, and tactical level below that (Bowdish, 2013). The tactics, techniques and procedures at the lowest level support the achievement of operations, which then support a nation’s strategic goals at the highest level. At the strategic level, nations guide the facilitation and achievement of national goals and objectives, using critical infrastructure and other national resources to achieve them (Bowdish, 2013).
From the business literature, views on strategy abound (Drucker, 1958; Mintzberg, 1987; Quinn, Mintzberg, & James, 1988), however in one of the most highly-cited strategic management books of the last century, three generic competitive strategies were identified: 1. differentiation, 2. overall cost leadership and 3. focus (Porter, 1980). These generic competitive strategies form the basis of competitive advantage using resources to drive profitability (widely defined as total revenue less total expenses) (Barney, 2000; Grant, 1991; Porter, 1980). These strategies are used within the business domain by organisations selecting one and then using it to guide decision-making when implementing it operationally. These descriptions collectively reveal strategy to be an organisational-wide construct, affecting the direction and activities of the board and all staff in response to the competitive environment, in pursuit of a goal (commonly profit).

Information plays a critical role in sustaining business success by driving innovation and opportunities for the development of strategic competitive advantage (Gupta, Tan, Ee, & Phang, 2018). Preservation of the confidentiality, integrity and availability (CIA) of this information is therefore imperative for organisations, so a range of options must be examined. There are a range of actions available to an organisation to secure information, including the areas of security strategy, security policy, security education training and awareness (SETA), security culture, technological control tools, and risk management (Ahmad et al., 2014a). Coordination of these areas begins at a high level with the implementation of an appropriate information security strategy which is then used to organise the other security mechanisms across the organisation via a comprehensive framework (Ahmad et al., 2014b). When considering its business strategy, as well as internal factors, organisations must also consider external environmental factors such as competition, suppliers and regulators (Mithas, Tafti, & Mitchell, 2013).
CHAPTER 1: INTRODUCTION

1.1.1.4 Information security

Information security has been defined as “a well-informed sense of assurance that information risks and controls are in balance” (Anderson, 2003, pp. 310). Information security is native to the information systems discipline, originating wholly from information-related concepts and the systems it is hosted by (Moody, Iacob, & Amrit, 2010). It is applicable at different levels, including individual, group, organisational and also shared information at the inter-organisational level. Degradation of key information over time diminishes resource utility and could potentially prompt the attrition of organisational sustainability.

Information security evolved to include non-technical aspects and has been defined as the protection of information and the systems that it resides on (Whitman & Mattord, 2011). The goal of information security seeks preservation of the confidentiality, integrity, availability, non-repudiation of business information (McCumber, 1991; Posthumus & Von Solms, 2004; Siponen & Oinas-Kukkonen, 2007). Adding identification and authentication to this list of properties extends the definition of information security to become one of information assurance (Ezingeard, McFadzean, & Birchall, 2005). Other benefits that organisations can enjoy from successful information security include greater shareholder value, new business opportunities and improved governance (Partida & Ezingeard, 2007).

A lot of research on information security to date has been at tactical level of a technical nature however information security can no longer be treated as technical only (Antoniou, 2018; Bowdish, 2013; Dhillon & Backhouse, 2000). Computer security, at times referred to as information and communication technology (ICT) security, is the security of networks, computers, and other physical IT infrastructure (VonSolms & Van Niekerk, 2013). Computer security goals are the confidentiality,
integrity, availability, authenticity, non-repudiation, reliability, and accountability of information (VonSolms & Van Niekerk, 2013; Whitman & Mattord, 2011).

Cyber security is a term that is used increasingly more commonly in recent times however the focus of this thesis is on information security, so an explanation of cyber security is included here to assist in providing a delineation of topics. Cyber security is more extensive than information security and expands beyond it to consist of not only the defence of information but also non-informational assets (Dutta & McCrohan, 2002; VonSolms & Van Niekerk, 2013). Cyberspace has been defined as “a time-dependent set of interconnected information systems and the human users that interact with these systems” (Ottis & Lorents, 2010, pp. 268). Cyber-security was then further defined as not only the protection of cyberspace but non-informational assets as well (Van Schaik et al., 2017). The cyber security goals and general security objectives are the confidentiality, integrity, and availability of an organisation’s IT resources including infrastructure, personnel, networks, and information (VonSolms & Van Niekerk, 2013).

There has also been a considerable amount of research conducted into operational areas related to information security, with a focus on improving human aspects with management control, planning and communication (Arhin & Wiredu, 2018; Backhouse & Dhillon, 1996; Dhillon, Torkzadeh, & Chang, 2018). This approach highlights the view that organisational information not only resides on ICT infrastructure but in human’s minds as well as on paper.

The board of directors in a business organisation (or comparable minister in a government organisation) is ultimately accountable however for information security and eventual organisational success or otherwise (VonSolms, 2001). More research is required at strategic level because “unfortunately, there has been very little research undertaken on information security from the perspective of the board of
CHAPTER 1: INTRODUCTION

“directors” (McFadzean, Ezingeard, & Birchall, 2006, pp. 4). More recently, there is still a paucity of current research on boards and their governance to reduce security breaches (Higgs, Pinsker, Smith, & Young, 2016). Extant research on strategy for information security is fragmented and sparse, as detailed more fully in Chapter 2 Research Background.

1.2 Statement of the Problem

There are a number of ways that security breaches are perpetrated, including internal attacks from trusted employees, external attacks from anonymous adversaries, and physical attacks on the medium that stores the information (McFadzean, Ezingeard, & Birchall, 2007). The effects of external threats can be demonstrated by Sony Corporation, which was famously hacked in 2011. The PlayStation Network outage was the result of an external intrusion on Sony’s PlayStation Network (Dhillon, 2018). The attack occurred in April 2011 and forced Sony to completely turn off the PlayStation Network, attacking the availability of their information. On May 4 Sony confirmed that personally identifiable information from each of the 77 million accounts appeared to have been stolen. The outage lasted 24 days and on May 23, 2011 Sony stated that the outage costs were $171 million (Dhillon, 2018; Garrie & Mann, 2014).

A famous example of a physical attack on information was the incident involving the Bank of New York Mellon (BNY Mellon) in 2008. In February 2008, BNY Mellon sent ten unencrypted backup tapes to an external storage facility on a truck. When the storage firm’s truck arrived at the facility, however, only nine tapes were still on board. The missing tape contained social security numbers and bank account information on 4.5 million customers. Coincidentally, the bank retrenched 1,800 staff and received $3 billion in emergency relief funding from US Treasury later that year (Gupta & Sharman, 2012).
To illustrate an insider attack, a famous example was when Edward Snowden once revealed over a million classified documents in 2013 to various news agencies, which he had copied whilst working as a contractor for the US Central Intelligence Agency, contractor at the National Security Agency, and as a counterintelligence trainer at the US Defense Intelligence Agency. Snowden's release of classified material about global mass surveillance was called the most significant leak in US history (VonSolms & Van Heerden, 2015) and as of 2015, international loss of trust in the US has damaged trade by as much as $180 billion.

The impacts from these three examples - substantial unanticipated remediation expenses, reputational damage with financial repercussions, and trust issues resulting in economic damage - serve to highlight the scale and scope of the problem. The risks from these increasingly complex threats require the setting of a novel information security strategy to counteract them (Maynard, Onibere, & Ahmad, 2018; Onibere, Ahmad, & Maynard, 2017). Effects from a security breach on information can impact at individual, group, organisational, inter-organisational or even country level.

What makes organisational efforts to secure information more problematic is when access restrictions to information become unknown or porous. For example, in accordance with a bring-your-own-device policy, corporate emails may be downloaded to personal mobile devices, or information-based files may be stored on personal Dropbox accounts not corporate accounts, or business discussions may take place on social media such as LinkedIn. This can then lead to problems with information availability, such as when a cloud storage vendor becomes bankrupt and the organisation experiences difficulties with retrieval of their information (Catteddu, 2010). The boundaries of modern storage platforms are obfuscated and porous, yet their access is increasingly cheap and easy.
Following a recent trend in openness, large organisations have begun to publicly disclose their significant information security breaches, the magnitude of which are often surprising given the volume and sophistication of security controls at the disposal of large organisations to prevent and respond to security incidents (Garrie & Mann, 2014; Pilgrim, 2017). Often the identification and value of information are frequently overlooked, creating security exposures that are significant enough to warrant the attention of organisational leaders. One reason for this is a lack of attention often paid to cataloguing and controlling key sources of information. Other reasons are that usage of emerging disruptive technology can create porous network borders, that security controls to protect information can be expensive and complex, and that organisational leaders may resist the implementation of security controls due to a perception that they impede productivity.

Although management and employees can take a very practical approach, it is unclear what steps organisational leaders can take to reduce liability and impact in anticipation of an information security breach. To be clear about who’s at fault in the event of a breach, an information security attack is the fault of the attacker. However, constructing inadequate organisational defences against preventable known threats might be seen as the fault of security specialists and leaders within an organisation. The international standard for the governance of information security states that organisational leaders who form the governing body are accountable for overseeing efforts made towards establishing, approving and using an information security strategy within an organisation (ISO/IEC, 2013). They can share responsibility for this with executives and managers but ultimately, they are accountable for setting strategy, properly funding information security efforts as well as ensuring that all the necessary initiatives have been conducted to prepare the organisation for a possible information security attack. Organisational leaders are obliged to monitor financial risk, liquidity risk, operational risk, and informational risk might be simply another
operational risk to be addressed and mitigated. To date however, there is a lack of available options and direction to leaders to direct whether an organisation should enlist the services of an outsource partner to assist with the storage and handling of information, for example a public cloud vendor, or a contractor.

To describe the process, information security governance standards stipulate that an organisation’s executive management should begin by developing an OrgISS, for the governing body to approve, and then subsequent implementation (ISO/IEC, 2013). This relationship where executives assist the governing body in their decision-making around the setting of information security strategy, rather than decisions being made at an operational security manager level, is key and is the primary perspective taken throughout this entire thesis.

Further, organisations should then track their progress towards the achievement of an information security strategy. However there appears to be no commonly accepted guidance on how organisational leaders can choose an appropriate strategy for the security of their organisational information, given their unique circumstances, or what the contents of a strategy might be. There are no clear guidelines to opening a new office in another country and safeguarding against espionage, overfunding or underfunding information security efforts within an organisation accurately, or allowing information to pass securely between stakeholders to an organisation, e.g. suppliers, customers, regulators, staff and directors. Compounding this lack of direction, only 50 percent of company directors even claim to be cyber literate and the number drops to just 15 percent for co-directors (ACS, 2016). Although these conditions collectively amount to a large problem, researchers have been encouraged to investigate problems that are substantive (Weber, 2003).
1.2.1 Research Question

Research questions are constructed based on the problem and gaps that exist in knowledge to date (Sandberg & Alvesson, 2011). Therefore, the initial research question used to guide this research and the examination of extant information security literature in the next chapter is:

RQ: How can organisational leaders select an information security strategy that best benefits the organisation?

This question necessitates an understanding of information security strategy, which is reviewed and defined during the academic literature examination. The aggregated understanding of the conceptual nature of the topic is then used to guide an extensive search of the literature. To answer this research question, several sub-questions must be answered first:

I. What is an information security strategy?

The research first seeks to understand what an information security strategy is, in terms of its definition, conceptualisation, levels of analysis, measurement and relevant supporting theory. As well as its constituent properties, I also examine what environmental conditions motivate the use of one and what value and benefits can be enjoyed post-adoption.

II. How is an information security strategy selected by organisational leaders?

Organisational leaders must take a lot into consideration when determining the most appropriate selection. For example, they must consider the purpose and objects of the organisation, stakeholders such as regulators and shareholders, and internal capabilities. The answers to the first sub-question on the nature of information security strategy will dictate how it is selected, which will then dictate any other supporting activities.
III. How can an information security strategy best benefit an organisation?

The selection of an information security strategy might have implications for organisational leaders, or management and staff who are required to make operational and tactical decisions as part of their job. This research investigates on balance what usage best benefits the organisation, considering its purpose and stakeholders.

This research will improve understanding of what an information security strategy is, how it is selected, and how it is used. In Chapter 8: Conclusion, this research question is revisited again with a view to answering it based on the findings from the discussion.

1.3 Aim and Scope

The aim of this research is to increase understanding of information security strategy in organisations. This requires an investigation of its conceptualisation to identify strategic approaches that organisations take when securing information. The difference between strategic and operational is a subtle distinction but an important one. This investigation intends to uncover the factors and considerations that lead to the selection of one information security strategy over another, as well as the benefits that organisations can obtain post-adoption.

The scope of this study includes analysing information security strategy as defined in the information systems literature and experienced within Australian-headquartered organisations. I gain an understanding of the phenomena under investigation from individuals who are accountable or responsible for securing information within their respective organisations, and who have personal experience with information security at the strategic level. The research subjects included both private and public organisations, from medium to very large in size, in order to analyse differences and similarities between them all. This study does not include empirical testing of the
CHAPTER 1: INTRODUCTION

resultant theory’s concepts or relationships because “the generation of a theory is a legitimate outcome of the study” (Creswell, 1998, pp. 58). Theory building studies can usefully contribute to knowledge by producing an explanation and prediction theory, which can be tested as a separate exercise (Gregor, 2006).

Although small organisations make up the vast majority of organisations operating in Australia in terms of sheer numbers, they were not included in the scope of this study due to a lack of available employees who were solely dedicated to the security function, or who dealt with information security as a significant component of their work, and could potentially participate as research subjects. Other restrictions on scope include the absence of investigation into the topic at operational level, or the tactical level below that, to remain focussed on strategy and the interaction between the highest governing body of an organisation and the executive layer, who then oversee management and employees. The scope of the study is understanding strategy, not a strategic plan or framework of operational initiatives. Given that the nature of the topic is security, questioning was restricted to broad strategic questions to maintain confidentiality by preventing any disclosure of specific architecture or technological controls that an organisation deploys to secure information (Kotulic & Clark, 2004). This research examines information but did not examine data due to the widely-held belief that people’s brain are platforms that host (i.e. remember) information and knowledge not data (see Glossary for terms). It also did not examine knowledge, instead focussing on information which resides on platforms such as paper, databases, and computer servers (VonSolms & Van Niekerk, 2013).

1.4 Significance

The significance of this study is established via five outcomes (Evans, Gruba, & Zobel, 2011). First, this qualitative study advances theoretical knowledge in the information security strategy field beginning with the finding of a set of antecedent
motivations and considerations that prompt the setting of an information security strategy. These environmental stimuli may affect an organisation at various levels such as inter-organisational, organisational and group levels, which will impact stakeholder groups and their relationships. A second outcome is developing an understanding of the key concepts and relationships in information security strategy and a third outcome is to identify the range of benefits that organisations can obtain following strategy adoption, regardless of whether the organisation is public or privately held. This conceptual understanding of information security strategy is intended to be generalisable across other contexts, but further research is required to investigate this, and this type of generalisation is not included within this thesis.

Fourth, a practical outcome of this research program is to provide guidance for practitioners in evaluating strategic options for information security strategy. I focus on identifying a discrete set of alternative choices that members of a governing body within an organisation, such as a board of directors or a ministerial office, can select from based on their unique challenges. Finally, a fifth outcome is a set of sequenced steps in the assessment of an organisation's environment and information, to select and approve a strategy. Approval of a strategy is intended to subsequently guide the implementation of a framework of customised information security initiatives that together form a strategic plan, tailored for individual differences in organisation size and ownership, although development of this type of strategic plan is not included within the scope of this thesis.

1.5 Contributions to Knowledge

This thesis makes several contributions towards the body of knowledge on why organisations should adopt an information security strategy and how organisational leaders should take steps to evaluate and select a strategy in practice. Specifically, the contributions to theory are:
1.5.1 **Contribution 1: A Definition of Information Security Strategy in Organisations**

Based on the literature review, I construct a definition proposing the meaning of information security strategy:

"Information security strategy guides the achievement of organisational goals and objectives using IT infrastructure and information resources to achieve them, is motivated by antecedent conditions that balance internal information needs and external environmental factors to yield information security benefits to the organisation, and is selected from a small set of generic strategies to guide decision-making when implementing operationally."

1.5.2 **Contribution 2: A Conceptual Framework of Core Concepts Relating to Information Security Strategy**

The literature review from this research involved thematic analysis which identified a set of core concepts organised by level and relationship. The levels included individual, group, organisation and inter-organisation. The relationships included antecedents, constituents, and yields. The examination of extant literature in information systems identified several concepts and these were expanded quite significantly after data collection and analysis.

1.5.3 **Contribution 3: A Conceptual Model of Information Security Strategy**

The conceptual model of information security strategy depicts all abstract concepts and their relationships, generalised from the data. The relationships are proposed ones only without explanations. This model was then used as a representation of reality from which to base the development of a theory on information security strategy.
CHAPTER 1: INTRODUCTION

1.5.4 Contribution 4: A Theory on Information Security Strategy

The theory on information security strategy states that there are four generic strategies that guide the security of information within organisations. The depiction shows how core categories, their relationships, including properties of information, along with organisational and environmental conditions, affect selection of the most appropriate approach to securing information, which in turn offers a wide array of strategic-level organisational benefits.

1.5.5 Contribution 5: A Set of Practical Steps to Select an Information Security Strategy

This research provides guidance for practitioners in identifying all structured and unstructured information owned by the organisation, evaluating environmental challenges with securing that information, and selecting a strategy to secure it. The governing body then sets the most appropriate strategy, which can then be used to guide executives and management when making operational decisions to secure information.

1.6 Overview

This section adumbrates the thesis structure, which has been kept simple. This thesis comprises six main chapters, with this introductory chapter being the first. To recap, chapter one introduced the topic, gave some context to situate the information security strategy topic within the broader field of information systems, defined the problem which gave some clarity about the motivation for the study, outlined a singular aim of the study and the scope given the limited resources available, explained the significance of advancing knowledge about OrgISS, and offered a high-level overview of the following thesis structure.
Chapter two continues by reviewing the extant literature related to OrgISS, describing the key concepts and grappling with their conceptualisation. One of the contributions from this research is to build on this conceptualisation and form a definition of information security strategy in organisations. The conceptualisation and definition are then used to search the information systems literature by surveying the OrgISS topic, grouping key authors and their lines of argument, and identifying gaps in knowledge. The knowledge gap-spotting confirms the neglected areas within the OrgISS literature which include an agreed understanding of the nature of OrgISS, therefore making it a suitable point to commence this research program. A concise version of chapter two has been published in Australasian Conference of Information Systems conference proceedings and a more developed version was then published in Australasian Journal of Information Systems journal, details of which are listed in the Preface of this thesis.

Chapter three articulates the research design and methodology, starting with the ontology which is nominalist. The epistemological position follows, which is constructivist. The research approach is interpretivist and the methodology chosen to examine industry practitioners and understand OrgISS is phenomenological grounded theory, which was initially exploratory in nature to allow for uncovering new ideas about OrgISS. The data collection methods chosen were interviews, observations and document analysis, which allowed for triangulation across multiple sources to achieve a consistent view.

Chapters four to six summarise the findings of the collection of primary data, to provide supporting material from which to direct the subsequent discussion and conclusion chapters. The primary data consisted of interview transcripts, observations, and OrgISS documents, when they existed and were permitted to be shared. The qualitative data sets are organised thematically after analysis and the resulting information is described in relation to the aim of the study, noting any gaps
or incompleteness. These analyses are then interpreted to create new knowledge which is presented as logically and completely as possible.

Chapter seven contains the main discussion, building on the findings drawn in the previous chapters and the literature review. It combines a detailed understanding of the current information systems literature on information security strategy with the findings from the data collection, elevating the discussion to a theoretical level. The subsequent discussion details a model for OrgISS, which emerges from core concepts identified in the data analyses.

Chapter eight lists the conclusions drawn from the discussion, key findings, and makes my contributions to knowledge explicit, including a definition of information security strategy and a theoretical model of it. The thesis is then closed with limitations and future research suggestions. References and appendices follow, which include a list of the core papers analysed in the literature review, a list of relevant theories from extant related work, the ethics approval statement from the institutional ethics board, the interview protocol with questions used during data collection, an example full interview transcription, descriptions of concepts and relationships from the findings in chapters four to six, and a data structure that summarises the coding process.
Chapter 2: Research Background

For some of the world’s largest organisations, including governments and multinational corporations, dependence on information has grown rapidly in recent years. However, reports of information security breaches and their associated consequences continue to indicate that attacks on organisations are still escalating. In order to conduct more research to better understand how organisations should formulate strategy to secure their information, I begin by reviewing the current research. Through a thematic review of academic security literature, I analyse (1) antecedent conditions that motivate the potential adoption of a comprehensive information security strategy, (2) themes related to information security strategy, and (3) the yields and benefits that might be enjoyed post-adoption. A contribution from this chapter includes a definition of information security strategy and also identification of the gaps in literature that suggest possible launching points for a research program.

2.1 Chapter Aim

Information resources play a critical role in sustaining business success by driving innovation and opportunities for the development of competitive advantage. As such, preservation of the confidentiality, integrity and availability of these information

---

2 Elements of this chapter are published in the following peer-reviewed articles:


resources is a significant imperative for organisations, as is the need for a viable OrgISS to facilitate information transfer at an organisational level.

The aim of this chapter is to examine extant literature related to information security strategy to understand security of information for the benefit of those decision-makers accountable for driving strategic-level organisational security and ultimately organisational success. The scope of the research is limited to examining the conceptual construct of OrgISS within the IS literature. In particular, I am motivated by calls from other information systems researchers for the development of a comprehensive security strategic framework (Baskerville, Spagnoletti, & Kim, 2014), and for future research into the role that boards of directors may play in information security practices (Higgs et al., 2016; McFadzean et al., 2006; McFadzean, Ezingeard, & Birchall, 2011).

Significantly, some of the world’s largest organisations, including governments and multi-national corporations, have quite publicly suffered security incidents (Dhillon, 2018; Gupta & Sharman, 2012; VonSolms & Van Heerden, 2015). By broadly reviewing the extant literature, a perspective will be established that can support the development of a comprehensive OrgISS, which could then be generalisable to other organisations. This chapter commences with a critical literature review on the topic of OrgISS. Papers from various researchers were analysed and evaluated before being compared for depth of understanding and conclusions drawn. The chapter commentary is explicative, interpretative and centres on the determination of the theory of OrgISS.

This chapter continues in four major sections. Initially I introduce OrgISS, discuss its origins and existing definitions whilst expanding on some of its more central properties. Second, I review the construct space of OrgISS to understand prior research on how OrgISS is conceptualised, the level of analysis from which OrgISS
is approached and contend with propositions for measuring the distinct elements of an OrgISS. Third, I review the nomological network space to assess the environmental antecedents, conceptual elements, and possible yields from an OrgISS. Finally, I draw conclusions and construct a definition to advance understanding of information security strategy.

2.2 Defining Information Security Strategy

Before searching the literature for references to information security strategy and mapping the territory, a clear and precise definition of information security strategy is required. This definition of information security strategy will then be used to guide a review of the literature in subsequent sections of this chapter. Extant definitions of OrgISS are infrequent in the information systems literature so to begin with, in an indulgent departure from convention, the exploration of the term information security strategy is author-centric rather than concept-centric.

Information security strategy is defined by Beebe and Rao (2010, pg. 330) as “the pattern or plan that integrates the organisation’s major IS security goals, policies, and action sequences into a cohesive whole”. These authors believe OrgISS is a documented plan which matches an assessment of external cyber threats with a financially-informed set of internal countermeasures, including the required supporting policies and procedures. Strategy is seen as the means to influence an organisation’s environment through the careful selection of internal controls.

Park and Ruighaver (2008, pg. 27) define information security strategy as:

“an art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defence (sic) organisation’s information infrastructure(s)
against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective”.

These authors believe OrgISS has been developed from the military literature and therefore tends to be focussed more on how to deploy strategies than focus on what goals the organisation is trying to achieve. The environment dictates that OrgISS focus on protection of an individual employee rather than the whole organisation. The focus is more defensive than offensive and is an operational-level threat mitigation process. In terms of attempting to classify OrgISS, their analysis of earlier literature leads them to the conclusion that OrgISS balances three dimensions which are time, space and the decision-making process. The human factor means that OrgISS is not consistent so is more art than science.

Ahmad et al. (2014b) and Park and Ruighaver (2008) believe OrgISS can be used to incrementally improve the quality of the information security program, however there must be a strong link from the OrgISS to the organisational strategic plan to support it. OrgISS is necessary to prevent threats to an organisation’s information. OrgISS can take the form of one of several areas which include deterrence, prevention, surveillance, detection, response, deception, perimeter defence, compartmentalisation and layering. Senior business sponsorship of the security function is also required.

Hong, Chi, Chao, and Tang (2003) do not define OrgISS per se but assert that it is a function of policy orientation, risk management orientation, control and auditing orientation, management systems orientation and contingency management. Contingency management is assessed by the authors as a function of the organisational environment, management and technology.

Sveen, Torres, and Sarriegi (2009) contend that an OrgISS is like any other business strategy: it is the process of building up resources. Information security strategy is
comparable to business strategy in that directs the process of compiling and using resources. These resources however are used to create technical, formal and informal controls to proactively safeguard the organisation. The relationship between the controls needs to be understood to prevent inadvertently exposing the organisation to threats. Typically, organisations do not yet view information security at a strategic level and act reactively to security issues instead of proactively managing risk. By explaining what an OrgISS is, Sveen et al. (2009) describe the construct but have not provided a formal definition. Their insights are still useful however in building up a cumulative understanding.

Carcary, Renaud, McLaughlin, and O'Brien (2016, pp. 24) describe information security strategy as being a capability building block within a framework to “develop, communicate, and support the organization’s information security objectives.” The information security strategy must be linked to the IT strategy and business strategy, and the risk appetite. Another aspect is that the information security strategy must acknowledge regulatory compliance requirements of the organisation.

These definitions give an insight into the difficulties with achieving unanimity on defining OrgISS. Using conceptualisation of OrgISS as an example, Beebe and Rao (2010) explain it is a plan, Sveen et al. (2009) assert it is a process and conceptualisations from Park and Ruighaver (2008), Ahmad et al. (2014b) and Hong et al. (2003) do not fit within either of these. There are many other researchers who have used the term ‘information security strategy’ in their literature however they have not provided an explicit definition.

2.2.1 Information Security Strategy: Plan or Process?

There are two main conceptualisations espoused by organisational scholars when describing OrgISS. These include (1) a static plan, described as an artefact to be shared amongst stakeholders (Beebe & Rao, 2010; Bowen, Hash, & Wilson, 2006;
VonSolms & Von Solms, 2004), and (2) a dynamic process, to be followed by stakeholders concerned with protecting organisational information (Booker, 2006; Brotby, Bayuk, & Coleman, 2006; Flores, Antonsen, & Ekstedt, 2014; McFadzean et al., 2006; Sveen et al., 2009; Van Niekerk & Von Solms, 2010). An understanding of the differences between these interpretations will shed light on its theoretical nature which will affect how to apply OrgISS in practice.

Some information systems researchers view OrgISS as a static plan; a central artefact to be developed that describes the linkages between various organisational concepts such as goals, mission, size, policies and action sequences (Baskerville & Dhillon, 2008; Beebe & Rao, 2010; LeVeque, 2006). In a process orientation, OrgISS involves using a strategy-setting process, whilst incorporating the organisational information systems security goals, such as regulatory compliance, as input. This strategy-setting process can group actions taken according to either the end product ultimately derived such as a strategic security plan, or the processes required such as aligning OrgISS with organisational strategy (Baskerville & Dhillon, 2008). Finally, some information systems scholars do not conceptualise OrgISS at all or characterise it in abstract terms only (Hong et al., 2003; Park & Ruighaver, 2008).

Generally, information security strategy has been defined as an organisation-level construct, that takes direction from organisational goals, and integrates resources and capabilities for securing information to support the achievement of those goals. This aggregated understanding of the definition of information security strategy will now be used to guide a review of any extant literature articles that relate to the concept of “information security strategy”.

### 2.3 Information Security Strategy in Information Systems

Information systems researchers have made individual contributions towards understanding OrgISS from various perspectives. The focus of these researchers
was to address problems including adequate support for organisational strategic vision, information systems-business cohesiveness and coordination of information security efforts. However, a complete and methodical evaluation of OrgISS within the information systems literature has not been accomplished. Therefore, this research seeks to (1) examine what information systems researchers have analysed about the OrgISS construct and (2) the OrgISS nomological network describing its various elements. The OrgISS construct denotes the theoretical domain of OrgISS, specifically how it is conceptualised, at what levels of analysis it can be stratified, and measurement proposals to ensure unit specificity. The OrgISS nomological network refers to an understanding of OrgISS phenomena in the information systems domain, captured through the completion of a thematic analysis.

2.3.1 Literature Review Method

My initial search for information security strategy was for manifestations of it in peer-reviewed information systems journals and selected conference proceedings, found through searching institutional repositories, Google Scholar and the Association of Information Systems basket-of-eight journals (Tarafdar & Davison, 2017). The search consisted of articles that included the complete search string “information security strategy” in English. I searched backwards to discover prior articles and forwards for articles that cited seminal articles (Webster & Watson, 2002). I did not restrict the search based on article age or grade of journal, preferring instead to examine each artefact found for nuances, no matter how small, which could shed light on the evolving understanding of the concept. I also included articles that referred to “information security” but included the word strategies (plural) instead, to facilitate an investigation for example into whether use of the singular ‘strategy’ or plural ‘strategies’ could indicate a shift in level of analysis within an organisation. Finally, I included articles that centred on information security but discussed an implicit aspect
CHAPTER 2: RESEARCH BACKGROUND

of strategy. Note that ‘organisation’ is a term used to denote private companies, public governments, not-for-profit societies and educational institutions.

I included an international standard on information security, as I thought this could have important implications for motivating the use of an OrgISS; however, I did not include any practice-oriented literature such as vendor white papers due to issues with accessibility and peer-review process. Out of the results, 45 articles were deemed of interest, which are listed in Appendix A.

I then examined each article to explore how OrgISS relates to the article’s core paradigm. The following four classifications stratify how central OrgISS is to each article and is adapted from Roberts, Galluch, Dinger, and Grover (2012):

1. *Implicit use of the term*. Information security forms the article’s central theme and strategy is implicit only. Information security strategy does not form the central argument of the article, e.g. (Van Niekerk & Von Solms, 2010).

2. *Provides conceptual support*. Articles use information security strategy to support the development of their concepts, e.g. (Flores et al., 2014).

3. *Used in the research question or hypothesis*. Articles use information security strategy explicitly in their findings or analysis, e.g. (Posthumus & Von Solms, 2004).

4. *Forms the conceptual base for the paper*. These articles are entirely consumed with the discussion of information security strategy, e.g. (Baskerville & Dhillon, 2008).

In summary from Table 2.1, 35 percent of articles (16 papers) that were collected implied some aspect of OrgISS when discussing information security. 27 percent of articles (12 papers) provided theoretical or conceptual support for developing the logic of OrgISS. 18 percent of articles (8 papers) used OrgISS in some part of their
hypothesis, research question or proposition. One fifth of articles (9 papers) were focused purely on discovery of aspects relating to OrgISS. In the next section, I discuss the role of OrgISS in information systems research in more detail.

2.3.2 The Information Security Strategy Construct

From the previous sections, it could be perceived that OrgISS has not been widely developed in the information systems literature, so a more profound analysis is warranted. The following sections discuss in more detail the (1) conceptualisation, (2) levels of analysis and (3) measurement domain of OrgISS.

2.3.2.1 Conceptualisation

I examined what researchers understood the main conceptual context for the OrgISS construct was. The three groups used for this construct are (1) as a plan, (2) as a process, and (3) neither of these.

Table 2.1 presents some conceptualisations (i.e. plans, processes, or neither conceptualisation) and the role of OrgISS in the information systems literature. Out of the 45 articles that were examined, 20 percent (9 papers) used OrgISS as the core of the entire article. 78 percent (35 papers) gave neither explicit conceptualisation of OrgISS. In terms of patterns, when OrgISS is used in the research question (row 3) or forms the theoretical basis for the paper (row 4), it becomes apparent that OrgISS is largely viewed by information systems authors as neither plan nor process.


### Table 2.1. Information Security Strategy Conceptualisations and Role in Information Systems Research

<table>
<thead>
<tr>
<th></th>
<th>Plan</th>
<th>Process</th>
<th>Neither Plan nor Process</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Implicit use of the term</td>
<td>1</td>
<td>1</td>
<td>14</td>
<td>16</td>
</tr>
<tr>
<td>2. Provides conceptual support</td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>3. Used in research question or hypothesis</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>4. Forms theoretical basis for paper</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>3</td>
<td>7</td>
<td>35</td>
<td>45</td>
</tr>
</tbody>
</table>

Given IS researchers generally do not conceptualise information security strategy as plan or process, for the purposes of this thesis, the conceptualisation of information security strategy will be adapted from the military and management perspectives of strategy. Adapting the conceptualisation from Bowdish (2013) in Chapter 1, strategy guides the facilitation and achievement of organisational goals and objectives, using IT infrastructure and information resources to achieve them. Further adapting the conceptualisation of strategy from Porter (1980) in Chapter 1, there are a small set of strategies that offer choices and can be used by organisations by selecting one and then using it to guide decision-making when implementing it operationally.

#### 2.3.2.2 Levels of analysis

For the purposes of clarification, in this thesis a group is a set of individuals who are responsible for some aspect of security within an organisation. Also, in this section where a paper discusses aspects of responsibility for the application of OrgISS at two different levels, the higher of the two was recorded for the purpose of this analysis. This is because the higher level is seen to be more complex, with greater relationship interdependencies.

Table 2.2 shows that while OrgISS is acknowledged to be a multilevel construct, researchers (with only 3 from 45 papers, or 7 percent) do not typically characterise OrgISS from an individual perspective. A significant 60 percent (27 from 45 papers)
of the information systems literature examined contend that OrgISS belongs at an organisational level. At an organisational or inter-organisational level, it is apparent (with 35 from 45 papers, or 78 percent) that scholars believe OrgISS is neither plan or process.

Information security strategy has been applied at country-level to centrally coordinate responses to security incidents involving critical infrastructure and to publish standards for the protection of national assets, however this is outside the scope of this thesis which seeks to understand information security strategy within organisations only (Min, Chai, & Han, 2015).

<table>
<thead>
<tr>
<th></th>
<th>Plan</th>
<th>Process</th>
<th>Neither Plan nor Process</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Individual</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2. Group</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>3. Organisation</td>
<td>3</td>
<td>5</td>
<td>19</td>
<td>27</td>
</tr>
<tr>
<td>4. Inter-organisational</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>7</td>
<td>35</td>
<td>45</td>
</tr>
</tbody>
</table>

The majority of IS researchers consider that the level of analysis for information security strategy is organisation-level, which will be the perspective adopted for the purposes of this thesis.

2.3.2.3 Measurement domain

When operationalising OrgISS, measuring conceptual elements improves their reliability, although extensively focussing on precise quantitative approaches reduces the discovery of interrelated concepts (Strauss & Corbin, 1990). A number of the papers used in this core review confusingly use the word ‘measure’ as an abbreviation for ‘countermeasure’, which is a control installed to mitigate the risk arising from a threat to an asset (Ahmad et al., 2014b; Beebe & Rao, 2009; Park &
Ruighaver, 2008). Two papers contained no mention of ‘measure’ at all (Hong et al., 2003; Kayworth & Whitten, 2010).

Of the papers that addressed the measurement of some aspect of OrgISS, the main areas which were measurable included risk management, goal achievement and quality. Risk management can be measured by efficacy, efficiency and effectiveness of mapping assets and risk against likelihood and impact to create threat assessment based on value, keeping in mind that the value of the security control must not outweigh the value of the asset (Baskerville & Dhillon, 2008). Quality measurement is a key aspect of information security strategy that allows for incremental improvements in security based on measuring currently predicted threats and risks and applying controls to deliberately reduce risk. Predicted threats are the known threats that can be measured and controlled (Baskerville et al., 2014). Information security strategy also includes a finite set of risk-reducing security countermeasures that can be measured (Beebe & Rao, 2010).

To create security strategy-setting products, organisations must set information security strategy goals first, then determine the products of strategy, e.g. vision, values, strategic plans. This strategy-setting process creates a security strategic plan. An organisation’s vision statement articulates desired future state, whilst their core values distinguish them from competitors. Statements of strategic rationale explain how an organisation converts their strategic security goals into an information security strategic plan. Strategic plans have various components such as vision, values, goals, rationale, plus activities for achieving those goals. Goal achievement is measured by the activities undertaken to achieve those goals (Baskerville & Dhillon, 2008).

The foundations of many management frameworks are drawn from quality control principles. The focus on controls and their performance represents a control-centred
security management that has been fundamental in information security strategy for decades. Quality management focuses on measuring histories of common threats with key metrics. This draws management's attention towards preventing threats. Quality improvement is a strategic goal that can be gained through the measuring of routine security tasks that together form a program for the prevention of security incidents. Quality measurement is then based on incremental improvements in security from measuring current threats and risks and applying controls to deliberately reduce risk (Baskerville et al., 2014).

Information security strategy may be matured by measuring and increasing the number and percentage of stakeholders who engage with and use the information security strategy (Carcary et al., 2016). There was no literature that purported to measure OrgISS as a whole, which is a problem that complicates construct validity (Cronbach & Meehl, 1955). For the purposes of this thesis, measurement will be defined via a simple maturity scale, by assessing whether an information security strategy exists or not, and if so, then whether it has been implemented via a strategic process and plan.

2.3.3 The Information Security Strategy Nomological Network

In this section I undertake a thematic analysis within the information systems literature to conceptualise OrgISS at various levels within an organisation and develop a nomological network map to explain the construct and its interrelationships. Thematic analysis is a common technique that has been used by other researchers to examine the information systems literature (Leidner & Kayworth, 2006; Roberts et al., 2012). Thematic analysis is the process of conducting a qualitative content analysis on the literature of interest then listing meritorious ideas from each article before organising them related groups (Cline & Jensen, 2004). To conduct the thematic analysis, I first analysed 45 papers for their interpretation of
OrgISS and then grouped key constructs according to similarities of themes. This resulted in three distinct themes emerging from the analysis, which were antecedents, constituents, and yields.

Antecedents are the precursor conditions that prompt an organisation to consider the use of an OrgISS. Examples of affected organisations include military forces with top secret files, pharmaceutical companies conducting experiments for clinical drug trials and banks facilitating online trading. Constituents are the elements that make up the core of an OrgISS, to be adopted by an organisation seeking to secure its information. Examples include risk management process to understand persistent common threats, security auditing to satisfy external regulators and governance activities to align organisational efforts. Yields are the benefits that can be enjoyed after successfully setting an OrgISS. Examples include the confidentiality, integrity and availability of information, protection of competitive advantage and brand protection and trust.

Based on the thematic analysis and discussion in preceding sections, a logical grouping of the conceptual elements of OrgISS is drawn from the literature and depicted in Figure 2.1. This depiction maps the concepts discussed in the following sections of this review.

![Thematic Map of Information Security Strategy in Organisations in IS Research](image-url)
The sections below discuss these themes in more detail. The assessment is focused on conceptual elements that can be contributed from each journal paper and an overall understanding of what each author believes OrgISS is.

### 2.3.3.1 Antecedents

Antecedents are the precursor conditions necessary to prompt the use of OrgISS and emerged as a theme in the information systems literature after conducting a thematic analysis, as described in the previous section.

At an individual level, there did not seem to be any antecedents apparent in the literature. It is impossible to make an exhaustive claim about this but certainly this is an area that warrants further attention from researchers.

At a group level, one OrgISS antecedent is the requirement for global ubiquitous information availability and a capability to distil incomprehensible threat intelligence complexity and volume in a timely fashion. Incomprehensible threat intelligence leads to uncertainty about the effectiveness of security controls, which security teams avoid (Hofstede, Hofstede, & Minkov, 2010). Ongoing regulatory compliance burden is also a driver. Alignment of IS security strategy with business strategy and goals is paramount (Booker, 2006).

Extensive knowledge about the current applications being used by various groups within an organisation is another requirement for the setting of an information security strategy, along with the inherent ability for organisations to adapt the use of information systems toward supporting the achievement of an organisation’s vision and mission (Dawson, Watson, & Boudreau, 2010).

At an organisational level, antecedents for OrgISS that were apparent in the literature included gathering intelligence about the external environment. An organisation’s information security strategic posture involves a dependence on the external threat
environment, not the continued successful achievement of organisational goals. The increasing complexity and sophistication of dynamic, targeted attacks over time naturally causes a general shift in balance from a preventative posture towards a more response-oriented approach (Baskerville et al., 2014). Organisational ownership of information assets of value is also a key driver towards the adoption of OrgISS (Kelly, 1999). These information assets of value served as the basis for achieving organisational goals and a key motivation for adopting an information security strategy is the achievement of these goals (Szabó, 2017). Organisations also recognise the threat to the health and safety of their customers and employees which motivates the adoption of an information security strategy (Layton, 2016). A risk assessment can inform the scope and scale of an information security strategy, which is selected in turn to support the achievement of organisational goals (Layton, 2016).

At the inter-organisational level, an OrgISS is the broad-based approach to organisation-wide information security that supports regulatory compliance. Regulation imposes a significant coercive effect on organisational decisions to implement security initiatives (Hu, Hart, & Cooke, 2007). Compliance is seen as the prescriptive minimum set of requirements to prevent security incidents. An organisation must consider the implications of possible future security incidents to develop awareness of information distribution and protection mechanisms (Banker, Chang, & Kao, 2010; Kayworth & Whitten, 2010; Tutton, 2010). This regulatory compliance-driven approach however only forms part of a holistic approach to security (Anderson & Choobineh, 2008). Government regulations can be coupled with self-administered internal regulations and these all affect an organisation’s information security strategy (Lee, Kauffman, & Sougstad, 2011). Information security strategy selects controls to ensure regulatory compliance, protect the IT infrastructure that the information resides on and deliver CIA to users. To expand, the
internal requirements of an OrgISS are to address business issues and protect the IT infrastructure, and the external requirements are legal and regulatory compliance and adoption of standards and best practices are also required (Posthumus & Von Solms, 2004). As well as passing regulations for organisations to comply with stipulating that they must develop an information security strategy, governments must actively monitor and reward or punish organisations for the regulations to be effective (Hou, Gao, & Nicholson, 2018).

Examination of the industry in which the organisation competes and sufficient knowledge of industrial and economic considerations of an organisation’s competitive landscape are also required. OrgISS must be created at the same time as the business strategy and depends on accurate needs analysis prior. Senior and middle management are responsible for ISS creation and it is designed to support internal communication and decision making. Corporate knowledge assets can then be inventoried, and values defined (Baets, 1992). The organisation’s market position in the industry it competes in is also important, because if it is the market leader through innovation, then managing its information better should improve security, but if it relies on operational efficiency to maintain a leading market position, then improving threat intelligence or increasing security controls is a better strategy (Majchrzak, 2014).

The existence of a strategic information systems plan is notable, as it dictates the formulation of the information security policy by providing essential details of the business context or competitive landscape (Doherty & Fulford, 2006). Failure of political pressure and economic sanctions are important preconditions that may motivate the commencement of information warfare (Baskerville, 2005, 2010).

OrgISS is inconsistently defined but is largely perceived to be a mix of technical, formal and informal controls that seek to deter and prevent information attacks
against an organisation, according to security executives. It is primarily based on prevention of incidents arising from advanced persistent threats (APT) using technical controls against external threats that are seen to be increasingly more frequent, novel and costly (Beebe & Rao, 2009).

Environmental and organisational conditions, managerial understanding and actions, quality improvement initiatives and organisational achievement lead to use of OrgISS (Cline & Jensen, 2004). Regulatory, political and legal compliance plus adoption of standards and best practices motivate the use of OrgISS (Kim, Wang, & Ullrich, 2012; Posthumus & Von Solms, 2004). Standards exist which detail management of information security which in turn could assist with OrgISS development (Brotby et al., 2006; ISO/IEC, 2013).

2.3.3.2 Constituents

Constituents are the central conceptual elements of OrgISS and emerged as a theme in the information systems literature after conducting a thematic analysis, as described in Section 2.3.

*Individual level*

This section seeks to explore what role an individual has in contributing towards the overall success of the strategic use of information security. At an individual level, there were no constituent elements that specifically related to information security strategy, however this is unusual because it is commonly accepted that overall security depends on the weakest link which is typically an individual. To make it easy for individuals to follow an information security strategy and reduce stress, it should be simple to understand and not complex (Ament & Haag, 2016). This may represent an opportunity for further research.

*Group level*
This section examines the IS literature to discover the dynamics of groups working to support the strategic use of information security. At a group level, the constituent components of the OrgISS construct are varied and numerous. One is the identification and protection of knowledge assets, which can be resources forming a competitive advantage and can be either held in the human brain or in organisational documents, routines, procedures and practices. Knowledge leakage is a security incident which can temporarily affect an organisation’s competitive advantage and affect its reputation, revenue streams, remediation costs and productivity. One way to mitigate the risk of information leakage is to classify information as either core or non-core, and then gain benefits such as cost reduction by outsourcing the management of the non-core information (Feng, Feng, Zhang, Chen, & Li, 2018).

Tangible knowledge assets typically leaked include strategies, policies, product knowledge and customer details. The information security strategy goals are to ensure knowledge assets’ confidentiality, integrity and availability (Agudelo, Bosua, Ahmad, & Maynard, 2015; Daneva, 2006). Mitigation or protection of knowledge is achieved through initial classification of information assets, then compartmentalisation, development of technical solutions, policies, procedures, culture and legal support (Ahmad et al., 2014a; Shedden, Ahmad, Smith, Tscherning, & Scheepers, 2016).

OrgISS should guide the overall security budget for an organisation, to enable the security staff group and their management to fund and implement security resources that optimise security outcomes based on expense versus benefits (Anderson & Choobineh, 2008). When using an OrgISS to allocate security budget to fund security controls to secure information, organisations should balance spending between both the technical aspects as well as the social or human aspects (Park, Na, & Chang, 2016). OrgISS includes the examination of stratified responsibility within an organisation that cohesively achieves overall information systems security. Decisions
made by one layer of responsible agents affect decisions made by agents in other layers and their communication is vital. OrgISS success depends on action taken by responsible agents rather than technological controls. Achievement of OrgISS allows alignment with policies and regulatory compliance efforts (Backhouse & Dhillon, 1996).

One essential element of OrgISS is a mix of technical, formal and informal controls to ensure regulatory compliance, protect the IT infrastructure that the information resides on and deliver CIA to users (Beebe & Rao, 2009; Posthumus & Von Solms, 2004; Sveen et al., 2009). One of the effective controls that should be introduced at the organisational level is a comprehensive information security education, training and awareness program, along with clear governance processes for allocating responsibility within the organisation (Alshaikh, Maynard, Ahmad, & Chang, 2018; Maynard, Tan, Ahmad, & Ruighaver, 2018; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). Other elements of an information security strategy, specifically in the government industry, are examination of the types of data held, human considerations, strategic policies, and the technological infrastructure (Priyambodo & Prayudi, 2015).

An information security strategy needs to take a comprehensive approach to security and address not only the technical side of controls, but the human interaction required ensure their effectiveness as well. OrgISS typically suffers from a lack of resourcing in organisations due to it not increasing revenue or reducing expenses. OrgISS also clashes with business attempts to make information available to increase productivity. SETA is also required to ensure user adoption, as is a strong security culture. As well as information being seen as a security asset, properly trained employees can be seen as security assets as well, which lowers overall risk (Van Niekerk & Von Solms, 2010).
Information security strategy is used to defend an organisation against external threats and therefore most of the content in an OrgISS is centred on controls that mitigate risk from external threats. Information security policies are an important part of OrgISS however SETA and constant monitoring is required to ensure employees read and comply with the policies. Limited resources mean tough decisions must be made about what controls will be put in place to mitigate threats and unfortunately due to the most trusted advice to executives coming from technical people (Chief Information Officer and below), technical controls are purchased instead of also focussing on the social side of security (Taylor & Robinson, 2014; Van Niekerk & Von Solms, 2010). OrgISS includes the capability to respond to attacks effectively, which stems from supplementary forces creating a time buffer through the employment of defence-in-depth design to allow the responding forces enough to time to deploy to the breach from the central holding point (Burnburg, 2003). In order for an organisation to develop this capability to respond to attacks, a high level of technical competence is required, which must be explicitly addressed through an OrgISS (Hall, Sarkani, & Mazzuchi, 2011; Tu & Yuan, 2014).

Information systems solutions underpin business products and services and are therefore critical in maintaining an organisation’s competitive advantage. An OrgISS must focus on how to maintain competitive advantage in the face of rapidly changing ICT infrastructures. Significant investment in technologies that quickly become outdated might not be the best use of valuable resources and instead organisations could consider the use of innovative emerging ICT solutions (Lee et al., 2011). These considerations fall into two categories: 1. Business alignment, which includes all higher order business process management, customer management, supply chain management, and 2. Technical alignment, which includes the use of emerging IT and its integration into existing ICT infrastructure. Security is paramount in the decision
about whether to use emerging ICT to fill business alignment gaps and enable competitive advantage (Cegielski, Bourrie, & Hazen, 2013).

Organisational level

The organisational level is where most influence can be exerted internally to achieve success in supporting a strategic application of information security and deserves special attention in an examination of the IS literature. At an organisational level, OrgISS can be used to incrementally improve the quality of the information security program. There must a strong link from the OrgISS and the IT strategy to the business strategic plan to support it (Drnevich & Croson, 2013; Dutta, 1996). The OrgISS needs to be completely aligned with the business strategy to ensure that security needs can be met whilst the business strategic and operational objectives, chief amongst them being availability of applications and infrastructure, are also met (Fibikova & Mueller, 2012). This allows strategic plans to incorporate appropriate investments and allows for organisation-wide coordination of security processes (Carcary et al., 2016; Flores et al., 2014; Hou et al., 2018; Tu, Yuan, Archer, & Connelly, 2018).

OrgISS belongs to one of a number of areas which include deterrence, prevention, surveillance, detection, response, deception, perimeter defence, compartmentalisation and layering. These generally fall into one of two focus areas: time (pre- or post-attack) and space (inside or outside the organisation's network). Senior business sponsorship of the security function is also required. (Ahmad et al., 2014b; Park et al., 2016).

Information security strategy fits within the context of information security governance within the boardroom and the public sector (Fitzgerald, 2016). An OrgISS is the collection of security activities that support the overall agency strategic plan and they are documented so that performance against plans can be reported on annually.
OrgISS is a process which annually evaluates suggestions made by security staff at different levels in various divisions and funds them based on merit. This OrgISS is a framework, documented in a plan, which supports incremental improvement, alignment with agency mission, and awareness and monitoring of external threats (Bowen et al., 2006; Johnson & Goetz, 2007).

OrgISS protects only the more valuable information assets in order to reduce expenditure. This is achieved through policies and communication structures, director-level sponsorship of security initiatives, measuring success and administering sanctions for security policy violations (Da Veiga, 2016). It is important for organisations that are emergent and depend on web-based capabilities to develop policies that are equally dynamic (Baskerville & Siponen, 2002). Identity and access management is important to overall success as is security incident detection and response activities (Ahmad, Hadgkiss, & Ruighaver, 2012; Ahmad, Maynard, & Shanks, 2015; Kelly, 1999). Corporate knowledge assets can then be inventoried and values defined (Baets, 1992).

Information security strategy has been described as a balance that can be actively chosen by organisations when directing efforts to increase security towards either prevention or response-oriented principles and practices based on the external threat environment. This choice is then termed the information security strategic posture. Uncovering the predilection of organisations towards one or the other can be exposed by examining activities undertaken both pre- and post-security incident. If security functions are outsourced to other companies or individual contractors, then these actors need to equally adhere to the policies and strategy adopted by the parent organisation.

The implementation of information security strategy can be dynamically changed should the review and analysis of a serious incident suggest this is warranted. The
increasing complexity and sophistication of dynamic, targeted attacks over time will naturally cause a general shift in balance from preventative towards a more response-oriented approach. Information security strategy in the past has often focused on the applicability of controls to neutralise threats. The focus on controls was elevated to a strategic level within organisations. An organisation’s information security strategy must adhere to the principles and practices of either the prevention (pre-security incident) or response (post-security incident) paradigms and a weighting on one over the other can result in a reduced number of security incidents or increased security. An organisation’s information security strategic posture involves an emphasis on either paradigm which is causally linked to the external threat environment but not to the continued successful achievement of organisational goals. If the labour involved with security functions is outsourced to other companies or individual contractors, then they need to equally adhere to the security policies and strategy adopted by the parent organisation (Baskerville et al., 2014).

OrgISS is a documented plan which matches an assessment of external cyber threats with a financially-informed set of internal countermeasures, including the required supporting policies and procedures. OrgISS is the means to influence an organisation’s environment through the careful selection of internal controls, and can use situational crime prevention to introduce a deterrent option within the risk management section (Beebe & Rao, 2010).

For an information security strategy to be effective, it must receive executive-level sponsorship and be linked to the organisational short and long-term goals. It is centred in risk management, identifying controls to mitigate known threats (Da Veiga & Eloff, 2007). Better alignment of the business strategy with the information security strategy should improve the awareness, funding and effectiveness of security controls (Tu et al., 2018). For organisational-wide risks, an OrgISS must lower risk by increasing security, in an inverse relationship. Risk is measured as unanticipated loss
and can include intangible loss as well as tangible. Reducing risk lowers anticipated loss, which changes an organisation’s security posture. Quantifying risk of anticipated loss requires recording of previous loss from security incidents (Cavusoglu, Cavusoglu, & Raghunathan, 2004; Ryan & Ryan, 2006).

Conceptual constituents also include regulatory compliance, teleworkers, organisational agility, business justification requirements, reactive quality improvement and community cloud initiatives. Applied constituents include securing the network, compute and storage ICT infrastructure, then securing applications and information before regulatory compliance and governance. Global governance can still allow for regional control (Booker, 2006).

Information security depends on information security strategy and is a function of policy orientation, risk management orientation, control and auditing orientation, management systems orientation and contingency management. The external environment places various demands on the organisation which changes to continue the achievement of the organisational objectives. The OrgISS is contingent on the environment when changing to maintain focus on the organisational objectives (Hong et al., 2003).

The operational objectives of OrgISS are to protect information assets from the risk of loss, lack of business continuity, misuse, leakage, unavailability and corruption. OrgISS is a top-down process that links with the business processes, both physical and technical, and strategy. Standards exist which detail management of information security that could assist with ISS development. OrgISS consists of policies that promote the business goals and strategy. It couples with governance to provide boundaries and procedures for employees along with their roles and responsibilities. SETA must be constantly provided to staff, along with adequate resourcing to ensure success. The staff includes on-site and off-site professionals, managers, executives,
senior executives and boards of directors. Business alignment occurs when it provides input to the OrgISS along with business processes, risk assessments, and information resources. An OrgISS program applies policies, roles, responsibilities, authority, accountability, control framework, risk assessments, information asset classification, controls for people, process and tools, linkage with the business processes, security incident response, identity access and management, performance measurement, and SETA (Brotby et al., 2006; Da Veiga & Martins, 2015; Hinde, 2002).

Information security strategy aligns business objectives with operational processes. It requires pervasive reinforcement of SETA with employees to be effective. The OrgISS must consider the production, sales and maintenance phases involved in an organisation’s product or service lifecycle. The reason is that security risk must be objectified as an entity that is shared between manufacturer and consumer and both must decide their risk posture to allow them to make smarter procurement decisions (Oshri, Kotlarsky, & Hirsch, 2007).

Information security strategy is a strategic framework that guides decisions and priorities at operational and tactical levels of an organisation across all divisions. It is constantly revised and takes into consideration the organisation’s risks and culture, performance and assurance, SETA, suppliers and customers. It is technology-based but driven by the business to be cost-effective and focussed on priorities (Hinde, 2002).

Information security strategy is built on IT products and solutions but extends to include the employees in the business. Specifically, OrgISS integrates director-level security sponsorship and hierarchical structures that provide security governance. Responsibility for ISS, including its policies and standards, is held by the business not IT because an appreciation of the competitive landscape of the organisation must
be included. The three goals are balancing information confidentiality against availability, ensuring regulatory compliance and conforming to the organisational culture (Kayworth & Whitten, 2010).

OrgISS requires the attention and approval of the board of directors and Chief Executive Officer (CEO) because they are accountable for its outcomes (Da Veiga, 2015). Members of the governing body put an OrgISS into effect by using corporate governance, specifically a corporate information security policy, as a tool to communicate with and direct management in the organisation (Kinnunen & Siponen, 2018). Information security policies can direct the setting of an information security strategy document as well as lower-level security documents such as technical manuals (Kinnunen & Siponen, 2018).

The role of information security strategy is to be a form of communication from the board of directors to all the stakeholders involved, including management, business and external stakeholders as well (Bobbert, 2015). Although developed by executives, managers and technologists within the organisation, it is a means through which the directors can shape employee behaviour by the policies enshrouded within, which then leads to culture development (ISO/IEC, 2013; Ruighaver, Maynard, & Chang, 2007). An information security culture assessment can serve as an input to an information security strategy, to improve guidance to employees in an organisation on managing information, as per any strategic information security policies that have been set (Da Veiga & Martins, 2015; Ruighaver et al., 2007). Information security strategy is set by the senior executives in an organisation and includes a set of policies that are guided by the advocated corporate values and based on tacit assumptions typically set by the company’s founder.
OrgISS is perceived as both a passive entity, i.e. a plan, and an active entity, i.e. a process. OrgISS should include SETA early in the process of its development to assist with OrgISS selection to solve key issues. A crucial point around OrgISS is ownership and people. Directors are accountable for security and delegate the responsibility for the development of OrgISS to managers who then consider how the employees interact with it. Information security strategy is used by the governing body to direct the efforts of executive management. The process is that executive management develop the information security strategy, the governing body then approves it and then the executive management implement it (ISO/IEC, 2013). It is an artefact developed as part of a process.

OrgISS requires the attention and support of the board of directors and CEO because they are accountable for its outcomes. They affect OrgISS by using corporate governance, specifically a corporate information security policy, as a tool to communicate with and direct management in the organisation. Two-way communication is then required back from management to the board and executive in the form of regular progress reports. This allows for incremental quality improvement (ISO/IEC, 2013; McFadzean et al., 2006; Posthumus & Von Solms, 2004; Vroom & Von Solms, 2004). OrgISS must consider corporate governance, organisational, policy, best practice, ethical, certification, legal, insurance, personnel/human, awareness, technical, measurement/metrics (compliance monitoring/real time IT audit) and audit aspects of an organisation. Partial implementation simply delays the full implementation of an OrgISS causing frustration. OrgISS must also include top level sponsorship, liaison with the business, build on known threats and begin with a preventative approach, leverage best practice as well as standards, include policies, compliance enforcement and monitoring, governance structure, SETA and providing those responsible for security with autonomy (VonSolms & Von Solms, 2004).
OrgISS constituents include risk management components such as disaster recovery and business continuity, insurance, audits and new business units and groups (Cline & Jensen, 2004). Without a focus on business continuity, it is entirely possible than in the event of an ICT infrastructure disaster a lack of business continuity translates directly into quantifiable revenue loss. This loss is quantifiable and needs to be prevented with an OrgISS. The organisational goals, strategy and policies are required to support services such as confidentiality, integrity and availability plus also accountability, authenticity and reliability (Van Der Haar & Von Solms, 2003). The way that management focuses on risk influences the strategic approach taken to mitigate identified risks, and the controls then implemented against various threats (Taylor & Robinson, 2014).

Information security strategy needs to focus on people and process not only tools, as these are often the main causes of security failure by hampering the protection of information (Da Veiga, 2015). Security culture lowers risk to information assets by reducing insider threats from malicious and non-malicious employees, which can have economic benefits (Da Veiga & Eloff, 2010; Hua & Bapna, 2013b). OrgISS seeks to protect against rational individuals perpetrating attacks rather than automated technical attacks. The preventative approach relies heavily on deterrence and advocates that effectiveness is derived from sanctions being believed to be swift, severe and certain (D'Arcy & Herath, 2011; Kankanhalli, Teo, Tan, & Wei, 2003).

**Inter-organisational level**

The inter-organisational level of information security is where organisational benefits can potentially be mutually shared by contributing organisations for their individual success and factors that influence this are examined in the following section. At an inter-organisational level, compliance must be audited and a firm’s auditing costs, incurred through engagement with an external auditor, can be lowered through a
focus on IT assurance. This IT assurance includes high-quality IT documentation and an emphasis on systems security which lowers the cost because it makes the work of an auditor easier and quicker, therefore considerably lowering the time and materials auditing cost (Banker et al., 2010).

OrgISS facilitates information warfare, which forms just one layer of a conflict with an adversary. The four layers of a nation attack are political, which then escalates to economic sanctions, then information warfare and finally full kinetic warfare (Baskerville, 2010). Some information assets may be resources that create strategic competitive advantage for organisations. If these lose their confidentiality through a security incident, then their integrity may be lost forever, along with the value of the advantage (Feng et al., 2018). When a security incident of this nature is disclosed to the market, there are implications for the organisation’s share price (Campbell, Gordon, Loeb, & Zhou, 2003).

OrgISS is the process of dynamically assessing customer perceptions of the organisation’s online transactions, with a view to increasing the security of transactions to prevent a decrease in brand trust in the marketplace. Regulatory pressures have increased the requirement for this defensive process (Datta & Chatterjee, 2008). OrgISS must include an organisation’s business and cyber policy considerations and depends on the political environment in an organisation’s country of origin, which must synchronise with that of governments from other countries. The legal frameworks in various countries must harmonise globally to allow prosecution in the event of an attack. Shouldering the responsibility for lowering attacks will involve constitutional examination for potential conflicts, a willingness to collaborate and a system for measuring attacks however the benefits are that the world will be a safer place (Kim et al., 2012; Majchrzak, 2014). OrgISS can be used by a country to align defensive resources and capabilities to protect the country from a cyber-attack (Min et al., 2015). Refer to Table 2.3 for a summary of these concepts.
2.3.3.3 Yields

Yields are the goals achieved from the successful use of OrgISS and emerged as a theme in the information systems literature after conducting the thematic analysis described in Section 3.3. At an individual level, the development and application of a robust program to actively shape and improve the information security culture within an organisation leads to transforming individuals from weak links into strong allies for protecting organisational information (Karyda, 2017). At a group level of analysis, there were no apparent benefits arising from OrgISS. At an organisational level, the security goals are to ensure information assets’ confidentiality, integrity and availability (Ahmad et al., 2014a). Another yield is that high quality information is made readily available (Doherty & Fulford, 2006).

OrgISS is about deciding the overall security budget for an organisation, to enable security staff and their management fund and implement security resources that optimise security outcomes based on expense versus benefits (Huang, Hu, & Behara, 2008). These security resources include plans, staff, procedures, guidelines and technology. The OrgISS depends on an organisation’s risk appetite, threat prevalence, commercial dependency on internet and staff training. Losses depend on size of organisational assets, business continuity capabilities, profitability, threat intelligence and risk appetite. Security budgets are bounded by expected probable losses. Security is often compliance-driven rather than a holistic approach to security (Anderson & Choobineh, 2008).

Loss prevention efforts should also guard against revenue loss (Van Der Haar & Von Solms, 2003). Performance reporting is another goal but requires tracking of key KPIs including systems, assigned assets, people, processes, compliance and auditing and customer service (Booker, 2006). Finally, the protection of competitive advantage remains an important business goal (Cegielski et al., 2013).
At an inter-organisational level, OrgISS yields can include the misdirection of an adversary’s attack assets, even from other nation-states, to protect information assets and physical critical infrastructure assets. Yields can also include the disablement of adversary CI, reduce foreign military abilities and impair foreign government operations (Baskerville, 2010). OrgISS goals centre around an organisation’s security needs and the requirement to lower impacts from security incidents, and can also lower the risk of adverse litigation outcomes and achieve information confidentiality, integrity, availability, authenticity and non-repudiation (Brotby et al., 2006). An important benefit is share price protection and shareholder value (Campbell et al., 2003; Hovav & D’Arcy, 2003). Regulatory compliance avoids adverse sanctions by ensuring external agencies are kept fully informed (Banker et al., 2010). OrgISS yields also include retaining customers, security incident prevention, improved business processes and public reputation (Cline & Jensen, 2004). Failure to implement an OrgISS sensibly may result in estranged customers and tarnished reputation (Datta & Chatterjee, 2008; Oshri et al., 2007). Refer to Table 2.3 for a summary of these concepts.

### 2.3.3.4 Key findings of thematic analysis

Several gaps in knowledge have appeared through the conduct of this research. At an individual level of analysis, there appears to be very little research conducted into the role of an individual when supporting OrgISS. There appears to be many contributors to various aspects of the OrgISS construct but there does not seem to be any one unified conceptualisation or theory. Information security cannot be managed only at an organisational level but must include an inter-organisational level as well to take advantage of most of the yields.
Table 2.3 presents a thematic map of OrgISS derived from the results of the literature review, as described in the previous sections, and summarises the key themes found.

Table 2.3. Thematic Map of Results from Literature Review of OrgISS

<table>
<thead>
<tr>
<th>Antecedents</th>
<th>OrgISS Constituents</th>
<th>Yields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-organisational</td>
<td>Inter-organisational</td>
<td>Inter-organisational</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>Regulatory compliance</td>
<td>Foreign adversary impairment</td>
</tr>
<tr>
<td>Industrial factors</td>
<td>Information warfare</td>
<td>Litigation risk management</td>
</tr>
<tr>
<td>Economic factors</td>
<td>Information asset protection</td>
<td>Share price protection</td>
</tr>
<tr>
<td>Political factors</td>
<td>Environment scanning</td>
<td>Regulatory compliance</td>
</tr>
<tr>
<td>Legal factors</td>
<td></td>
<td>Public reputation</td>
</tr>
<tr>
<td>External threat</td>
<td></td>
<td>Customer trust</td>
</tr>
<tr>
<td>environment</td>
<td>Standards</td>
<td></td>
</tr>
<tr>
<td>Organisational</td>
<td>Organisational</td>
<td>Organisational</td>
</tr>
<tr>
<td>Valuable information</td>
<td>Boardroom accountability</td>
<td>Confidentiality, integrity</td>
</tr>
<tr>
<td>OHS</td>
<td>Quality improvement</td>
<td>and availability</td>
</tr>
<tr>
<td>Risk</td>
<td>Information asset management</td>
<td>Probable loss mitigation</td>
</tr>
<tr>
<td></td>
<td>Labour source</td>
<td>Performance reporting</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td>Competitive advantage</td>
</tr>
<tr>
<td></td>
<td>Organisational agility</td>
<td>protection</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business continuity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>People and process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident prevention</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Group</td>
<td>Group</td>
</tr>
<tr>
<td>Ubiquitous information</td>
<td>Knowledge leakage prevention</td>
<td>None</td>
</tr>
<tr>
<td>availability</td>
<td>Security budget</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Responsibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident response</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICT infrastructure</td>
<td></td>
</tr>
<tr>
<td>Individual</td>
<td>Individual</td>
<td>Individual</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>Culture</td>
</tr>
</tbody>
</table>

68
2.4 Theoretical Background

The role of prior theory and theoretical frameworks can be useful in qualitative studies and sensitivity to these can help identify key concepts that have been previously discovered or help inform the choice of methodology to be used in the study (Corbin & Strauss, 2008; Wiesche, Jurisch, Yetton, & Krcmar, 2017). Both a thematic and a theoretical literature review are recommended prior to grounded theory data collection (Urquhart & Fernandez, 2013). Identification and use of related theoretical frameworks however should not inflexibly dictate the terms of original qualitative research but rather offer a departure point from which the burgeoning study can begin (Corbin & Strauss, 2008). Researchers have even been advised to only briefly review previous theoretical research to reduce undue negative impact on creative development of concepts and relationships and confirmation bias (Corbin & Strauss, 2008; Gioia, Corley, & Hamilton, 2013). Accordingly, I review information systems theories within the context of information security strategy, and the findings follow.

In contrast to deductive studies that seek to ‘prove’ or disprove theory, the aim of grounded theory is to understand meaning when generating concepts, categories and properties from data and this is assisted by theoretical comparisons (Corbin & Strauss, 2008). Reviewing extant theories allows the researcher to understand the concepts of ‘information’ or ‘security’ for example, so that this understanding can then be brought to bear on emerging concepts from collected data to improve comparison with existing concepts (Birks, Fernandez, Levina, & Nasirin, 2013; Corbin & Strauss, 2008). Theoretical comparison occurs before the data is collected to improve later analysis, not after theory development (Corbin & Strauss, 2008).

Although finance, economics and criminology disciplines have theories in their literature related to the security of assets against threats, an examination of all these
is beyond the scope of this thesis thus the scope of this thesis is limited to research within the information systems discipline (see Section 1.3 Aim and Scope). Larsen and Eargle (2018) maintain a web-based resource that lists theories which are commonly used in information systems, including theories originating from other disciplines (Larsen & Eargle, 2018; Straub, 2012). It is designed for both doctoral students and senior academics to assist in developing their theoretical sensitivity and has been used to support research published in top journals (Markus & Saunders, 2007). As such, it formed the basis of my search for theories in information systems that potentially relate to information security strategy. The 104 theories currently listed on this website were searched for the keywords: asset, resource, threat, control, information, security, or strategy. These keywords are based on common terms found during the thematic literature review. This search yielded a list of 34 theories (see Table B.1 in Appendix B: Theoretical Background for the complete list) which were then reviewed for relevance and limitations in the context of information security strategy, and a resulting summary of theories is listed in Table 2.4, with format adapted from Ransbotham and Mitra (2009).
Table 2.4. Information Systems Theories and Information Security Strategy

<table>
<thead>
<tr>
<th>Philosophical stance</th>
<th>Summary and References</th>
<th>Relevance for OrgISS</th>
<th>Limitations for OrgISS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social control theories</td>
<td>Organisation are made of groups which are made up of individuals, which all require structure and governance to maintain order (see references 1, 4, 10, 17 in Appendix B).</td>
<td>Interaction between groups and organisations via information technology, categorises information and applies rules.</td>
<td>Originates at individual or group level not organisation level. Does not assess interaction with external threat actors.</td>
</tr>
<tr>
<td>Systems theories</td>
<td>Organisations don’t exist in a bubble. Like a Venn diagram, information is used by organisations and customer/supplier/other stakeholders to interact at their boundaries (see references 2, 11, 19, 29, 33, 34 in Appendix B).</td>
<td>An OrgISS is organisation-level, involves stakeholders, and is different depending on the organisation using it, with a focus on reducing costs.</td>
<td>The focus on describing information but not threats or security controls does not fit with OrgISS.</td>
</tr>
<tr>
<td>Motivational and productivity theories</td>
<td>Goal achievement is predicated on willingness and ability of individuals (see references 3, 6, 9, 12, 13, 14, 15, 20, 21, 22, 25, 31 in Appendix B).</td>
<td>OrgISS selected from generic strategies for organisation-level adoption, using information resources to improve performance.</td>
<td>The focus on individual-level offers no link to strategy or approaches to securing the resource.</td>
</tr>
<tr>
<td>Organisational environment theories</td>
<td>Organisations compete in industries, interact with regulators, and are subject to laws (see references 5, 7, 8, 23, 28, 30 in Appendix B).</td>
<td>Strategic approach to securing information needs internal and external contextual examination.</td>
<td>Non-core focus on competition, and substitute products and services, also lacks explanatory power.</td>
</tr>
<tr>
<td>Valuable information and resource theories</td>
<td>Controlling value in information to create resources that can be used to achieve organisational goals (see references 16, 18, 24, 26, 27, 32 in Appendix B).</td>
<td>Information-based factors that affect organisation-level strategic performance.</td>
<td>Lacking focus on security of information in response to threats to maintain its utility as a resource.</td>
</tr>
</tbody>
</table>

Upon completion of this review of extant theories in information systems, it is apparent there are no theories where the philosophical stance relates directly to information security, much less directly to information security strategy. This gap offers an opportunity to contribute to knowledge by investigating the philosophical stance and properties of information security strategy.
2.5 Proposed Definition of Information Security Strategy

Based on the literature review, I construct a definition proposing the meaning of information security strategy:

“Information security strategy guides the achievement of organisational goals and objectives using IT infrastructure and information resources to achieve them, is motivated by antecedent conditions that balance internal information needs and external environmental factors to yield information security benefits to the organisation, and is selected from a small set of generic strategies to guide decision-making when implementing operationally.”

2.6 Chapter Summary

This literature review surveyed the literature, mapped the territory and identified gaps. It illustrated various aspects of information security strategy and key themes were explored and grouped. In terms of gaps, there is no single, well-developed definition or conceptualisation apparent in the literature that comprehensively explains the information security strategy construct and its relationships. Additionally, information security is ostensibly lacking to a large extent from the strategic organisational literature and even from strategic information systems literature.

This review of this literature was used to inform the development of initial questions for interviews, as described more fully in the following chapter. For example, some of the yields that can be gained from employing an information security strategy (as listed in Table 2.3) are reduction of litigation risk, share price protection, regulatory compliance, public reputation, customer trust, confidentiality, integrity and availability, probable loss mitigation, performance reporting, and competitive advantage protection. These factors together form the basis for a question about yields in the interview protocol, as can be seen in Appendix D: Interview Protocol.
Chapter 3:  Research Approach

This chapter explains the proposed research approach for investigating the research topic information security strategy. There are many interpretations to be made when analysing a research topic within the context of existing research frameworks. It is important to articulate the philosophical stance taken when investigating the research question because if there is a mismatch between the research foundations set in the literature review and the approach taken to investigate the phenomenon, then that can affect the viability of the final contribution.

3.1 Chapter Aim

This chapter aims to explain every part of the research framework, from ontological reality all the way through to the data collection methods and analysis procedures. This chapter responds to the research question that was articulated in the chapter one, describing the most appropriate approach to create new knowledge and fill the gap. It begins with an introductory overview of the design for this research programme, giving an account of each of the areas in the overall research process map. It continues by describing ontological reality, the epistemological approach to understanding how the reality of the subject matter can be assessed, the philosophical stance that ties together the epistemology and the methodology, a defence of the selected phenomenological grounded theory methodology (GTM), and finally the methods and data collection processes.

3.2 Aim of the Research

To reiterate from Chapter 1: Introduction, the singular aim of this research is to develop an understanding of how an information security strategy is best used by
organisational security leaders to secure information. This understanding should then lead to the building of a theoretical model of information security strategy. For the purposes of this research, *theory* is defined as “*any coherent description or explanation of observed or experienced phenomena*” (Gioia & Pitre, 1990, pp. 587).

To achieve the research aim, this research program will investigate what an information security strategy phenomenon is, how one is selected, how one is used, and what some of the benefits of using one are.

### 3.3 Research Process Structure

The design of research begins by identifying the research problem, which must be significant enough to warrant the research effort to resolve it (Evans et al., 2011). The research aim is written to solve the research problem, which sometimes examines how two variables affect one another, or instead develop a deep understanding of a concept (which is the focus of this thesis). It is always singular in form (i.e. there can only be one aim in a research project) (Evans et al., 2011). The research hypothesis is sometimes an informed claim that two variables listed in the research aim either affect each other in a particular direction or have no effect (null hypothesis), but sometimes can simply offer a proposed understanding (Evans et al., 2011). A carefully crafted research question often responds to the research hypothesis and directs the overall research activity (Bono & McNamara, 2011; Evans et al., 2011).

The research question must be compatible with the nature of the research design. That is, if the research hypothesis posits the causality of a variable change, then the research question must allow for variable measurement more than once (introducing a time interval between measurements), or manipulating a variable that is linked to another variable (Bono & McNamara, 2011). Alternatively, qualitative studies may instead search for a deeper understanding on a topic, which is what this thesis offers.
3.3.1 Overall Research Process Map

This section describes the overall process for conducting research into this topic. The theory-building in this study begins with phase 1a literature review (see Figure 3.1) which surveys the literature on the topic and orders the results via a simple framework to organise concepts in the extant knowledge. This map demonstrates how the existing knowledge is organised to help identify the gap in knowledge that this thesis fills. As well, phase 1a identifies the supporting theoretical base that guides the subsequent model formulation, which in this case is contingency theory. The data collection consists of three parts, phase 1b conducting 25 expert interviews, phase 1c recording field notes whilst observing research participants during the course of their interviews, and phase 1d analysing several information security strategy documents, when they existed and could be anonymised and released to me. Before any data collection was conducted, ethics approval was sought and obtained from the institutional ethics review board and a copy of the approval letter can be viewed in Appendix C: Ethics Approval.

![Figure 3.1. Overall Research Process Flow Chart](image)

The data from phases 1b, 1c and 1d were analysed and interpreted to develop a proposed conceptual model of information security strategy. This model is iteratively...
developed and refined using constant comparison during the conduct of the data collection. After careful analysis, the model is abstracted to the level of a substantive theory on information security strategy.

3.4 Adopted Research Approach

Social science differs from natural science which has long been the bastion of scientific research. Where natural science lends itself, for example, to the discovery of physical laws through controlled experiments, social science focusses on developing theory within a humanistic social context, without the benefit of highly controlled environments. These two philosophical approaches have been at odds for centuries amongst the academic community and the following section provides an overview of how these approaches affect this study on information security strategy.

3.4.1 Aligning the Research Framework

Research design refers to the process of compatibly aligning the philosophical elements such as approach, ontology, epistemology, methodology, and then identifying the timeframe that the research should be completed within, along with an appropriate method (Gray, 2013).

After identifying the ontological reality of the topic, alignment of the research framework continues with the appropriate identification of an epistemology, based on whether the research topic can be objectified and measured or not (Gray, 2013). This then increases the relevancy of a philosophical stance, although it is important to note that elements of multiple epistemologies and philosophical stances can overlap (Creswell, 2003). Methodologies are selected based on their broad tendency to align with particular philosophical stances but this alignment should not be interpreted as a concrete relationship (Creswell, 2003; Gray, 2013).
There are two types of timeframes, shorter and longer, and these correspond to two study types which are cross-sectional and longitudinal respectively (Yin, 2011). A cross-sectional study takes a snapshot of the research topic by collecting data at one point in time, typically using a survey methodology (Gray, 2013). A longitudinal study allows collection of data at multiple points in time and so can measure changes in variables (Yin, 2011).

The purpose of the research also plays a part in the selection of a research framework. There are four types of purpose which are named exploratory, descriptive, explanatory and interpretive (Gray, 2013). Exploratory research begins with nothing and explores a topic related to a problem. This exploration can involve conducting a literature review and interviewing expert practitioners before a decision is made evaluating the significance of the study and viability of an interesting outcome (Gray, 2013). Exploratory studies are purely inductive in nature without a guiding hypothesis or research question and are not appropriate for PhD research (Perry & Coote, 1994; Phillips & Pugh, 1987).

Descriptive studies describe a phenomenon or event and attempt to convey what happened, compare subjects against referent standards, or express the relationships between subjects (Gray, 2013). One of the weaknesses of descriptive studies is that they do not delve into why an event has occurred (Gray, 2013). Explanatory studies go one step further and do ask ‘why’ and ‘how’ questions (Gray, 2013). Explanatory studies explore and attempt to uncover correlation and causality (Gray, 2013). Interpretive studies conduct inductive analysis to explore and interpret perceived social reality from subjects (Gray, 2013). Interpretive studies typically employ qualitative methods to collect and analyse data (Gray, 2013).
3.4.2 Information Systems Discipline

There are many definitions of what information systems is and one holds that it is both a science and a profession (Lee & Baskerville, 2003). Another definition purports that information systems is divorced from information technology and is purely a social information system based on human interaction (Shanks, Arnott, & Rouse, 1993). One paper that reviews 22 different definitions of information systems concludes by proposing a definition that information systems focuses on individual and organisational use of information technology for the purposes of conducting work (Alter, 2008). Another definition is that information systems is not just information technology, nor simply the people who use technology, but rather it is what emerges from people using technology and any associated processes and norms that arise (Paul, 2007). This last definition is used by this thesis because technology, information, and processes arose as important concepts related to the topic during the literature review in the previous chapter.

Information systems has its own set of assumptions about relevant topics and appropriate research methods that differ to other reference disciplines such as engineering or mathematics, which researchers need to remain conscious of (Tarafdar & Davison, 2017). The objective of information systems is predominantly practice-oriented and seeks to improve the activities of IT practitioners (Zmud et al., 2001). Applied research examines existing knowledge and practices to look for ways to improve them, using objective and systematic approaches (Shanks et al., 1993). This social science orientation has implications for the design of research in information systems.

3.4.3 Philosophical Orientation

Options for the various elements of the research framework can now be assessed against the research question and the most appropriate methodology can be
selected. The purpose of research is to develop reliable and valid new knowledge in the theoretical and practical understanding of information security strategy. This section describes information security strategy in relation to philosophy and the research design used in this study. An appropriate research design is an essential step in establishing reliable and valid new knowledge.

Research overall is a complex combination of novel and established processes (Evans et al., 2011). These processes and research techniques link to abstract issues in philosophy (Neuman, 2014). The abstract philosophical issues involve what moral pressures affect research, what the ethical boundaries might be, why research is conducted and how I know whether a good research outcome has been achieved (Neuman, 2014). Philosophers have developed broad research traditions or approaches which are based on differing ontological and epistemological assumptions and principles (Neuman, 2014). These assumptions need to be understood by the researcher in order to guide the decisions made about an appropriate methodology and method (Neuman, 2014). The very nature of the existence of information security strategy must be considered to uncover the most appropriate methodology and methods to investigate it.

3.4.3.1 Philosophical Reasoning

At some stage of the research process, the researcher must identify a research approach and the decision about when this adoption occurs determines whether the research follows deductive or inductive logical reasoning (Gray, 2013). If the researcher begins with a proposed model and then conducts research to prove it or otherwise, then the approach can be said to be deductive (Yin, 2011). The deductive approach tests a hypothesis, and the principle is then confirmed, refuted or revised (Yin, 2011). In deductive studies, it is common for the conceptual elements that form the proposed model to be operationalised with specific measurements to assist with
observing whether the hypothesis has been falsified or not (Gray, 2013). It is worth acknowledging that perhaps no IS research is purely deductive and that there are differing views on what defines a deductive study (Lee & Baskerville, 2003, 2012; Tsang & Williams, 2012; Williams & Tsang, 2015).

If the researcher begins by collecting fragmented data and then collating and analysing it to build a proposed model, then the approach can be said to be inductive (Corbin & Strauss, 2008). This approach means the final model can be said to have been ‘discovered’ from common themes emerging from the data (Strauss & Corbin, 1990). The research is not completely directionless, as the topic was chosen in the beginning which then guides the data collection process; however it does not set out to prove or disprove a theory (Gray, 2013). Deductive and inductive processes are compatible however and can be used in the same research project at different stages (Gray, 2013). There are various perspectives on what defines induction and generalisation (Lee & Baskerville, 2003, 2012; Tsang & Williams, 2012; Williams & Tsang, 2015).

This research follows an inductive approach. The reason for this is the lack of existing theory on information security strategy that could be used to guide research attempts or build upon. Extant guidance on the nature of the topic was not universally agreed, so an inductive approach was most appropriate. In this research, a literature review is conducted, a research question posed, data is then collected and the results examined and analysed, and a model is proposed from the results – steps that are all consistent with an inductive approach (Gray, 2013).

### 3.4.3.2 Ontology

Ontology has been defined as “an area of philosophy that deals with the nature of being, or what exists” (Neuman, 2014, pp. 94). It is the study of being, what exists and whether it forms part of reality (Gray, 2013). The many beliefs that have been
developed through the centuries on ontology are beyond the scope of this thesis to list, however most philosophers ascribe reality to one of two main ontological positions, which can be termed realist and nominalist (Neuman, 2014). Realist philosophers believe that the world contains objects that simply exist, which can be empirically studied, independent of human interpretations of the data or results (Crotty, 1998; Neuman, 2014). These objects are visibly formed with identifiable attributes that can be assigned symbols or names (Gray, 2013). Nominalist philosophers believe that all data are viewed from the eyes of human researchers, who bias the data by subconsciously applying their own tacit values, preconceptions and cultural beliefs (Neuman, 2014). The data emerges in a changing world to form meaning that can be formless, chaotic and even absent (Gray, 2013).

From the literature review in Section 2.2.1 Information Security Strategy: Plan or Process?, consensus was that the form of information security strategy was contentious, as some scholars thought that it was a static plan and others thought it was a dynamic process. There was disagreement about whether information security strategy sits at the group, organisational or inter-organisational level. There were three ways of measuring it uncovered in the literature, which measured its risk management, goal achievement and quality, however none of these measures the entire information security strategy construct but rather some singular aspect of it.

This inability to grapple with the nature of the form of information security strategy gives us clues as to its reality. Does information security strategy exist independently of consciousness, the same as a tree? The answer would have to be no, as information is constructed through conscious efforts, information’s security is considered and appropriately managed in relation to threats, and strategy is formulated through the conscious deliberations of organisational leaders.
Nominalist ontology assumes that any external reality is always being interpreted by humans based on their previous experiences and biases (Neuman, 2014). These subjective cultural beliefs cause the object to be viewed through a lens that colours the subject’s perception of the topic (Neuman, 2014). Information security strategy is often documented, the contents of which are organised into categories and patterns sub-consciously by the organisational author. Once information security strategy documents have been written, then an information security strategy for that organisation now exists in corporeal form. These factors are consistent with this researcher adopting a nominalist ontological position.

3.4.3.3 Epistemology

Epistemology has been defined as “an area of philosophy concerned with the creation of knowledge” (Neuman, 2014, pp. 95). It focusses on how the knowledge is created and what are the most appropriate ways to make it truthful (Neuman, 2014). There are a number of branches of epistemology such as objectivism, constructivism, subjectivism, and empiricism (Crotty, 1998; Gray, 2013; Neuman, 2014).

Objectivist epistemology is based on a realist ontology and dictates that meaning exists independently of human consciousness, validated by perception; that objects and their meaning can exist without humans even being aware of them (Crotty, 1998; Gray, 2013). Perception using the senses is the only truthful form of validation of reality, therefore the only way to build knowledge (Crotty, 1998). Objectivism relies on the senses to perceive objects and validate them to construct reality and build knowledge; however, prior to an information security strategy document being written, it did not exist. If no object exists, then the senses cannot perceive it. Therefore, objectivism is incompatible with this body of research.

Empiricism is where empirical research based on developing evidence allows the discovery of truthful ideas (Neuman, 2014). Aggregating and organising these truthful
ideas allows the discovery of laws or principles that are based on reality (Neuman, 2014). This research can either work deductively by testing ideas about reality against the empirical evidence or inductively by aggregating the empirical evidence to allow the discovery of generalised laws (Neuman, 2014). Empiricism relies on developing empirical evidence to allow the discovery of truthful ideas however without a means to measure information security strategy, then empirical evidence cannot be collected. Empiricism is therefore inconsistent with this research.

Subjectivism is where meaning is not derived from the interaction of the subject with the object (like in constructivism) but rather where subject assigns meaning to the object (Crotty, 1998; Gray, 2013). The object offers no contribution to the subject when meaning is derived or imposed but rather the subject constructs meaning from their values and beliefs (Crotty, 1998; Gray, 2013). Subjectivism dictates that meaning is assigned to the object and the object makes no contribution towards the generation of meaning (Crotty, 1998). However, once an information security strategy has been documented, then it exists and does have meaning. The document-object contributes towards the generation of meaning of information security strategy. For this reason, subjectivism is not consistent with this research.

Constructivism is where social reality is created from a subject’s interaction with the world (Gray, 2013). Since research subjects are interpreting their thoughts and actions when interacting with the researcher who is also interpreting, the researcher cannot then generalise to make claims that are true for all people in all situations, and results might be difficult to reproduce (Crotty, 1998; Neuman, 2014). The researcher can only make generalised findings about specific individuals in specific situations through an inductive process of aggregating their observed actions and experiences (Neuman, 2014).
If an information security strategy is written and therefore materially exists, then this has been constructed whilst being written. Whether this constructed reality is purely a product of the subjective knowledge and values of the organisational authors, or whether it arises through some form of interaction with the security aspects of organisational information will be explored in this research.

Constructivism contends that meaning is not discovered as per objectivism but rather constructed based on a subject’s interaction with the world (Corbin & Strauss, 2008; Gray, 2013). That is, meaning exists as a result of the partnership between subject and object, which differs based on culture and era (Crotty, 1998). Meaning in the world is not created; it is constructed subjectively using the world and pre-existing objects in the world. In terms of information security strategy, the building blocks are organisations and the information assets they own, the organisational environment and all its accompanying threats, and the controls organisational staff can apply to counter threats. These objects can be examined and combined to construct a meaningful information security strategy, one that is meaningful to that specific organisation. A constructivist epistemology is consistent with research into information security strategy.

### 3.4.4 Philosophical Stance

A philosophical stance (sometimes termed *theoretical perspective or research approach*) relates the epistemology chosen by the researcher, with the methodologies and methods that are used to conduct the research (Crotty, 1998). It explicitly states the assumptions that guide the choice of a methodology (Crotty, 1998). The stances include positivism, interpretivism, critical inquiry, feminism and postmodernism, amongst others (Crotty, 1998; Gray, 2013; Neuman, 2014). There are three main stances common for studies in social science, which are positivist, interpretivist and critical, with the first two being most popular and influential (Gray,
2013; Neuman, 2014). Other less-common stances in information systems include social constructivism, advocacy and pragmatism (Creswell, 1998; Neuman, 2014; Shanks et al., 1993). The broad range of definitions and understandings about the nature of information systems has resulted in debate about the most appropriate philosophical stance to develop knowledge about it (Shanks et al., 1993).

Organisational research is paradigmatically oriented and Burrell and Morgan (1979) have suggested four main paradigms to anchor research, namely (1) radical humanist, (2) radical structuralist, (3) interpretivist, and (4) functionalist (see Figure 3.2). Choice of a paradigm guides the philosophical stances adopted in the research (Gioia & Pitre, 1990). Given the nature of information security is more oriented towards uniform regulation than towards radical changes, radical humanist and radical structuralist can be ruled out for the purposes of this research.

![Figure 3.2. Sociological Paradigms (Burrell and Morgan 1979)](image-url)
The functionalist paradigm is typically characterised as an objectivist view of the world, taking a deductive approach to selecting existing variables and hypothesising about a causal effect from their relationship, tested using statistical measures (Burrell & Morgan, 1979; Gioia & Pitre, 1990). Given existing variables in information security strategy from the literature are scarce, and the topic information security strategy seems to have a strong social reality to it, then the functionalist paradigm seems inappropriate. The interpretivist paradigm however seeks to discover explanations that diagnose problems and understand a phenomenon under investigation, which is the intended direction for this research (Burrell & Morgan, 1979; Gioia & Pitre, 1990). Selection of a paradigm allows the appropriate recognition of assumptions that support theory developed within it, such as the interpretivist assumption that human agency is central to the construction of rules for structuring activities (Gioia & Pitre, 1990).

### 3.4.4.1 Common Philosophical Stances in Information Systems

The positivist stance has been around the longest and appears in the majority of relevant published papers (Neuman, 2014; Shanks et al., 1993). Positivism holds that meaning exists externally to the researcher and can be factually measured by what is observable about it to the researcher (Gray, 2013; Neuman, 2014). Positivist researchers aim to produce results that are seen as objective facts (Gray, 2013). Criticisms of positivism include that theory can also be developed based on what is non-observable, for example astronomical black holes (Gray, 2013). Researchers have also disputed the claim that objective facts are produced from positivist research because theories cannot be proven, they can only be disproven (think of the famous case of the black swan) (Gray, 2013). There are variations of views about what positivism is and what many IS scholars assign to (say) “positivism” may not be “positivistic” in the light of the philosophers who constituted, for example, logical
positivism, which was a variation of positivism that argued that only claims verifiable through direct observation or logical proof are meaningful (Siponen & Tsouhou, 2018).

Critical social science is a system of research inquiry that questions whether unknown social structures, values and assumptions are having undue influence on the research results (Crotty, 1998). The main premise is that powerful social entities have an oppressive influence on other social groups and cause outcomes to be skewed in their favour (Gray, 2013). Critical inquiry investigates values and assumptions to challenge social structures and power relations that unjustly oppress groups. Given that the aim of information security strategy is to protect organisational information, the aim of critical inquiry does not seem relevant. Positivism dictates that meaningful social reality exists externally to the researcher and that observing it is the only way to measure it (Gray, 2013). Observing information security strategy presents somewhat of a problem, if for example information cannot be seen when it resides on a solid-state Network Attached Storage device.

Feminism is similar to critical inquiry in that proponents believe social oppression causes a power imbalance which distorts knowledge distribution and social reality, however the difference is that the oppression applies only to women (Crotty, 1998). This affects the choice of research approach and methods because in particular, positivist and objective approaches to research are seen as male-oriented, prioritising male assumptions and values (Gray, 2013). In contrast, ethnography is seen as compatible with feminism because the female researcher can make explicit her assumptions and values when interacting with the object (Gray, 2013). Given that there has been no indication in the academic literature that information security strategy is affected by gender, then a feminist approach will not be taken in this research.
Postmodernism arose through a rejection of positivism and the objective focus on a singular explanation of social reality (Crotty, 1998). Instead, postmodernism constructs meaning from multiple fragmented realities, each of which is embedded with its own ambiguous meaning and values (Gray, 2013). The literature on information security strategy does not appear to be based on the postmodern values of nihilism or anarchism, so a postmodern approach will not be taken (Neuman, 2014).

Interpretivism is a perspective that there is no single, unique relationship between the object and subject (Crotty, 1998). The relationship is formed as the subject cognitively interprets actions of individuals to form social reality (Gray, 2013). Interpretivism is aligned most closely with the constructivist epistemology (Creswell, 1998; Gray, 2013). Interpretivism has a number of varieties which include symbolic interactionism, hermeneutics, realism, naturalistic inquiry, constructionism, ethnomethodology, cognitive, idealist, phenomenology, subjectivist, and qualitative sociology (Crotty, 1998; Gray, 2013; Neuman, 2014).

Amongst the interpretivist approaches, symbolic interactionism is an approach to creating meaning where the subject interacts with the world to derive meaning about an object from the interaction (Gray, 2013). Thus, the meaning is developed from the subject’s perspective, which the researcher needs to take into account when deciding on an appropriate methodology, for example ethnography, and method such as participant observation (Gray, 2013). Phenomenology is an approach to understanding the culture of a research topic through the personal experience of a subject engaged within that social reality (Gray, 2013). Ethnography on the other hand is also focussed on the culture of social reality however the topic is viewed externally from the researcher’s perspective (Gray, 2013). Realism is an approach where social reality is taken to exist independently of the subject or researcher (Gray, 2013). Since culture and social reality are taken to exist naturally, they can be
studied using scientifically, whilst acknowledging the fallibilities of the subjective processes of the researcher biasing the results (Gray, 2013). Hermeneutics contends that social reality is too complex to be measured through scientific observation so the researcher must interpret first-hand to fully understand the topic (Gray, 2013). Naturalistic inquiry considers that there are multiple social realities that must be accounted for during the research process, the results of which are constructed to be generalisable only to phenomena in a similar context or environment (Gray, 2013).

3.4.4.2 Adopted Philosophical Stance

There are a few philosophical stances commonly used in information systems, namely positivism, interpretivism, and critical inquiry (Gray, 2013). Of these, interpretivism is most closely associated with constructivist epistemology plus nominalist ontology and asserts that reality occurring in the natural world is different to reality occurring in the social world, requiring different methods to assess them (Gray, 2013; McFadzean et al., 2006). These methods need to be unique, individual and qualitative to account for the subjective lenses through which the object is viewed by the researcher. This seems consistent with information security strategy because only information security practitioners working within an organisation would have a full understanding of the pressures that are applied to that organisation’s information from its environment and internal stakeholders. The practitioners have developed tacit perspectives from previous security-related experiences, organisational values, and organisational culture. An interpretivist research approach is therefore consistent with this research.

Risk is measured by practitioners interpreting perceived threats to information and balancing these threats with what they perceive is an adequate level of security controls, therefore interpretive research is required. Some advantages of research conducted in the interpretivist paradigm include combining the technical aspects of
security research with a study of motivations and decision-making for the security of an organisation (Backhouse & Dhillon, 1996). Interpretivist research also allows researchers to study security as viewed by the subject from their perspective (Strauss & Corbin, 1990).

3.4.5 Phenomenology and Grounded Theory Methodologies

A methodology is a plan of action that informs the choice of method in practice, which links back to the desired research outcome (Crotty, 1998; Gray, 2013). The methodology offers a rationale for the choice of method and how it is employed (Crotty, 1998). The choice of methodology depends on whether the researcher considers that the truth exists independently in the world or whether the truth is uncovered by interpreting research subject’s perspectives on the topic (Gray, 2013). Other factors to consider are whether the researcher adopts a deductive or inductive approach to the research (Gray, 2013).

3.4.5.1 Common Methodologies in Information Systems

Common methodologies in information systems include experimental research, analytical surveys, ethnography, phenomenological research, grounded theory, heuristic inquiry, action research, case study, discourse analysis and feminist standpoint research (Crotty, 1998; Gray, 2013). The following is a description of some of these with an explanation of their strengths and weaknesses.

Experimental research allows the researcher to quantitatively hypothesise about the causal relationship between an independent variable and a dependant variable, while controlling the environment and manipulating the independent variable to eliminate alternative explanations (Gray, 2013). A weakness of the experimental approach is that it is resource-intensive, difficult to obtain comparable experimental and control groups, organisational support is difficult to obtain, and also alternative explanations are difficult if not impossible to eliminate (Gray, 2013; Shanks et al., 1993).
Phenomenological studies examine meaning about a topic as expressed in the lived experiences and interactions with the topic by the research subjects (Shanks et al., 1993). This meaning or interpretation is inductively examined by iteratively identifying phrases related to the topic, transforming them into theoretical themes, before reintegrating the themes into a general description of the topic (Gray, 2013). The strength of phenomenological studies is the multidimensional comprehension of the research topic and the weaknesses are the subjectivity of the results, lack of data reliability, low generalisability of results, and the exposure to alternative explanations (Gray, 2013; Shanks et al., 1993).

Analytical surveys test a theory by investigating the association between concepts and variables (Gray, 2013). They collect data from a smaller cohort of a population and then typically generalise the analysis results as representative of the population (Shanks et al., 1993). The data are either qualitative or quantitative in nature and gathered via interviews or questionnaires. Surveys are then analysed and qualitative data are often coded to allow quantitative techniques to be used (Gray, 2013). Given the use of interview questions or questionnaires, a weakness of this method is researcher bias affecting the questions when being written. A strength of this method is the availability of powerful analytical techniques to analyse the data such as regression and factor analysis (Shanks et al., 1993).

Action research is where the researcher actively engages with the organisation which results in a study that is emergent, responsive, action-oriented, participative and critically reflective (Shanks et al., 1993). The strength of action research is the practical nature of the research results and can use structured quantitative or unstructured qualitative methods (often a case study), following an inductive or deductive approach (Gray, 2013). The weaknesses are that the subject data results are typically highly subjective, the researcher biases the study indelibly, and alternative explanations cannot be excluded (Shanks et al., 1993).
Heuristic inquiry is a process where the researcher poses a research question based on an identified personal problem and then employs active methods to assimilate and participate in the problem area, with the intention of inductively uncovering insights (Gray, 2013). It is a reflexive exercise reliant on self-awareness that commences phenomenologically and becomes deeply subjective, therefore excluding generalisability (Gray, 2013).

Case studies typically collect data on a research topic from a sample organisation or group of organisations (Yin, 2013). Case studies are exploratory in nature to uncover new concepts or descriptive in nature to confirm the existence of a previously discovered concept. The strength of case studies is that they allow for insightful, multidimensional data to be collected. The weaknesses are generalising the results of a study into a small number of organisations across all organisations in the population and secondly, researcher bias subjectively affecting what data are collected (Shanks et al., 1993). Case studies have confusingly been called a method instead of a methodology (Crotty, 1998; Gray, 2013; Shanks et al., 1993).

Grounded theory accepts that the normal manifestation of social reality in practical situations is best analysed by developing grounded conceptualisations (Strauss & Corbin, 1990; Yin, 2011). Grounded theory usually begins with an open-minded collection of data from social contexts representing reality and then codification of the data to categorise emergent themes that can then be said to be ‘grounded’ in reality (Gioia et al., 2013; Strauss & Corbin, 1990; Yin, 2011).

Aside from these common methodologies, there are other methodologies that are also appropriate to research in information systems. One such methodology is simulation, which is applicable when the researcher knows the two variables under investigation but is unsure of how the two will interact with each other. By developing a model of the two variables and changing them in a simulated environment, the
researcher can study their interaction. The downside is whether the model precisely represents the real world environment (Shanks et al., 1993).

Conceptual studies elicit data from research subjects that are entirely subjective in nature (Shanks et al., 1993). Conceptual studies avoid empirical data and allow subjects to interpret their observations when presenting speculative data. The strengths are that it allows for critical thinking and creative new ideas. The weaknesses are that researcher bias could distort the research subject questions and evaluation of the responses (Shanks et al., 1993).

### 3.4.5.2 Selected Methodologies for This Research

In this research, a combination of methodologies is used, which include a phenomenological approach to the type of data collected and a grounded theory approach to data collection and analysis. Grounded theory is flexible and can be combined with other methodologies (Urquhart & Fernandez, 2013). The phenomenology methodology puts the focus on understanding the lived experiences of the research participants and the grounded theory aspects guide the techniques for data collection, analysis, and presentation. This section will describe phenomenology, then grounded theory, in more detail then finish with a detailed description of data collection and analysis procedures.

Interpretive social science, often called qualitative research, has a variety called phenomenology, which was founded by Edmund Husserl (Husserl, 1931; Neuman, 2014; VanScoy & Evenstad, 2015). Although there are many variations of phenomenology, such as transcendental, dialogical, empirical, existential, and social, there are two main branches, descriptive and interpretive (Creswell, 1998; VanScoy & Evenstad, 2015). Descriptive phenomenological philosophy uses the lived experience to represent worldly objects in the consciousness of the mind, creating awareness of these objects (Polkinghorne, 1989). This awareness comes as a result
of the person-world relationship and is created through experience (Polkinghorne, 1989). Examining the lived experience of research subjects therefore forms the basis for understanding meaning about a research topic in a phenomenological study (Polkinghorne, 1989). It is essential to separate particular occurrences of a topic under investigation and the meaning behind them, which is why phenomenological studies look to capture multiple lived experiences where the subject perceived an object as reality and then search for structured meaning within the common essence (Polkinghorne, 1989). There is a certain intentionality in experiencing an object derived from consciousness of the object, which is different to mechanical causation (Polkinghorne, 1989). Phenomenological research is descriptive and qualitative research, as it examines the human aspects of reality to understand structures and meaning (Giorgi, 1975; Polkinghorne, 1989).

The other main branch of phenomenology is interpretive, sometimes known as hermeneutical phenomenology (VanScoy & Evenstad, 2015). While descriptive phenomenology seeks to uncover a general description of the experience, hermeneutical phenomenology seeks to understand the interpreted structures of experience (VanScoy & Evenstad, 2015). Hermeneutical phenomenology is an approach to understanding meaning about a phenomenon by examining related objects such as pictures, text, and notes in their entirety, breaking them into parts to understand meaning segments, then recombining the parts into one profound, deep understanding of the phenomenon under investigation (Neuman, 2014). Researchers may not gather data solely from people, for example by asking about lived experiences in an interview, but also gather data by interpreting the meaning of objects, for example reading the text in a document and reflecting on what the intent from the original author was (VanScoy & Evenstad, 2015).

The major strength of phenomenology is the richness of understanding that is derived about the phenomenon identified as information security strategy.
Phenomenology searches for understanding rather than causation (Polkinghorne, 1989). It explicitly makes clear the suppositions and assumptions of both the research subject and the researcher, which is important for a topic that is not well-defined such as information security strategy (Shanks et al., 1993). The weaknesses are the subjectivity of the interpretations of the data, unreliable data from research participants, and an incapability to exclude confounding explanations (Shanks et al., 1993). As this research is primarily theory-building, the weaknesses were deemed tolerable as it is hoped that in future other researchers might take an interest in information security strategy and continue to develop knowledge further in a more positivistic fashion based on the contributions that this thesis offers.

Phenomenological studies typically use the same data collection procedures as non-phenomenological studies, such as interviewing a variety of key research participants, making observations, and jotting down field notes (Yin, 2011). The data analysis procedures of a phenomenological study are also likely to be similar to those used by a non-phenomenological study, such as interpreting significant words and conducting a thematic analysis (Yin, 2011). The main point with phenomenological studies is that they are qualitative research studies that study human experiences with phenomena of interest in the real world and they resist the use of previously identified concepts or labels that might distort the researcher’s perceptions of the subject’s view (Polkinghorne, 1989).

There are five major procedural areas that warrant the attention of a researcher intending to conduct a phenomenological study and these five areas are all considered during this program of research (Creswell, 1998):

1. The idea of epoche is central to any study in phenomenology, where the intent of the research is to understand the phenomenon under investigation from the perspective of the research subject, requiring the researcher to bracket their
preconceived ideas and notions about the topic away from the study. This is to ensure that, as much as possible, the researcher truly gets a picture of the topic from the subject’s perspective without the researcher’s biases distorting the data (Moustakas, 1994).

2. The researcher writes questions for the study that explore the lived experiences of the subject.

3. The researcher collects data from participants who have actually experienced the phenomenon under investigation. These data are typically collected via long interviews with additional field notes made by the researcher during the conduct of the interview. The typical number of interview participants ranges from five to 25 (Creswell, 1998; Mruk, 1983; Polkinghorne, 1989).

4. The data analysis procedures in a phenomenological study are generally the same across methods. The steps are to disassemble the data, group the data into clusters of meaning, then reassembled to create a general representation of the experience (Creswell, 1998; Moustakas, 1994; Polkinghorne, 1989).

5. The study ends with the reader of the report understanding the single, unifying construct that unites the experiences from all the subjects (Creswell, 1998).

Grounded theory is an approach to theory development that dictates there should be strong interaction between data and theory, to support a claim that a proposed theory is built and grounded on the data (Urquhart, Lehmann, & Myers, 2010). It was originally developed by Glaser and Strauss (1967) to move social research away from the functionalist paradigm and more towards the interpretivist paradigm (Burrell & Morgan, 1979; Urquhart et al., 2010). It was famously developed further by Strauss and Corbin (1990) and Charmaz (2008), adopted widely, to the point where grounded theory was once labelled a common feature of qualitative studies (Miles & Huberman, 1994). As a result, grounded theory enjoys strong adoption in many sociological fields including information systems (Urquhart & Fernandez, 2013).
The phenomenological methodology places a focus on collecting detailed descriptions of the lived experiences of research subjects to understand the essence of information security strategy. The reason phenomenology has been used is because, from the literature review in Chapter 2, an information security strategy is created from the conscious efforts of employees, so must be understood by studying the same people who created it.

The reason that grounded theory has been selected as a methodology for this thesis is that, to answer the research question, the lack of existing theory on information security strategy meant that theory building was required using cogent analysis. Senior scholars in information systems have suggested that GTM is appropriate for understanding the insider’s view of information security (Crossler et al., 2013). A recent review of GTM in information systems discipline shows that of all the articles in information systems that are theoretical papers adopting GTM, there are ten articles that have specifically developed a theory in information systems (not a theoretical model or theoretical rich description) (Wiesche et al., 2017). Of these ten theory articles, nine used the “Anselm Strauss” variant of GTM with only one using a “Barney Glaser” variant (Wiesche et al., 2017). Accordingly in this research, I also adopt a Straussian approach to GTM use, specifically the approach, techniques and procedures prescribed in Corbin and Strauss (2008). The Straussian approach also allows for a literature review to be conducted before data is collected (see Chapter 2 of this thesis) and the researcher’s personal plus professional experience to be considered, which is practical for doctoral researchers (Strauss & Corbin, 1994; Thornberg, 2012). The reason for this is that “familiarity with relevant literature can enhance sensitivity to subtle nuances in data” (Corbin & Strauss, 2008, pp. 37).

Combining aspects of these two methodologies is consistent with published literature on interpretive research, as evidenced by the masterful exploration of computer mediated-discussion by Trauth and Jessup (2000), which used hermeneutic
phenomenology criteria and grounded theory techniques to evaluate the data to set a precedent.

An explanation is required on the writing of a literature review (Chapter 2: Research Background in this thesis) before the collection and analysis of research data (Chapter 4: Findings in this thesis) if the selected methodology for this research is grounded theory, where scholarly dictum would prescribe delaying the review until after data analysis to avoid biasing the researcher (Glaser & Strauss, 1967). This delaying approach was not taken in this research because (a) a literature review was required to be completed prior to ethics review by the researcher’s institutional board, (b) preconceptions in the researcher were inevitable due to an extensive professional career in information security, and (c) a cumulative research tradition resulting in incremental advancements in knowledge can only be achieved with a full understanding of extant knowledge, and all of these reasons are perfectly reasonable (Thornberg, 2012). Countering preconceptions in the researcher and bracketing biases can be effectively performed through the careful adherence to the prescriptive procedures espoused by the GTM (Charmaz, 2008; Thornberg, 2012).

3.4.6 Methods

A method is a technique or procedure that can be used to gather research data and analyse it against a research hypothesis (Crotty, 1998). Methods commonly used in social science include:

“sampling, measurement and scaling, questionnaire, non/participant observation, interview, focus group, case study, life history, narrative, visual ethnographic methods, statistical analysis, data reduction, theme identification, comparative analysis, cognitive mapping, interpretative methods, document analysis, content analysis, and conversation analysis” (Crotty, 1998, pp. 5).
The distinction between qualitative or quantitative research and the decision about which to use is made at the methods level, not at the epistemological or philosophical stance level (Crotty, 1998). Researchers should accept that whatever epistemology or methodology is chosen, any method or combination of methods, whether qualitative or quantitative in nature, can be chosen to achieve the research outcome (Crotty, 1998). Methods are grouped as qualitative or quantitative and this fluidity of choice only applies to the methods chosen, not to the choice of epistemology or research approach which do need to be consistent (Crotty, 1998).

Methods can also be mixed instead of simply aligning with one research epistemology and methodology (Gray, 2013). Reasons for this include the fact that the researcher may need to respond to multiple research questions in the study, data may need to be collected from multiple sources which are different in form, and to allow the strength of one method to cover the weakness of another so that the study overall is stronger (Gray, 2013). This last combination of methods, which is used to check and establish internal validity in studies by analysing a research question from multiple perspectives to arrive at consistency across data sources or approaches, creates a research outcome that is more rich, robust, comprehensive and well-developed and is called triangulation (Gray, 2013).

There are four main types of data collection activities, which are (1) interviewing, (2) observing, (3) collecting and examining, and (4) feelings (Yin, 2011). Of these, there are three main methods used to collect the data in this research program, which are interviewing, observing, and collecting and examining the contents of documents. The researcher learns a lot about the topic under investigation in the process of collecting the data, and can allow these experiences to shape the structures that develop during data analysis (Polkinghorne, 1989). For this reason, it is essential that only the researcher who participates in the data collection analyses the data and so,
in this study, interrater reliability using the assistance of other researchers to increase validity through triangulation will not be attempted (Polkinghorne, 1989).

### 3.4.6.1 Research Method Constraints

Before the data collection methods are described, a brief note on the expected difficulty with collecting security data from organisations where I am not a trusted employee. Data collection from organisations in information security research is more difficult than in other disciplines because it is intrusive and there is a general mistrust of any outsider who attempts to probe within organisations on security-related matters (Kotulic & Clark, 2004). It is also problematic to get organisations to adopt the completed research into their practice (Siponen & Baskerville, 2018). Previous research has shown that it is almost impossible to collect data about an organisation’s information security by mailing surveys or questionnaires (Kotulic & Clark, 2004). A slow, cautious style is advised for research programs in insufficiently researched fields, for example organisational-level information security, or which are on a sensitive topic (Kotulic & Clark, 2004). Based on this advice, I anticipate difficulty with recruiting a large number of subjects, such as could be used for a survey or questionnaire.

### 3.4.6.2 Interviewing Individual Participants

The primary method selected is interviews, long enough to investigate the topic in depth, to last 30-60 minutes but sometimes to last up to a few hours, which are to be audio-recorded and transcribed (Polkinghorne, 1989). The ideal target for the total number of research participants is 25 (Creswell, 1998; Mruk, 1983; Polkinghorne, 1989). The focus of the interview is on the lived experience of the subject with themes in the research topic, not focused on the person themselves (Polkinghorne, 1989). The qualitative aspects of the interview seek to elicit the subtly-nuanced aspects of any description the subjects impart in their sentences, not what the
subject reflects should have happened or what they thought was theoretically possible (Polkinghorne, 1989). The best way for me as the researcher to avoid prematurely categorising answer data into theories and asking follow-up questions that are misguided is to directly ask the subject for real examples of what they experienced (Polkinghorne, 1989).

Interviews take the form of either structured interviews or qualitative interviews. Structured interviews are often precisely scripted through the use of pre-planned questionnaires, which are uniformly administered across a representative sample of participants (Yin, 2011). To achieve this uniformity, the interviews often involve surveys comprised of closed-ended questions (i.e. limited set of responses), to allow for comparison between answers. Qualitative interviews differ in that they are loosely structured based on the overall research direction set by the researcher (Yin, 2011). The interview questions are open-ended to allow for variability in the respondent’s answers and follow-up questions may be interjected by the researcher (Yin, 2011). Structured interviews can therefore be said to seek meaning from the researcher’s view of a topic whereas qualitative interviews seek to understand a research topic from the participant’s perspective (Yin, 2011).

Understanding the views of key organisational decision-makers is desirable but the difficulty lies in engaging with directors and executives on the topic of information security, as research shows that this is difficult to achieve (Kotulic & Clark, 2004). Given executives are time-poor and likely to ignore questionnaires, the most productive method to engage with subjects and maintain their attention is interviews.

With the five major procedural tenets of a phenomenology methodological study from the previous section in mind, an interview protocol was developed and can be viewed in Appendix D: Interview Protocol. In accordance with this advice, the protocol includes questions that probe the subject’s understanding of the topic, written in a
neutral language that, as much as possible, reduces the researcher’s biases affecting the data. There are also questions that ask the subject for examples of aspects of the phenomenon as experienced in their everyday working life. The sample of research subjects were carefully selected to include people who purport to be accountable or responsible for information security across the entire organisation, placing them at the strategic level and ensuring they have some real-life experience with the topic. They were asked about this when signing the participation consent form as they were required to agree with the following sentence: “I have some experience of participating in the information security strategy-setting process.”

To develop and refine phenomenological interview questions, the method that will be used is to follow a procedure where the first step is for me as the researcher to reflect on the topic and then brainstorm a list of questions that are on-topic and thorough (Colaizzi, 1978; Gioia et al., 2013). The second step is to conduct a few pilot interviews and modify the questions after each interview based on dimensions that were omitted from the initial list or discovered during interviews (Colaizzi, 1978; Gioia et al., 2013). This may sometimes lead to the rewording of the research question, which is a normal and expected step in qualitative research as it progresses (Gioia et al., 2013).

The data analysis steps include disassembling the data, grouping the data into clusters of meaning, then reassembling to create a general representation of the experience, as described more fully in the following section about data sources. This thesis ends with a rich explanation of the detailed understanding of information security strategy as created during the conduct of this research program.

3.4.6.3 Observing During Interviews

Observing is a valuable method of data collection because the researcher can sense and perceive the subject and topic with their own eyes, unfiltered by the subject’s
perceptions (Yin, 2011). This observing technique allows the researcher to apply their own reflections of the interview to the topic, which, depending on the level of experience of the researcher, is just as valid as the data collected from research subjects (Yin, 2011). Clearly this form of primary data is highly subjective, which should be noted, however acting as a participant-observer can be invaluable. The researcher must be careful to compartmentalise preconceived notions about the topic under investigation however simply being aware of this requirement offers some level of protection (Polkinghorne, 1989). The research subject observing me as researcher recording notes during the conduct of an interview may increase their level of apprehension about what is being recorded, however this apprehension could also result from being informed that the interviews are audio-recorded. I contend that any potential apprehension could result in some level of acquiescence bias or halo effect and so note this potential effect on the data.

3.4.6.4 Collecting and Examining Documents

Collecting refers to the accumulation of a set of documents on the research topic, in this case information security strategy artefacts (Yin, 2011). Although these documents may be collected from a library or online sources, they are typically collected in the field and can include such abstract topics as an organisation’s policies and procedures (Yin, 2011). Reviewing the documents in a hermeneutic manner requires the researcher to attempt to understand both the author’s original intent and also their own perceptions while reading the documents (Polkinghorne, 1989). Advantages include that data from literary works often offer profoundly powerful descriptions and can be collected from a variety of geographical locations (Polkinghorne, 1989).

Unfortunately, due to the sensitive nature of the information security strategy documents of interest, disadvantages include that there is difficulty with gaining
permission to access them. The other difficulty with this method is the vast size of the documents, as some not only contain the organisation’s strategy, but it’s strategic plan for implementing the strategy, which can run over 100 pages. Therefore, collecting documents will not always be possible from every research subject and cumbersome to analyse, so is only a complimentary part of the data collection.

3.4.7 Data Sources

Phenomenological research seeks to gather data that describes the lived experiences of research subjects when interacting with the research topic (Polkinghorne, 1989). The researcher can then examine all these instances of subjects interacting with the research topic and tease out structures, based on what the subject consciously perceives them to be (Polkinghorne, 1989). It is important that the research subjects reflect on their own lived experiences when engaging with the research topic, not report the experiences of others as consciousness and consequent perceptions may be distorted (Polkinghorne, 1989). This places the onus on the researcher to construct questions for the interview that do not allow the subject to wander off-topic and give scholarly definitions or the experiences of others (Polkinghorne, 1989). There are three main sources of data that researchers can draw upon during collection, which are (1) self-reflections from personal experiences with interacting with the research topic, (2) the reflections from research subjects who have interacted with the research topic in the past, and (3) artefacts that embody some aspect of the research topic (Polkinghorne, 1989).

There are four main qualitative research activities that access sources from which to collect research data, which are (1) interviewing, (2) observing, (3) collecting and examining, and (4) feeling (Yin, 2011). Collecting data from multiple sources is encouraged in qualitative studies because this practice lends itself to triangulation of evidence, which strengthens the validity of the study (Gioia et al., 2013; Yin, 2011).
Triangulation of data occurs when multiple sources converge on the same conclusion about particular points in the research topic (Yin, 2011).

Data collection by sensing feelings was not used in this study. Feelings refers to the practice of the researcher reflexively examining their feelings during the course of the data collection to detect any resonant or discordant intuitions that may affect, for example, the researcher’s perceptions about the truth of an interviewee’s statements (Yin, 2011). This primary data needs to be triangulated but may provide insights into the research topic that are not available from other sources (Yin, 2011). Some of the interviews were conducted via recorded phone call so without face-to-face contact, sensing feelings was perceived as too unreliable.

The data analysis phase is the most important stage of an interpretive study because this is when the essential structures and the unifying relationships in the research topic are uncovered (Polkinghorne, 1989). Importantly, the subject’s experiences are not nebulous or nondescript, rather they are naïve and ordered, full of meaning. During data analysis, the researcher’s role is to bracket out preconceptions and reduce the meaningful descriptions down to the central essence, or *epoche* (Moustakas, 1994; Polkinghorne, 1989). Any implicit meanings within the descriptions become explicit in the form of a lived-structure.

The following is a description of the three data sources selected for this study and their method relationship; interview transcripts from conducting interviews, field notes from observing interviews, and documents for collection and examination. The next section includes an explanation of the strengths and weaknesses of each and an explanation of the data collection and analysis procedures for each type of data.

**3.4.7.1 Interview Transcripts**

Interview transcripts are written recordings of interviews that have taken place between the researcher and subjects. Interpretive studies typically use other people
as the primary data source of lived experiences with the research topic (Polkinghorne, 1989). The major benefit of this approach is the avoidance of using only my own reflections while developing an understanding of the topic, which would create a risk of “subjective bias” (Polkinghorne, 1989). Data in the form of transcripts from interviews with subjects is coupled with data in the form of self-reflections to provide a more complete picture (Polkinghorne, 1989).

3.4.7.2 Field Notes from Observations

Field notes are data collected by observing research subjects and passively forming impressions without having to rely on the reports or impressions of others (Polkinghorne, 1989; Yin, 2011). Although I could not observe all things at all times within an organisation, I could be selective about when and what I observed and so can take field notes during interviews to record my observations (Polkinghorne, 1989; Yin, 2011). Observing participants will to some extent affect the participant’s actions and their actions may influence my thoughts, all of which affects the data collected (Polkinghorne, 1989; Yin, 2011). The field notes are highly subjective based on my thoughts as the researcher, so are therefore complementary to interview transcripts as the primary form of data. I do not intend to use field notes to record the interviews verbatim but rather to record insights and thoughts I have during the interviews, based on the research subject’s answers. They are also used to identify any presuppositions or biases I hold after a period of reflexion post-interview (Polkinghorne, 1989). The benefit of this approach is to help me as researcher to bracket out the biases that I bring to the study and understand the phenomenon purely from the subject’s perspective (Polkinghorne, 1989).

3.4.7.3 Document Collection and Examination

Collecting and examining documents and artefacts from the field can be an invaluable source of data, particularly for abstract topics such as an organisation’s
security policies and procedures, which are captured in documents (Yin, 2011). Although costly to collect and examine in terms of time, the exercise will result in primary data (Yin, 2011). Combining the collection and examination of documents with interviews also serves to speed up the interview, as the researcher should not have to continually interrupt the subject to ask for clarification on names, titles and locations (Yin, 2011).

3.4.8 Data Collection Procedures

First and foremost, interviews are the most significant source of data for this study. A slow, interpersonal-style of data collection method was selected, which was semi-structured interviews with open-ended questions (Yin, 2011). The interviews are semi-structured in that a set of questions guide the format of the interview, however interesting answers are investigated further with unstructured follow-up questions. The interview questions are designed to allow me as researcher to speak in only modest amounts, asking open-ended questions, directing the answers only by shaping the question, and keeping the phrasing of the questions neutral to reduce my personal biases colouring the participant’s answers (Polkinghorne, 1989; Yin, 2011).

In terms of sampling, the interview participants are drawn from my network of personal contacts on the basis that they hold responsibility or accountability for the security of organisation-wide information. The assumption is that they would therefore have some experience with the phenomena of strategic-level information security strategy, thus this was a form of theoretical sampling (Wiesche et al., 2017). The organisations are from a mix of government, business and educational sectors to provide a full range of descriptions of the phenomena (Polkinghorne, 1989). The data is to be collected from both public and private organisations, from medium to very large in size, to triangulate sources and improve research validity (Creswell, 2003). The interviewees are drawn from personal contacts and from referrals from contacts,
following an open-sampling strategy to maximise opportunities for enhancing the relevant data (Strauss & Corbin, 1990).

When generalising data from phenomenological studies, the focus is not on population features but rather how specific the description of the topic essence might be (Polkinghorne, 1989). When generalising, the description of the topic essence must be made in so as to dispel any doubts in the reader’s mind that the understanding is applicable in different situations (Polkinghorne, 1989). The tactics for generalising are based on stratifying the sample of research participants so that they are representative of the types of people to whom the findings hold (Polkinghorne, 1989).

Before the interviews begin, I will deliver a uniform speech on the collection and analysis procedures, with assurances that accidental self-disclosures will be redacted out of the final transcripts. The participants are informed that the interviews will be audio-recorded and are asked to sign informed consent forms prior to the interview commencing. Once the recording has begun, the participants are to be reminded that the interview is being recorded and asked to confirm verbally that they agree with this. The venue for conducting the interviews may vary based on availability and rapport, from a quiet office setting to a loud café. The interviews are designed to be conducted over 45 minutes and are open-ended, semi-structured and discovery-oriented (Flint, Woodruff, & Gardial, 2002). The data collection focuses on organisational information, strategic documents, inherent risk, value, controls, contextual factors, outcomes and stakeholders.

Observations will be made during the course of the interviews and recorded in field notes. Before each interview, I create printouts of the research questions and use them as the basis for the field notes, spacing the questions out to create room for notes on the paper. I annotate the top of each sheet with the participant number to
identify it. Then when I ask each question, I make notes when the answers are unusual or unexpected. Not every answer from the participant will yield an interesting response.

Information security strategy documents are collected as well, from research participants who undertake a research interview. During the interviews with research participants, I ask a question about whether an information security strategy document exists within the organisation:

Q: “Does your organisation have an information security strategy document?”

If the answer is yes, then I follow up with a supplementary question:

Q: “May I please get a deidentified copy of the document for further analysis?”

This request is combined with a verbal statement that reiterates that the document will be held securely within the university for a period of five years following the date of the last publication from the research data and then destroyed.

3.4.9 Data Analysis Procedures

Data analysis should ideally begin immediately after the first interview has been completed, to identify related concepts and begin to refine interview questions for the next interview (Corbin & Strauss, 2008; Glaser & Strauss, 1967). This is not always possible, simply due to the impracticalities of interviewing people; for example, a few participants might coincidentally want to be interviewed on the same day because they are collocated at an interstate conference, giving the researcher no time between interviews to analyse data. The initial concepts related to information security strategy which were identified during the literature review were used to develop initial interview questions and this is an example of theoretical sampling (Corbin & Strauss, 2008).
Coding is the process where data are disassembled, inspected, conceptualised and then integrated to form a cohesive theory (Strauss & Corbin, 1990). The process examines raw data and abstracts key parts of them to a conceptual level and there are various stages to coding (Corbin & Strauss, 2008). Open coding is the first stage of examining primary data and then breaking them up into concepts according to ideas or themes that are related to the research topic (Corbin & Strauss, 2008; Glaser & Strauss, 1967; Wiesche et al., 2017). Using open coding to analyse the results allows for the appearance of unexpected themes (Gioia et al., 2013; Strauss & Corbin, 1990). One way to approach this is to begin with a list of codes identified in the literature review and then revise them as the data are examined (Corbin & Strauss, 2008; Miles & Huberman, 1994). Every statement from a research participant should be examined and potentially assigned to a concept, so the number of concepts will grow quite quickly right from the beginning, perhaps leading to hundreds of concepts. The data should be coded so that they are preserved in the language of the participants and assigned to concepts.

Although there are many options, the two main ways to analyse data, as espoused by many qualitative researchers, are questioning and constant comparison (Corbin & Strauss, 2008). Questioning refers not to asking questions of the participant but rather of the data collected from the participant, examining particular phrases or ideas expressed for meaning (Corbin & Strauss, 2008).

Constant comparison is where the researcher compares separate incidents described in the data for similarities and differences and groups them as distinct concepts accordingly (Corbin & Strauss, 2008; Wiesche et al., 2017). The aim is to identify properties and dimensions of the concepts, illustrated by the separate incidents. A variation on this technique called theoretical comparison, where incidents in data are compared to concepts occurring outside the research, might also be used if the data are unclear as to what they represent (Corbin & Strauss,
These techniques will be used extensively in this research on information security strategy during data analysis. The interviews are transcribed and analysed after each is completed, which allows for the interview questions to be modified before the next interview. Modifications to questions may be necessary upon discovery of interesting concepts or realisation that questions are not uncovering concepts related to the research question.

Other common techniques used to analyse data include examining various meanings of a word (Corbin & Strauss, 2008). This may become quite important in this research because for example the literature review has revealed some authors using the word strategy (singular) and other authors using the word strategies (plural) in the context of information security, with different meanings as they might indicate an unconscious change in level of application within an organisation. Techniques such as flip-flop, using personal experiences, identifying red flags, emotions and time are also used (Corbin & Strauss, 2008).

Regardless of the techniques used, the intention is to break the data into smaller, more manageable chunks, examine the data for the ideas or the essence contained within, and then apply a conceptual label to the text (Corbin & Strauss, 2008). These labels can then be compared with data from other sources for similarities or differences.

At a practical level in open coding, every interview is audio recorded and then transcribed verbatim. These transcripts are then modified to remove identifying features such as individual and organisation names that are inadvertently self-disclosed throughout the course of the interview, remove any profanity, remove umms and ahhs, and reconfirm unintelligible sections. I then import the transcripts into the qualitative analysis software tool NVIVO and manually code the content into nodes, which are key concepts identified in the data. The field notes completed while
observing interviews are manually reviewed for interesting insights with the research topic in mind. The field notes are reviewed at the end of each interview for completeness and to also allow for some reflexion on the research topic. The field notes from observing each research participant are used to both improve the cumulative understanding of the research topic and to also improve the interview questions, when they caused difficulty or uncertainty when eliciting a response from the participant. The information security strategy documents are manually inspected for clues about the organisation’s fixation on themes arising from information security strategy as discovered in the literature review, based on formatting, layout, order, diagrams, and tables.

The second step is axial coding, where all the concepts that have been created may start to appear similar or different to each other (Gioia et al., 2013). Axial coding requires the researcher to relate concepts with other concepts to create categories (Corbin & Strauss, 2008; Wiesche et al., 2017). The concepts can be merged if similar and thus the total number of concepts can be reduced to a more manageable number, perhaps somewhere in the order of 25 to 30 (Gioia et al., 2013). These concepts can then be labelled (still using participant terms) to make identification easier. In axial coding, the researcher can apply their own intuition, knowledge and experience to theoretically group the concepts by theme (Corbin & Strauss, 2008; Gioia et al., 2013). This can then affect the subsequent interviews as the researcher may modify research questions based on what has been uncovered so far (Gioia et al., 2013). The researcher then identifies whether the themes that have been uncovered can be treated as concepts that serve to describe some aspect of the topic information security strategy (Gioia et al., 2013). Concepts that don’t appear to be linked to existing theoretical concepts in extant literature (i.e. have “identity ambiguity”) warrant further attention (Corley & Gioia, 2004; Gioia et al., 2013). Concepts that do appear to be well described in the extant literature (i.e. have
“optimal distinctiveness”) become apparent quite quickly (Gioia et al., 2013; Gioia, Price, Hamilton, & Thomas, 2010). At some point, there will be no new concepts or themes added after interviews and the study will have reached “theoretical saturation” (Corbin & Strauss, 2008; Gioia et al., 2013).

The third step is selective coding, which is a coding step that identifies only those concepts related to the core category (Glaser & Strauss, 1967). The fourth step is “coding for process”, which is a coding step that identifies the relationships between the selected categories (Glaser & Strauss, 1967).

The final step, theoretical integration, is to cycle through all the terms, themes, dimensions, properties, and the extant literature to assess whether the concepts discovered have been documented previously (Gioia et al., 2013). This step compares both generated data and also extant theoretical literature at the same time (Alvesson & Kärreman, 2007; Gioia et al., 2013). As noted in the previous section, there will be no attempt to increase validity through triangulation using the assistance of other researchers to achieve interrater reliability (Polkinghorne, 1989). At every step, the researcher must cognitively analyse concepts as they emerge, consider their relationships and properties, and document insights in the form of memos (Corbin & Strauss, 2008; Wiesche et al., 2017). The final step is to publish findings by writing papers or journal articles (Corbin & Strauss, 2008; Wiesche et al., 2017).

This concludes the steps that will be used in the data analysis. The next step after the results have been analysed and reported in the Findings chapter is to generate an inductive theoretical model that is grounded in the data. This model will contain dynamic relationships between concepts, themes and categories, and will be described further in the Discussion chapter.
3.4.10 Trustworthiness of Findings

This study intends to improve trustworthiness of findings from analysis of the data through several aspects. First, the focus of this study should be on “credibility, plausibility and trustworthiness” (Glaser & Strauss, 1967, pp. 223), not validation which implies some kind of accurate positivistic, quantitative results. Other attributes of successful grounded theory studies are transferability, dependability, and confirmability (Sikolia, Biros, Mason, & Weiser, 2013). Validity, reliability, and truth are terms that are incorrectly used in relation to qualitative research, as they carry quantitative connotations (Corbin & Strauss, 2008). The data used to construct the theory cannot be reused as the data to validate the theory. The intent of this research program is to engage in theory building not theory testing, which is suggested as a future research direction.

The use of constant comparison, multiple slices of data, and multiple data sources, such as interviews, observations, and examination of documents, will be used to triangulate and correct any inaccuracies in the data to enhance credibility (Strauss & Corbin, 1998). Negative cases and variations of concepts will also be actively sought after and documented when found to also improve credibility, and prolonged engagement with participants is planned (Sikolia et al., 2013). Where possible, use of participant words (in vivo terms) will be used in the emerging theory to improve credibility (Sikolia et al., 2013). Clear descriptions of the research is planned to enhance transferability (Sikolia et al., 2013). Adherence to rigorous procedures for collecting, coding, analysing, and presenting data are what dependability in this grounded theory study should be judged on (Glaser & Strauss, 1967; Sikolia et al., 2013). Since this doctoral study was conducted by a single person and the ethics statement did not allow for data disclosure to other persons, assessing confirmability by presenting the same data to other researchers and comparing audit trails for procedure completion with the original researcher is not possible in this study.
3.5 Chapter Summary

The chapter began by identifying the overall aim of the research, based on the findings from the literature review in the previous chapter, which surveyed the literature, mapped the territory and identified gaps in knowledge. A research process flow chart was given depicting the steps that would be undertaken during the course of the entire research program. The adopted research approach begins with an examination of my understanding of the ontological reality of the research topic information security strategy, which in this case is nominalist. The key areas within research philosophy are described which include a constructivist epistemology, interpretivist philosophical stance, phenomenological GTM, and interview, observing, and collecting and examining methods. The data sources include interview transcripts, information security strategy documents, and personal field notes taken during the interviews. The data collection and analysis procedures were adapted from Corbin and Strauss (2008).

The next chapter describes the findings from collecting data based on the research approach described in this chapter, whilst remaining aligned to the research aim and the revised research question. The findings include analysis of transcripts from interviews with senior security executives within very large organisations, field notes detailing my observations during the conduct of the interviews, and examination of information security strategy documents where they existed and were permitted to be released. The collective results are analysed, and these analyses are then interpreted to create new knowledge.
Chapter 4: Findings – Information

Data collection via interviews, document collection and examination were conducted over a two-year period. This research was initially exploratory and then explanatory, focussed on building and developing new theory (Corbin & Strauss, 2008; Zmud, 1998). This chapter is titled Findings not Results to avoid ambiguity arising from any perception that this research involves empirical tests which would have results. Being a qualitative study seeking a profound understanding of a phenomenon from rich data, Findings is the more appropriate term (Gioia et al., 2013).

4.1 Chapter Aim

The aim of this chapter is to describe the findings after analysis of the data, providing a rich description of the concept of information security strategy, analysed for its properties and dimensions, noting any variations throughout. After the data were analysed, the analyses are aggregated into categories, integrated, and interpreted in relation to the overall research question.

4.1.1 Research Participant Demographics

The anticipated problems with collecting data of a sensitive nature, such as that related to information security strategy, were overcome successfully during this substantive research program. Security researchers have previously been advised to select a few organisations to study with which they have established a strong relationship and trust (Kotulic & Clark, 2004). I spent two years collecting the contact details of senior security executives at industry conferences and events before the data collection phase began and I believe these pre-existing relationships contributed greatly towards the high rate of success with research subjects agreeing to participate in the study. I avoided mailing surveys or questionnaires and instead
chose interviews as the key data collection method, which conformed to advice about adopting a slow, cautious style (Kotulic & Clark, 2004).

The interview data were gathered over a two-year period. This allowed for constant comparison between interviews and improved rewording of any questions that were confusing to the research participant or to elicit data on interesting concepts, as “it is only through interaction with data the relevant questions emerge” (Corbin & Strauss, 2008, pp. 216). In all, the research questions were reworded or changed 14 times. To briefly recap the data collection and analysis procedures, the interview phase sample consisted of twenty-five interviews with research subjects who all purported to be accountable or responsible for information security strategy in their organisation (see Table 4.1). Although the interviews were designed to be conducted over 45 to 60 minutes duration, there was individual variability in the results. The interviews were conducted as uniformly as possible however differences in answers or communication styles meant that some interviews were as short as 30 minutes and one was as long as 111 minutes. In total, 25 participants provided 23 hours 17 minutes of interview audio for transcription, which produced transcripts with 152,000 words for analysis.

Interviews were mostly conducted face-to-face however sometimes the interviewee was in another territory or country whilst travelling and the interview was conducted over the phone via a conference-call and recording service (Polkinghorne, 1989). I found it difficult to maintain rapport when the interview was conducted via a telephone call and experiencing intermittent latency issues with voice transmission, however I took the time to reassure the participants that I had designed the research to be as low-risk as possible to them, which went some way towards lowering their apprehension.
Audio-recording interviews offers a distinct advantage in allowing the interview to proceed uninterrupted without me as the researcher continually pausing the interviewee to allow me to catch up writing notes, as would be the case if I were to transcribe the participant’s answers during the interview. There were some risks with this approach however, as in one instance, I was using my mobile phone as a recording device and received a call in the middle of the interview because I had forgotten to switch it to flight-mode before recording. On another instance, the national voice data carrier had multiple outages and after several attempts to conduct the phone-based interview, it had to be rescheduled to another date. On another occasion when reviewing the audio-recording after an interview, I discovered that the audio-recording service had incomprehensively failed to fully record the phone-based interview and stopped half-way. Luckily the audio-recording service company had an IT department that was able to restore the full recording from backup after some effort. On another instance, for some reason there were latency and reverberation issues with the quality of the call. Whenever I asked a follow-up question, there was a few second delay which meant my words interrupted the participant, who had continued to talk. Overall, face-to-face interviews were the preferred option if possible.

The interview protocol contained semi-structured, open-ended, discovery-oriented questions (Flint et al., 2002). Data collection from interviews focused on organisational information, strategic documents, information sensitivity, controls, contextual factors, outcomes and stakeholders. Where an OrgISS document existed and was supplied, this formed a secondary source of primary data collection, serving to improve internal construct validity through triangulation (Creswell, 2003). Interviews were audio-recorded with permission and then transcribed. The transcriptions and strategy documents were imported into NVIVO, a qualitative analysis tool, and the content manually coded into themes, which are concepts in the
data (Strauss & Corbin, 1990; Yin, 2011). The data analysis began after the first interview and the use of constant comparison meant that the interview questions needed refinement and were changed to improve coherence and to more accurately investigate key concepts emerging from the data.

Of the 25 participants recruited to participate in this research, 24% (six organisations) were government departments. 16% (four organisations - TelCo1, TelCo2, EnerCo1, AvCo1) were private-sector but heavily regulated by government, which is a total sample of 40% public sector-oriented organisations, allowing a crucial insight into the public sector to assess whether the unit of analysis, information security strategy, has different properties or dimensions compared with other organisations. 16% (four organisations) were from the finance sector and 24% (six organisations) were from either the ICT or consulting sectors. 8% (two organisations) were from the education sector, 4% (one organisation) was from the pharmaceutical industry, one was from retail, and one was from resources sector.
Table 4.1. Data Collection Phase Sample – Organisation Demographics

<table>
<thead>
<tr>
<th>Participant</th>
<th>Industry</th>
<th>Size*</th>
<th>Job Title</th>
<th>Quals</th>
<th>Certs</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 FedGov1</td>
<td>Government</td>
<td>Very Large</td>
<td>CIO</td>
<td>MBus</td>
<td>None</td>
<td>15 years</td>
</tr>
<tr>
<td>2 StatGov1</td>
<td>Government</td>
<td>Very Large</td>
<td>CEO</td>
<td>MBA</td>
<td>None</td>
<td>10 years</td>
</tr>
<tr>
<td>3 ITCO1</td>
<td>ICT</td>
<td>Medium</td>
<td>CEO</td>
<td>MBA</td>
<td>None</td>
<td>10 years</td>
</tr>
<tr>
<td>4 FedGov2**</td>
<td>Government</td>
<td>Very Large</td>
<td>Dir ICT</td>
<td>None</td>
<td>None</td>
<td>6 years</td>
</tr>
<tr>
<td>5 FinCo1**</td>
<td>Finance</td>
<td>Very Large</td>
<td>CISO</td>
<td>MIT</td>
<td>CISSP</td>
<td>25 years</td>
</tr>
<tr>
<td>6 FinCo2**</td>
<td>Finance</td>
<td>Very Large</td>
<td>Head InfoSec</td>
<td>BMath</td>
<td>CISSP</td>
<td>22 years</td>
</tr>
<tr>
<td>7 ITCO2</td>
<td>ICT</td>
<td>Medium</td>
<td>MD</td>
<td>MBA</td>
<td>None</td>
<td>15 years</td>
</tr>
<tr>
<td>8 ITCO3**</td>
<td>ICT</td>
<td>Medium</td>
<td>CEO</td>
<td>BCom</td>
<td>CISSP</td>
<td>18 years</td>
</tr>
<tr>
<td>9 PharmaCo1**</td>
<td>Biopharma</td>
<td>Very Large</td>
<td>CISO</td>
<td>MSIA</td>
<td>CISSP</td>
<td>12 years</td>
</tr>
<tr>
<td>10 ITCO4</td>
<td>ICT</td>
<td>Very Large</td>
<td>CSO</td>
<td>MCM</td>
<td>CISM</td>
<td>16 years</td>
</tr>
<tr>
<td>11 FedGov3</td>
<td>Government</td>
<td>Very Large</td>
<td>Cyber Policy</td>
<td>BA</td>
<td>None</td>
<td>4 years</td>
</tr>
<tr>
<td>12 TelCO1**</td>
<td>Telecom</td>
<td>Very Large</td>
<td>CSO</td>
<td>MBA</td>
<td>None</td>
<td>5 years</td>
</tr>
<tr>
<td>13 EnerCo1**</td>
<td>Energy</td>
<td>Very Large</td>
<td>CISO</td>
<td>MBA</td>
<td>None</td>
<td>20 years</td>
</tr>
<tr>
<td>14 AvCo1</td>
<td>Aviation</td>
<td>Very Large</td>
<td>CISO</td>
<td>None</td>
<td>CISSP</td>
<td>25 years</td>
</tr>
<tr>
<td>15 MgtCo1</td>
<td>Consulting</td>
<td>Very Large</td>
<td>CISO</td>
<td>BCom</td>
<td>20+</td>
<td>20 years</td>
</tr>
<tr>
<td>16 MgtCo2</td>
<td>Consulting</td>
<td>Very Large</td>
<td>Partner</td>
<td>MBA</td>
<td>MIT</td>
<td>11+</td>
</tr>
<tr>
<td>17 StatGov2**</td>
<td>Government</td>
<td>Very Large</td>
<td>CISO</td>
<td>MIT</td>
<td>CISM ISO27001</td>
<td>18 years</td>
</tr>
<tr>
<td>18 StatGov3**</td>
<td>Government</td>
<td>Very Large</td>
<td>CISO</td>
<td>BA</td>
<td>CISA CISM CGEIT</td>
<td>20 years</td>
</tr>
<tr>
<td>19 EduCo1</td>
<td>Education</td>
<td>Very Large</td>
<td>CISO</td>
<td>BIT</td>
<td>CRISK</td>
<td>28 years</td>
</tr>
<tr>
<td>20 RetCo1</td>
<td>Retail</td>
<td>Very Large</td>
<td>CISO</td>
<td>MSc</td>
<td>CISSP</td>
<td>20 years</td>
</tr>
<tr>
<td>21 EduCo2</td>
<td>Education</td>
<td>Very Large</td>
<td>CTO</td>
<td>MBA</td>
<td>None</td>
<td>15 years</td>
</tr>
<tr>
<td>22 FinCo3</td>
<td>Finance</td>
<td>Very Large</td>
<td>Head InfoSec</td>
<td>MBA</td>
<td>SABSA</td>
<td>15 years</td>
</tr>
<tr>
<td>23 TelCO2</td>
<td>Telecom</td>
<td>Large</td>
<td>Chairman</td>
<td>BSc</td>
<td>None</td>
<td>10 years</td>
</tr>
<tr>
<td>24 FinCo4</td>
<td>Finance</td>
<td>Very Large</td>
<td>CISO</td>
<td>MSc</td>
<td>ISO27001 MCSE CCSE</td>
<td>20 years</td>
</tr>
<tr>
<td>25 ResCo1</td>
<td>Resources</td>
<td>Very Large</td>
<td>CISO</td>
<td>MIT</td>
<td>CISA CISSP</td>
<td>20 years</td>
</tr>
</tbody>
</table>

*Small= 1-20 employees, Medium= 21-100, Large= 101-1,000, Very Large= 1,001+

**Provided an information security strategy document during data collection
The 25 interview transcripts were analysed using open-coding techniques following the procedures set out in the previous chapter (Corbin & Strauss, 2008) and 152 concepts were initially identified. After analysis for duplicates, that number was reduced to 130. Then, after combining concepts that were very similar or underutilised, the number of concepts was reduced to 109, as “coding helps the analyst to get inside the data, to start to feel them at a gut level” (Corbin & Strauss, 2008, pp. 170). See Appendix G: Data Structure for a summary of concepts and categories.

Concepts in this context are defined as the word identifiers, created by the researcher after analysing the data, that describe ideas expressed in the data by the research participants (Corbin & Strauss, 2008). If a participant uses a word that describes a phenomenon so perfectly that it can’t be improved, then the researcher may borrow this word for use as the concept name, and this is called an in-vivo code (Corbin & Strauss, 2008). In the following Information section, four in-vivo concepts are identified in the data, which are fortification, devaluation, minimisation, and outsourcing, which are described further in Chapter 7: Discussion.

Concepts were identified and described in detail along with their properties, dimensions and relationships. A group of concepts that relate to each other can be aggregated under a higher-level concept known as a category (Corbin & Strauss, 2008). The following is a list of categories identified in the data and are summarised in Appendix G: Data Structure. They are primarily drawn from the interview data but are supplemented and reinforced using data from observations and document collection.

### 4.2 Information

Several concepts were identified that relate to the core category, information. The four main concepts that emerged from the data were accessing the functionality
provided by information, controlling information, information as an asset, and information value. A few properties of information were also identified which were information classification, information location, and information ownership. A description of these concepts and their properties and dimensions follows.

4.2.1 Information Asset

*To summarise this section, the key asset being secured is information, not the IT systems it resides on, which affects security governance, although variations exist.*

An important point is that the key asset being secured and used is information. It is important to state this because there was some variation in views about whether the infrastructure or platform that information resides on, or whether the staff or systems that interact with information, are assets of similar or greater importance. Of course, systems are important to enable the achievement of business outcomes, however, from this research data, information is the key asset around which the other stakeholders and platforms revolve. MgtCo2 stated “*we are pushing toward a data-centric approach to security, because ... we believe that [organisations] can then decide where they want to spend the money.*” AvCo1 shared,

“We use something called most valuable information. You’re probably familiar with the term crown jewels. With any company, there’s always a set of what you call mission critical assets and that can be a set of IT applications or information database or whatever. You’ve got mission critical assets that without them, the company would either cease to function or even go out of business if they were compromised or unavailable in some way.”

One variation on this view comes from TelCo1, who objected to the focus on information security and instead focussed on *converged security*, stating,
“converged security is a security accountability to one person in the organisation, the Chief Security Officer. So, from enterprise-wide, one side of the organisation to the other, all things security are accountable to me.

If you actually take the word security and you apply that to cyber security, to security operations, to security response, to facility security, that word security lies with one accountability, and that accountability belongs to me. I believe that is the sustainable organisational structure model for managing security as a business risk going forward, not just here in Australia, but it's a growing trend across the globe.”

TelCo1 held primary accountability and was then accountable to the board. TelCo1 held the view that information security can’t be separated from physical security or personnel security because they are too intertwined. The delineation between the security aspects of the roles and responsibilities of a multitude of executives in these different areas internally is too difficult and leads to confusion during and after a security breach. In TelCo1’s view, this causes difficulties both in timeliness and in ascribing culpability when conducting a post-incident review. This view on converged security however does not necessarily invalidate the view that information is the key asset being protected. Rather, it might strengthen it by improving accountability lines for information protection within the governance structures of the organisation.

4.2.2 Information Value

To summarise this section, an information property is value, which has dimensions ranging from low to high, and high can extend to being irreplaceable. This affects classification and security controls.

Information has a value, which is one of its properties. In terms of dimensions, research participants did not universally agree on how to precisely measure the value of information other than to say it was generally high or it was low. The one variation
on this was another dimension of high value information, which was when high value information was irreplaceable. Participants also held varying views on how to determine the value of information.

The journey for organisations to optimally manage the value of information held within the organisation is to begin by taking the time to discover and audit all the information holdings. On the storage of information with low value, ITCo4 lamented,

“Traditionally, organisations, particularly the on-premise environments, don’t make any distinction [between high and low value data] and that’s a part of the problem. So, they use really expensive hardware and services, and they just store all their data together.”

In assessing information to determine its value, if the information is used by the organisation to conduct core business then it has high value to the organisation. In this explanation, FedGov1, a health regulator, distinguishes between information related to collecting payments from customers (non-core business, in this case credit card numbers from health practitioners) and information about the quality of care they provide (core business),

“we don’t need credit card details to do our business. We do need to know that you’ve paid your fees, but I don’t need to know your credit card details necessarily. But I do need to know that you’re a practitioner, that you’re doing things that you say you’re doing, and I can identify you. That’s to do my business.”

In terms of how to assess the value of information, the nature of the information or what it relates to can determine its value, and hence its stakeholders and regulatory oversight. For example, FedGov1 identified that “we have information that identifies people and also some about their health, so that automatically puts us in the Privacy Act.” StatGov1 added “the closest we’ve got, I guess, is personnel data, so for our
own staff and potentially related health, like sick leave and that kind of thing." Some organisations followed a formal framework to assist in determining the value of the information so that a classification could be assigned, as EduCo1 shared,

“There is a framework associated to the data classification which facilitates the person or the data owner or the delegate to the data owner, facilitates the process for them to understand the business importance of that data element.”

FinCo3 saw merit in following a business value framework rather than a specific security-oriented one, stating

“We use our operational risk management framework, which is a broader framework than cyber security, to look at the impact of something either being not available, something being corrupted, or something losing its confidentiality, the classic CIA triad.”

ResCo1 used a business value framework that was based on business concepts such as reputation rather than security-oriented concepts such as confidentiality, sharing,

“We have an enterprise risk management framework that calls out things like impact to reputation, impact to finance, that sort of stuff, different things on what the impact is, and then, people assess the data based on that.”

It is important to note that the classification of information does not drive the value but rather the value drives the classification, which then has implications for the level of security controls put in place to protect it. FedGov2 illustrates “It’s not just the classification that determines how we store and handle our information, it’s the value.” FedGov2 then continued,
“we did some modelling on a high value asset data holding. So we did a full audit of asset holdings, and we had the business owners, or the data owners, apply a score to the level of protection they believed that their data required, and then we went down to the information management layer and started looking at how we segment, how we structure, how we tag, label, and mark the data accordingly, to afford it a level of protection”

FinCo3 also highlighted that the value of information drove decisions about the volume and type of security controls that are put in place to protect the information, stating,

“those labels on those documents … drive a differential application of security controls. So, things that aren’t very sensitive, we don’t put as much energy into securing them as we do those things that are very sensitive.”

This relationship where the presence of high value information causes an organisation to increase the volume and type of security controls is important and will be termed P1a in Figure 7.2.

In a sign that government regulators are getting their policies right, the value of the information informs the consequences should the organisation fail to protect it adequately, which then leads to defensive patterns of behaviour within the organisation. This linkage between culpability and consequences is crucial to driving improved behaviours. ITCo3 explained,

“most views of security are still defensive in nature. So, the question is: I’m not worried about losing credit card data because it’s valuable to me. I’m worried about losing credit card data because I’m going to get fined and get into trouble with [Payment Card Industry] Security Standards Council if I lose that data. And I’m worried about losing customer data, not because customer data is valuable to me, but because I might have to disclose that breach, and
I’ll get reputational damage. So, the approach is much more defensive rather than about value.”

Interestingly, beauty is in the eye of the beholder, in that sometimes the owner of the information might apply a subjective bias and overrate its value. EduCo2 impartially observed what when determining the value of information, “the answer would depend on who in my organisation you asked.” EduCo2 continued,

“So, research information, for example, has value to a specific subset of the organisation, and in all honesty, some of it probably has little value because we do generate lots of it. … But prima facie, research information that can then lead on to the creation of intellectual property [which] is a category of information that has value, both potentially, inside the organisation and outside.”

EduCo2 did note however that this was not always the case and that usually the value is more apparent, stating “there’s the usual categories of business information that has value around financials and information about employees, students, and so forth.” TelCo2 was also very clear about what their most important information was, stating,

“I’d say the first bin that we would classify data in would be according to the regulator. That which is sensitive from a regulatory point of view, that would come first and foremost because we have our licenses, and we must comply with those to remain in business.”

TelCo2 clarified their three main sources in decreasing levels of value, with “I’d say regulatory, … then customer, and then internal would be three that we would classify data in.”
4.2.2.1 Low Value Information

One property of information is value and one dimension of value is low. Low value information is often viewed as information that could either deliberately or unavoidably become publicly disclosed, negating the common security requirement for confidentiality. ITCo2 confirmed “low value equates to publicly available or can be accessed publicly. … You want [sales] brochures, you want information about the company, you want to know our addresses, etc. Fantastic, just let it go.” This did not negate the need for availability or integrity, as ITCo2 continued, “changing details can be as detrimental as anything else”. FinCo2 gave an example, “If you’re selling a product for $1,000, you don’t want somebody change the price to $10.” These two aspects of the CIA triad may still require strict security controls to be in place to protect the information, as ITCo2 offered “if you want to get specific data, or I want to change specific data … then you may need a certain level of authentication”.

One reason that information has low value is that it has lost its value over time, as PharmaCo1 explained “some data is obsolete, it’s out of date or whatever.” FedGov2 confirmed, “90 percent of the data that sits within our data holdings is probably short-term or volatile data. It’s good for a point in time, and then after that it becomes historical.”

That doesn’t mean that organisations can automatically blanket-delete all old information to lower risk, as FedGov2 continued, “The problem is that we’ve got these regulations around storage of data and having to keep certain amounts of data under the Privacy Act 1988 for seven years or longer.” PharmaCo1 experienced a similar situation, explaining “we’re a drug company. We need to retain things like manufacturing batch records for 30 years.” In the case that historical information was required to be kept, the approach PharmaCo1 took to protect itself was this “type of
Information is archived. When it is archived, it's encrypted, and then, quite frankly, I'm not sure if it's ever looked at again."

Some automation in governance around the deletion of information is useful though, particularly given the rapid proliferation of information throughout modern organisations (“A good example is SharePoint sites. Those things seem to grow like weeds”, PharmaCo1). ITCo4 found, “information can … be deleted because it's 10 years old. Or to use the classic government example, this is now 30 years old, so therefore it's automatically declassified for public release.” Sometimes assistance with the governance of destruction of information is helpful, as MgtCo1 stated, “We outsource those [deletion] functions, and they provide a compliance certificate of destruction.”

Some organisations saw merit in following an information lifecycle management system to manage their information. This was perceived as particularly useful because information lifecycle management offered more than just governing the timely deletion of information, as it included the initial identification of information, its classification based on value, and its storage. StatGov2 revealed,

“This our information is stored and kept and the whole life cycle is managed by the State Records Act 1998, and that decides how long we will keep that information. … earlier it was considered that an email was a record, and so we had to secure email for 20 years or 30 years, but what we have done is we said no. If the email is the record which you want to keep, you have to save it in the project folder and in the record management system. So now, our email retention policy is only two years. … If you need that information, … then you save it in [records storage system] and it will be categorised based on what type of record or information it has, and then it will follow the records retainer policy accordingly.”
The low value of information also has implications for the level of controls placed around the information to protect it, as ITCo3 broadly offered “if the information is low value then don’t worry about protecting it. We have this concept in our company of minimum viable security.” This idea, to use minimal efforts to protect information, may appear contradictory at first but there are business benefits to this approach.

This relationship where the presence of low value information causes an organisation to decrease the level of security controls is important and will be termed P1b in Figure 7.2.

One benefit to this approach is being able to employ plausible deniability against culpability in the event of a security breach, as ITCo3 explained, “Minimum viable security is: What do we need so that if something goes wrong we’re not seen as being horribly negligent?”

Although not immediately obvious, another business benefit is the conservation of security budget, so that more financial resources are available to protect high-value information with better quality security controls. TelCo1 clarified,

“By categorising the information, you can actually get bang for your buck. You can put the right security controls around the [information] that matters. … Which one are you going to protect?”

When questioned as to why that is important, TelCo1 responded “Well, you’ve only got a limited budget.”

### 4.2.2.2 High Value Information

Information was perceived as the life-blood of organisations, as FedGov2 observed that “business information is a business enabler”. PharmaCo1 added “We create new information and new ideas that turn into drugs. Information is the new currency.” StatGov1 assigned high value to information about stakeholder groups such as
employees and customers but was less concerned about their own organisational information, stating “Our financial data, who cares. It’s not something you want to leave on a bus, but if we did, no one would die.”

The possession of high-value information had implications for its storage, in that organisations should keep all their high-value information in one carefully defined location, as ITCo3 explained,

“we’re seeing organisations … trying to create a sensitive data environment, basically so that they can keep all their sensitive data in a relatively constricted set of systems and environments that they can apply more controls to, rather than having to apply all of those controls across everywhere. … If information is sensitive, then you effectively want to put it somewhere where most of those controls are already in place … because otherwise it’s going to cost you a lot to do it.”

The nature of the high-value information may also place restrictions on the location that it is stored in, and PharmaCo1 gave an example of, “In the case of personal identifiable information, there are also national and regional regulatory issues about data residency.” Identification of the most appropriate location begins with a risk assessment, as EnerCo1 explained

“We do risk assessments around whether that should be housed internally, whether that should be on cloud environment, what sort of management overhead is in need on that, and what are the basic tools and sets that need to be done at different levels.”

High-value information also requires a higher level of security controls to protect it, as FedGov3 explained that “there’s a range of interlocking physical and IT systems that are used to protect that information.” EnerCo1 uses a varying number of “about 130
In terms of deploying a range of controls, organisations take a methodical approach, beginning by identifying the main threats. Threat identification allows for more appropriate deployment of security controls to be deployed, commensurate with whether the threats are persistent or targeted, to protect information. FinCo4 said

“We take a defence-in-depth or layered approach. The first step we take is to hunt externally for threats and gather intelligence, for example from the dark web. The second step is to protect our perimeter. The next step is to protect our internal infrastructure and networks. The final step is to protect our servers, applications and data.”

In a variation on this approach, when information is embedded within other systems such as applications or databases, some organisations assessed the entire collection of systems rather than trying to separate them, as AvCo1 explained “we’re more focused on the application itself, … and then look at what makes up the ecosystem of that application.” Although this organisation stated they focus on the application, this approach does not invalidate this research’s focus on information as it was clear that AvCo1 were also focussed on information, with

“If you’ve got a reservation system that is obviously crucial to what we do in this organisation, it needs to be available all the time. You can’t afford to have any downtime, then that becomes good criteria to be the most valuable...
information. Also, ... that information contains sensitive information about passenger details”.

Controlling access to high-value information was a key consideration for research participants, as StatGov2 revealed “Only 26 people are allowed to receive or send or create or have access to security classified information in the organisation.” StatGov2 continued “the level of access is decided based on what is your need-to-know policy.”

4.2.2.2.1 Irreplaceable High Value Information

High value information caused a different set of behaviours when it was irreplaceable. The research participants seemed to instinctively understand that protection of trade secrets that were central to the core business of the organisation was crucial. Once trade secrets are leaked, they can’t be ‘un-leaked’ and the results of this loss can result in short to long-term damage, up to and including bankruptcy.

Identification of irreplaceable high value information has implications for the storage of that information, as organisations wanted to maintain complete control over it, reducing the risk of its loss as low as possible. ITCo4 confirmed “The highly-sensitive trade secret type information is generally kept on isolated systems within our corporate environment.” ITCo3 agreed that irreplaceable high value information must be protected at all costs, stating,

“If your IP is genuinely that much of – if you lose it, then it’s over kind of scenario, then, yeah, it’s going to be like the recipe for Coke and the recipe for Big Mac sauce and keep it locked in a vault and systems that are not internet connected, so that can rule out outsourcing.”

AvCo1 used the term Most Valuable Information to refer to irreplaceable high value information that has significant repercussions such as bankruptcy should it become lost, affirming,
“We use something called Most Valuable Information. You’re probably familiar with the term crown jewels. With any company, there’s always a set of what you call Mission Critical Assets and that can be a set of IT applications or information database or whatever. You’ve got mission critical assets that without them, the company would either cease to function or even go out of business if they were compromised or unavailable in some way.”

MgtCo2 agreed that “it’s normally around the criteria of crown jewels, as to what information is the most important that will either bring their business to a halt or will put them on the front page of the news.” FinCo4 offered an analogy to illustrate the point by equating irreplaceable high value information to the possession of his grandmother’s wedding ring, saying,

“This analogy refers to why wouldn’t I store my valuable information in an outsourcer’s secure environment. Sometimes that makes sense, because external cloud-based solutions can be more secure than what you have internally. For us however this doesn’t make sense. Our internal data centres are more secure than what can be found in the market as we have the funds to make this possible. The other reason I wouldn’t use an outsourcer’s service is that my grandmother’s ring is irreplaceable, and I don’t trust the outsourcer enough.”

4.2.3 Information Control

To summarise this section, control of information seems to take three different dimensions according to the data: 1. Full control, 2. Shared (partial) control, and 3. No control. Each of the three dimensions could be appropriate for use by organisations depending on their circumstances.
4.2.3.1 Full Control Over Information

Full control was adopted by ITCo1, who had experienced negative situations where information was shared onto cloud-based platforms, and the organisation had lost control of it because of the multitude of devices that were used to access the platform. ITCo1 explained that,

“It’s inherently insecure because it'll take documents and stick them on all different devices. You've got no control over where they are, no control over what's going on and the like. So, we made a ruling that not using Dropbox and got a shared drive … for that specific purpose.”

FedGov2 found that control of information by using an information management system enabled efficiencies in access and governance, commenting,

“when data gets stored in information management systems, you then just rely on things like your data filtering, and your identity, and access, and management controls to put the layers of protection around who sits in what role, and has what function, and what permission, and what access to what piece of information.”

FinCo1 maintained full control of their information by storing it on-premises and was able to maintain control even when moving it for processing off into the cloud to take advantage of its agility and efficiency,

“It's about the service, or the cost of the whole service, the infrastructure, or the application. … we do workload in the cloud but storage on premise so that we've got control of the data, and this has been going out for the workload and then brought back down. So, I don't think storage of information is the driver. It's the operational efficiencies and the agility of consuming services. And then we consider the appropriate storage as a result of that.”
RetCo1 saw no problem with maintaining full control over highly-valuable information when storing it off-premises on cloud-based storage. When asked whether RetCo1 would store trade secrets outside the organisation, RetCo1 decided “not in an outsource provider, but I will host it in a public cloud, yes”.

This relationship where the organisation maintains full control over high value information to increase its security is important and will be termed P2a in Figure 7.2.

Effectively, organisations can compartmentalise their information and restrict access to it by using encryption to block access. RetCo1 then explained,

“I own the controls associated with protection of the data, so I can put encryption controls over the data. I can manage the configuration of the databases where the environment is sitting in. I just have somebody managing underlying infrastructure for me, providing the underlying infrastructure. Will I put valuable information in the public cloud? Yes. Would I have somebody manage my valuable information on my behalf? No.”

4.2.3.2 Partial Control Over Information

Shared or partial control was adopted by organisations that outsourced the management of their information and sometimes also their ICT infrastructure. RetCo1 was very clear on outsourcing when stating the difference between maintaining control or sharing control,

“for me, outsourcing is I go to somebody and say manage my environment on my behalf. Outsourcing is not going to the cloud. Cloud is just a different hosting platform. Whether I book the data centre myself or I use somebody else’s data centre, it doesn’t really matter for me. I’m not outsourcing anything. I’m still managing the environment.”
To make the concept clearer, RetCo1 gave an analogy, using a car as an asset instead of information, towards a goal of being transported,

“If I go to a provider and say, hey, I never want to drive again. Come and pick me up, I need you to take me wherever I need to go. I don’t want to ever see a car or car invoice or anything like that again. I don’t want to drive or touch a steering wheel again. That’s outsourcing driving. Otherwise I’m just leasing a car.”

It is important to shape the outcomes expected when sharing control in an outsourcing engagement, by deciding beforehand on the terms and conditions that are acceptable and the level of service required. When referring to the outsourcing supplier, RetCo1 would state,

“You can manage everything on my behalf and just give me a monthly OpEx figure that I pay for. I don’t care how many people you need to use. Here’s the SLAs I want. Here’s the agreement that we have, and I don’t want to see anything else again.”

One insight into the concept of partial or shared control of information is that, in an effort similar to what organisations expend in ascertaining the trustworthiness of outsourcing partner organisations, customers also need to trust organisations that hold their personally identifiable information. FinCo1 explained “The customer doesn’t care that it wasn’t this organisation that lost their data. They trusted this organisation, not the third party.”

This relationship where an organisation can maintain partial control over high value information, yet increase its security is important and will be termed P2b in Figure 7.2.
With regards to outsourcing, there are more properties, dimensions and variability, which I will analyse in later sections. This section is focussed more on sharing control of information, which overlaps with outsourcing, hence the brief foray into the concept.

### 4.2.3.3 No Control Over Information

No control was adopted by organisations looking to reduce their compliance costs and responsibilities. ITCo3 stated “the bigger element is organisations just trying to avoid having the information at all.” ITCo3 explained “rather than take payments yourself, use PayPal. Just get rid of that [credit card data] so you don’t have that data that brings with it a regulatory burden”.

This relationship where the organisation maintains no control over high value information to increase its security is important and will be termed P2c in Figure 7.2.

### 4.2.4 Information Functionality Access

*To summarise this section, information doesn’t have to be owned to utilise it. The decision whether to own information or not depends on whether it is core to the organisation achieving its goals.*

A subtle but important theme that emerged from the data was the idea that organisations don’t hold information just for the sake of holding information. They want to use the information to obtain some sort of benefit. This separation between information and its utility is important because the end benefit can sometimes be derived without actually owning the information. Whether an organisation should use information owned by an external vendor depends on whether information forms part of a core competency or not, as core information needs to be owned. This has implications for the ownership and storage of information. As ITCo1 stated,
“If something's non-core, then you've got the ability to go out, but then if it's non-core you probably don't care as much anyway. But what would be an example of something non-core? I'd imagine if someone had credit card information that would be something you'd want to be really tight on. And sure, it might be great to have that credit card information, but you're better off finding another way to use that customer identity data, if you want to use the data, and not keeping their information ad-infinitum.”

This relationship where the ability for information to form the basis of a core competency negatively affects whether it can be stored externally is important and will be termed P3a in Figure 7.2. The relationship where information does not form the basis of a core competency, which positively affects its ability to be stored externally is also important and will be termed P3b in Figure 7.2.

4.2.5 Information Classification

To summarise this section, the classification ratings system is set by a Chief Data Officer, but the classification of information is performed by the information owner upon creation.

All organisations classified their information in some fashion, which FedGov2 did extremely rigorously, but others such as ITCo1 less so, at least “not in a structured, formal way” because, as ITCo2 says, “classification of data is hard”.

The labels used in classification systems by research participants that were government-based organisations were prescribed by the federal government’s legal department. FedGov2 shared,

“There’s some freely available information from the Attorney General’s department about the government security classification structure. In amongst
that is a load of different layers of assessing the business impact level and classification of sensitivity of data.”

FedGov2 went on to list the labels commonly used by government departments and agencies, offering “TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED. FOR OFFICIAL USE ONLY, which contains a whole bunch of dissemination limiting markers, and then UNCLASSIFIED or UNOFFICIAL.”

When classification labels are not mandated by a relevant authority and the organisation has the freedom to decide their own set of classification labels, they are best off keeping them simple for ease of understanding by the data owners and other stakeholders who interact with the terms. ITCo2 offered, “we use this arcane terminology that doesn’t make sense to the normal human being … we forgot the fact that it’s really about our employees and people in the business that need to do things simply.”

In publicly or privately-held organisations, the labels in the classification structure and guidelines for assigning them are set by a Chief Data Officer, as TelCo1 said “we do have document classification, … developed by the Chief Data Officer.” The data owners are then responsible for navigating the guidelines and applying a classification rating to their information, as FinCo1 says, “security doesn’t classify the data; the data-owners do.” A commonly-held belief is that the creator of information is also the owner, as FinCo1 says, “the creator of the information is the one that should be, from a classification perspective, classifying it. … It should be classified in creation.” The Chief Information Security Officer (or Chief Security Officer) is responsible for architecting all the security controls that are used in a coordinated framework to protect information of different value, reflecting the classification labels. They are responsible for increasing the number of controls used to protect high-value information and for deploying less controls for low-value information.
Importantly, business executives may decide not to take the advice of CISO and proceed with an alternative course of action that increases risk, against the recommendations of the CISO. There may be very good business reasons for deciding to do this. In this case, the CISO can simply direct the business executive to sign an acknowledgement form and accept the increased risk. TelCo1 would say to business executives,

“If you decide to still outsource the data and don’t protect it in this fashion, fine, good luck with that. I’ll be here to help you clean up the mess if something bad happens, but ultimately, there’s the risk acceptance form, there’s your signature on the bottom of it.”

There are three stakeholders at work in this scenario (data owner, CDO, CISO) and a lack of accountability can arise when a security incident occurs due to confusion around roles. TelCo1 confirmed,

“Here’s the thing from a Chief Security Officer’s perspective. In the past, we’ve been blamed for that. Sensitive data, which [wasn’t classified] correctly, is lost. All of a sudden, it’s the security person or the security group who has the problem. That’s wrong, and the reason that security finds itself in this situation we’re in is because we haven’t had enough aggression and understanding of the ownership of the issue.”

The root cause of issues arising with loss of high-value information can sometimes be attributed to the data owner not applying the correct classification to the information. TelCo1 offered,

“I can actually put things in place to mitigate the risk of protecting data once we’ve identified it, but if it actually turns out that they told us this is low-risk data, it shouldn’t be treated as such as anything else, it turns out it’s really
sensitive high-level data, can’t be my problem because I can’t save everything."

An alternate way to address confusion around accountability in roles is to consolidate responsibilities into one security role, as TelCo1 says, “If you’re going to blame me anyway, then I’ll do it properly for you, and I’ll get the right people together, and we’ll have the right synergies and the right engagement model, to do it properly.”

Government organisations commonly took a highly structured approach to identifying information and classifying it, as FedGov2 said,

“we did a full audit of asset holdings, and we had the business owners, or the data owners, apply a score to the level of protection they believed that their data required, and then we went down to the information management layer and started looking at how we segment, how we structure, how we tag, label, and mark the data accordingly, to afford it a level of protection.”

FedGov2 advised to avoid problems with holding large amounts of information that had not been classified, and “the best way to do that is to have a really good strategy for how your business users actually generate the documentation in the first place.”

4.2.6 Information Location

To summarise this section, information can reside on paper and in employee’s brains as well as on computer servers, networks and databases. The three main areas to decide between for digital information location are internal, external but within Australia, and external anywhere in the world. Factors such as control and risk of leakage affect this decision.

Information is stored and used in many physical and logical locations in modern organisations. Global trends in disruptive technologies such as social media, cloud, and mobile devices have changed that way that organisations must now deal with
information storage. The convenience and proliferation of these ubiquitous services means that if organisations don’t take the time to consider their adoption, then employees will simply circumvent security measures by storing business information outside the organisation’s core systems. Information can be stored internally, externally, and overseas seamlessly. In an effort from employers to become part of the conversation, employees are being encouraged to share information internationally with known entities. TelCo1 offered,

“A real good example of that is the recent PM&C (Prime Minister and Cabinet) request to, where possible, do third-party interactions around your data management with five-eye countries (US, AUS, CAN, NZ, UK) preferably.”

Information can be stored on paper and in employee minds as well as on digital systems, which pose their own unique challenges for maintaining control over their location. FinCo4 sought to contain the location of information held in employee’s minds by reducing reliance on contractor resources, stating, “We … have a high level of internal technical knowledge, so we don’t see any need to take risks by using external experts.” ITCo1 sought to reduce reliance on paper-based systems by converting them to digital artefacts, stating “we’ve now scanned all our old paper records, and everything’s stored online … so every part of our business is electronic.” ResCo1 also sought to control the location of high value information, stating they use,

“a virtual data room-as-a-service, which means they have the ability to onboard, offboard people who have the ability to manage documents and do all the things like watermarking and making sure who printed it and have all sorts of controls”.

All organisations have information but only 15 from 25 of the research participants claimed to actively discover and identify all information. This number dropped further
when considering identification of information held on modern platforms such as social media, mobile devices, and cloud-based storage. StatGov1 confirmed that the boundaries of organisational information are often not clear, with,

“So, there's a bit of greyness around whether government data … can be stored outside of the state or country, … I mean everybody's using Salesforce. That's definitely not sitting in Australia.”

There are various reasons that organisations might decide not to host externally, such as loss of control, security concerns from country risk, and environmental concerns. EduCo1 confirmed, “The locality of that service organisation data centre might be … located in an area that might be impacted by environmental factors such as volcanoes.” PharmsCo1 supported this view with,

“data residency and sovereignty laws go a long way to constrain the problem. High-risk countries … We have had situations where we have had to end agreements with outsourcing partners due to the security concerns.”

A clear source of concern for many research participants was the reduction in control and increase in risk of information leakage should they outsource the storage of information to third-parties. One property of information is that it can be replicated an infinite number of times. If organisations store their information in an external environment, either cloud-based or in an outsourcing arrangement, then it is impossible to determine its physical or logical location. Although the organisation can confidently state its primary location, it cannot be sure that the information has not been backed up (copied) to an unknown location. It cannot be sure that the information has not been shared with an undisclosed third party. It also cannot be sure that the information has not been stored overseas. FedGov2 acknowledged,
“if it's sensitive and needs to be held within the confines of your geographical location or your country location, and then they don’t even consider, … simple things like where’s the data stored?”

ITCo2 also agreed, sharing

“One of the reasons why Amazon created a data centre in Sydney was because everybody was saying, we don’t want the Patriot Act to be enacted and find our data sucked away or locked up for whatever reason.”

ITCo2 continued with, “The difficulty … is how do you know that, even if it's on-shore, that it’s not being backed up somewhere off-shore?” Governments and other regulatory stakeholders are beginning to support the requirement for organisations to have increased control. PharmaCo1 shared,

“We want that information stored on hardened systems at a known location. In the case of personal identifiable information, there are also national and regional regulatory issues about data residency. For example, in Europe, European citizens’ data must remain in Europe.”

Cleverly, this uncertainty over loss of control has led some suppliers to capitalise on the situation by tailoring their telecommunications service offerings to allay these fears. TelCo2 shared,

“It's really a question of where the data is stored. … all of our data centres [are] onshore. Also, interestingly, our call centres are onshore. We have differentiated ourselves with our customers who … like what we offer: data security, data sovereignty, and also, a local service provider.

A variation on adopting cloud-based services is whether these services are provided on-premises or off-premises. Externally-owned ICT infrastructure supported by external contractors can be located internally within organisation-owned premises.
CHAPTER 4: FINDINGS – INFORMATION

FinCo1 gave an example, stating “we do workload in the cloud but storage on-premises so that we’ve got control of the data, and this has been going out for the workload and then brought back down.”

The motivation for adopting this confluence of internal and external platforms was to provide increased resilience within the organisation. ITCo4 that they took the time to create both environments,

“to have data portability so that if something happens inside the outsourced environment, they can potentially bring that data back into their on-premise environment, or some other service provider, and get it up and running again really quickly.”

Not all organisations had the freedom to make the decision about whether to adopt externally-based platform services or not. There were a range of conditions that precluded the use of externally-based locations for information storage and use. When asked whether regulatory compliance obligations could constrain their organisation from deciding to outsource, ITCo3 answered “Yes, data sovereignty requirements around privacy, GDPR, the Privacy Act.” FinCo4 identified that regulatory compliance was an issue, with “We have no appetite to upset our regulators and risk losing our licence, so we comply with any stipulations the regulator places on us, such as a policy of no cloud allowed.”

This dyadic choice between internal and external seemed to make little difference overall however, according to the research participants. EnerCo1 stated “It doesn’t matter whether it’s offshore or outsourced here, insourced, … it doesn’t make it any more secure. So, the actual location, as such, it doesn’t necessarily change the security of the information.” ITCo4 pragmatically considered that the adoption of security controls meant that their information-storage platform could be location-agnostic, with “I encrypt all of that data on-premises before it leaves, and then inside
the outsourced environment I’m only ever storing encrypted information.” One caveat to external locations being perceived as possessing similar risk to internal locations was if the external platform involved co-location of information in a shared, segmented environment, creating increased risk. ITCo3 identified that,

“one interesting aspect … is the contagion risk, or in fact, the collateral damage risk in my threat profile. If I’m outsourcing to an organisation that is also the outsourcer for very, very high-risk organisations, then, in a sense, I’m going to be taking on some of their risk as well.”

Information may reside on external locations when shared with other organisations for various reasons. ITCo4 confirmed “We do actually enable our employees to use those kinds of information sharing in a controlled way.” A good example was shared by ResCo1 which regularly engaged in mergers and acquisitions, with

“Most companies may not have a secure data room that is externally accessible and allows for collaboration. … It’s when it comes to … discussions between two or three parties, then you need to provide a common platform that all three can trust, as opposed to one person’s premises.”

4.2.7 Information Ownership

To summarise this section, information must have an owner, who remains accountable even if they decide to share the management of information with an outsourcing partner. This has implications for achieving trust in the partner through parity in management efforts.

Problems arise with accountability when organisations are not clear about who owns what information. Most mature organisations mandate that there are business owners for information and don’t assign blanket ownership to the IT department.
FedGov1 had historically not identified information owners and had recently sought to redress the situation, stating “the idea with the information asset owner piece was that we would identify who's the actual owner because at the moment IT owns everything.”

Being designated the owner of information carries responsibilities, as ResCo1 stated “All of the data that we have electronically, the data owner has responsibility for it. One of the responsibilities of being a data owner is to manage the life cycle of it.”

Organisations need to remain cognizant that sharing responsibility for managing the storage or use of information did not diminish their ultimate accountability for ownership of information. It was clear from the data that responsibility can be shared with other organisations, but accountability cannot. FinCo1 was emphatic when stating “You can’t outsource accountability. … Our customers won’t be satisfied with me saying, sorry, you’ve lost all your credit cards because PayPal didn’t hold onto it. That doesn’t wash.”

The question then becomes how do organisations trust external organisations to manage information on their behalf and the answer is “it takes a lot of work”, according to FinCo1, continuing

“Any partnering or sourcing that we do, we go in hard from a security perspective. So, we’ve got pretty robust third-party security risk assessment, and … we have a supply council that looks at anything of materiality to my organisation, … where they ask us whether we’re happy from a security perspective that all of the things that we would do for ourselves are being met by our partner.”

Equivalence is the key issue when building trust. The security framework and structures being used to protect information in an external organisation looking to share responsibility for managing information must be the same or better that what is
used internally. No organisation exists in a bubble; they all have suppliers, customers, regulators, staff, and board directors, and information needs to be shared appropriately but securely. This ecosystem of organisations sharing information with other organisations requires harmonisation of levels of quality in security efforts. FinCo1 was pleased to report

“we’re seeing … anyone who wants to do business with us is asking us the same questions about our security. So that’s good. That shows the industry is understanding that no organisation is an island.”

The level of complexity goes up in organisations looking to outsource whole business processes not just discrete sources of information. FinCo1 shared it

“gets pretty tough sometimes, when there’s big, multibillion dollar deals that the business is thinking to … save a whole lot of money by sourcing this function to a partner. And we’re going, yeah, but you need to make sure you spend the right money up front from the security perspective because … our customers don’t care that we weren’t running the service.”

FinCo3 agreed about the complexity, stating

“there’s a spectrum. So, if you’re an application owner, you own a material business application, then yes, you would be very aware of the level of sensitivity of your application, and therefore, the obligations required of you. If you are, for example, the data owner of a single document, for example, much of my email, then you would be less aware because of the lower criticality of the individual elements.”

4.2.8 Information Summary

Information may be stored on many different platforms in different locations and Figure 4.1 summarises the ICT infrastructure commonly used to store information of
various sensitivities. Not only can contractors be used to manage infrastructure, but they can be used to either fully or partially manage information as well, although contractors are not used to manage trade secrets.

![Image: Summary of Common Platforms Used for Storing Information](image_url)

Figure 4.1. Summary of Common Platforms Used for Storing Information

The six service offerings identified in Figure 4.1 are as follows:

1. Professional and managed services onsite
2. Managed services for dedicated infrastructure onsite
3. Professional and managed services off-site
4. Managed services for dedicated infrastructure off-site
5. Managed services for shared segmented off-site
6. Professional services on public cloud

4.3 Chapter Summary

This chapter describes the findings from analysis of the data, providing a rich description of the concept of information security strategy, analysed for its properties.
and dimensions, noting any variations throughout. After the data were analysed, related analyses were aggregated into categories, which were integrated and then interpreted in relation to the overall research question.
Chapter 5:  Findings – Organisational Context

Continuing on from the findings about information owned and used by an organisation, this chapter describes findings about the external and internal context which affects the organisation. These contextual factors have a bearing on decisions that are made about the security of information.

5.1 Chapter Aim

The aim of this chapter is to describe the findings after analysis of the data, providing a rich description of the concept of information security strategy, analysed for its properties and dimensions, noting any variations throughout. After the data were analysed, the analyses are aggregated into categories, integrated, and interpreted in relation to the overall research question.

5.2 Organisational Context

There are three discrete categories of concepts that relate to the storage and use of organisational information. They are broadly labelled organisational conditions, outsourcing constraints, and outsourcing enablers. These three categories each contain a set of concepts with their properties and dimensions. Organisational conditions are those factors that describe the strategic and operational level aspects of an organisation that relate to information security. They include the organisation’s vision and mission, goals, governance structures, information resources, capabilities and performance. Outsourcing constraints are the conditions originating either externally or internally that affect an organisation’s ability to engage in outsourcing. Their existence may have an enormous effect on decisions made both in the director’s boardroom and operationally by management and staff. Outsourcing
enablers also have an enormous effect, as often outsourcing decision cannot be made without them.

5.2.1 Organisation

To summarise this section, organisations have various properties with dimensions, including goals and assets. Goals and assets combined affect strategic decisions.

The characteristics of an organisation affects decisions made within it, so this section begins with an examination of the organisation itself. The following section examines the concept Organisation and includes concepts that relate to the various properties of an organisation. Where possible, variations of these concepts and any property or dimensions are also analysed and described. There are eight key concepts analysed and described in the following sections, which are organisational goals, organisational strategy, governance structures over strategic, operational and tactical levels, platforms that support information, decision on whether to outsource, decision on whether to hold valuable information, information security, and organisational resources.

A number of these concepts, for example organisational goals or organisational strategy, are important because they affect how the organisation decides to approach its information, including storage, use and security. A positive relationship will be termed P4a and a negative relationship will be termed P4b in Figure 7.2.

There are two more concepts that relate to Organisation, which are Information and Strategic Impacts on Organisations, but these are core to this research and are described in their own sections. There are three more concepts that relate to a decision on whether to outsource, which are Outsourcing Constraints, Outsourcing Enablers, and Outsourcing Benefits. Constraints and enablers are described in the sections following Organisation, and benefits are described in the Strategic Impacts on Organisations section.
5.2.1.1 Goals

StatGov1, being a not-for-profit organisation, was focussed on improving customer satisfaction. Interestingly, StatGov1 saw increasing information security as a way to achieve that, commenting,

“Our goal is to drive cost down for our customers rather than make money for ourselves, and if we generate a surplus, … that surplus is turned into reduced prices, investing in new products, new services, beefing up our security, literally. Seriously, that's $6 million that's being used over the next three years for our very significant security uplift program.”

When questioned about what the goal of information security was, research participants sometimes stated the obvious, which was the goal is to keep information secure. AvCo1 for example, stated “the goal of information security in an organisation is, obviously, the CIA, confidentiality, integrity, and availability of information assets. That's the key goal.”

Goals often interrelated and supported each other however. Interestingly, the goal of information security was not always viewed however as simply keeping information secure. In a variation of this concept, the goal of information security was sometimes perceived as supporting the organisation in achieving its organisational goals. FinCo1 stated that their primary information security goal was to keep the organisation secure, so that it could pursue its organisation goal of improving customer satisfaction, commenting “the simple plan for us is to keep our organisation safe, and our organisation is our customers and ourselves”. FinCo2 added that the goal of information security was to “protect the operation of the organisation. Make sure the organisation is able to operate safely”. ITCo4 commented “The goal of information security is to enable the business to achieve its outcomes in a secure and managed way.” MgtCo1 agreed with “Goal of information security for us, I would
say, is to make sure that the business is able to do business in a more secure manner.” MgtCo2 thought the goal of information security was “to help the organisation accelerate its growth in a secure manner.”

Organisations instead sometimes viewed keeping information secure as the goal of implementing security controls. ITCo4 offered “the goal of security controls is to be able to technically implement control over the information that you are going to produce, generate, disseminate, and store in various locations.”

5.2.1.2 Strategy

To begin with, most organisations articulated their goals through their vision (externally-focussed) and mission (internally-focussed). The vision and mission then shaped the (typically five-year) business strategy. The business strategy was actioned using three-year corporate strategies and annual business plans. FedGov1 shared “We have a business strategy, then we have a business plan. The business plan’s pretty much the yearly budget type of thing.”

Sometimes divisions within the organisation were granted the freedom to articulate a version of the overall business strategy that was more applicable to them. FinCo2 stated “We have a top-level business strategy document which is then socialised across our entire organisation, and then each business unit underneath that top-level umbrella has their own strategies.” FinCo3 added “we have several layers of business strategy documents given the scale of our business.”

In a cascading approach, the business strategy then drove the IT strategy. FedGov2 stated they have a “strategy from a business perspective. There are elements of our IT strategy in that document, but we also have a separate standalone ICT strategy.”

An organisation’s IT strategy then drove their information security strategy. StatGov3 shared they have “a corporate plan, … then we have an IT strategy, then we have a
cyber security strategy, which is referred to in the IT strategy.” FinCo4 stated “We take the approach of cascading strategies, where a business strategy gets set first, then an IT strategy gets set, followed by an information security strategy.” EduCo1 summed up the three levels with,

“We have a corporate strategy, business strategy document. We have an information technology strategy that supports that business direction, and we have an information security strategy that aligns to the information technology strategy which supports the business strategy direction.”

In a variation on this concept, some organisation’s business strategy drove their information security strategy, which then drove their IT strategy. PharmaCo1 stated “we have a business strategy document that’s done by our strategy committee, which is senior leadership, but I also have a security strategy document that is mapped to that business strategy.”

The order of cascading strategies had implications for responsibilities and the human resource organisational chart structure. FinCo1 believed that business should drive IT, which then drives security, and has a lot of experience with “where you sit in on the org chart and what’s your relationship with the [Chief Information Officer]. I could talk for hours about what works and what doesn’t work and why our setup’s better than other organisations.”

5.2.1.3 Governance Structures

Ultimately the attention and support of the board of directors and CEO is required because they are accountable for organisational outcomes including security of information. StatGov1 (a CEO) shared “I'm accountable for everything that takes place in the organisation, so in that sense I'm accountable for information security within the organisation.” ITC01 (a CEO) agreed, stating “As head of the business, I'm ultimately … accountable to our clients. … I don't actually have anyone with
delegated authority for it, so ultimate authority would rest with me.” If a CEO identifies a material risk within the organisation, then it is incumbent on them to bring that risk to the attention of the board. StatGov1 related

“I’ll be taking [a contract] to the board in January because there are some risks associated with that contract that we simply cannot mitigate … I’d be taking that kind of thing to the board to say here’s a risk that I’m gonna be willing to sign off. What do you think guys? And we’ll see.”

Organisations use hierarchical structures to provide information security governance. FedGov1 shared “It’s a reporting function up to our Risk and Audit Committee” StatGov1 stated “The audit and risk committee would be interested from an information security perspective, and they report to the board. They’re a subcommittee of the board.” StatGov1 then continued “they probably do have a dotted line to me”

There are several levels that exist within organisations, which begin with strategic at the top, operational in the middle, and tactical at the bottom. Levels can also be split, for example business strategy can apply to the organisation as a whole and also to individual divisions within the organisation. FedGov1 aligned levels to the strategies that they were responsible for, stating,

“There’s a number of different levels of cyber security governance within this particular organisation. The tier one level is currently held by ASD, the Australian Signals Directorate. The tier one is responsible for whole of government and policy setting. And then I’m down at tier two where I manage the operational ICT security for my particular department.”

Similar to the cascading levels of strategy, accountability and responsibility for programs of work are also relevant at various levels. In a description moving from the security program upwards, StatGov2 stated “So the whole security program … has to
be linked with the IT program, and then it has to be linked with the business criticality, what the business wants.”

Some research participants had security strategies, not just business strategies, that aligned to various levels within their organisation, including at the highest level. FedGov1 continued with,

“Our general governance is driven through Attorney General’s department who publish the PSPF, the Protective Security Policy Framework, and from that framework, it flows down to ASD, who then publishes the Information Security Manual. That Information Security Manual is a principles-based document which articulates a whole bunch of strategies and controls under which we implement our ICT security regime. I guess, in a way, those two high level governance publications are our IT security management framework.”

The board and CEO then extend responsibility by sharing it with the next level down, to executives and management within the organisation. FedGov1 stated,

“there are also some governance functions that we have internally. We have an information governance and assurance group which I chair, and underneath that we also have some working groups that do things like information awareness, … and policy development as well.”

Strategy and risk are inextricably interrelated. Taking a risk-based approach is a key concept where decisions are made within a defined, formal risk management framework over multiple levels to implement the strategic plan. The first activity for the board of directors was to set the organisation’s risk appetite. Then the board sets the structures within the organisation for undertaking risk management. The board then sets reporting lines and engages in active monitoring of operations. FinCo1 illustrated their approach to governing risk-based decisions by stating that decisions,
“are usually made by an executive, depending on the appetite. So, if it goes outside the appetite set by the board, it has to go to the board, and then from the CEO and the executive leadership team have another level of delegation and it comes down. Some decisions from my own sourcing, for example, I can make myself, and then depending on the materiality, the higher it goes.”

Policy is another way that boards can govern actions within an organisation. The board can use policies to provide boundaries and procedures for employees, and repeated actions in turn shape culture. As an example, ITCo1 shared their governance experience being shaped by their employee termination policy, with

“When someone leaves our company, we have a process for exiting and taking them off all the systems they have access to. ... I make sure that everyone's actually been pulled off and followed back out, just so we don't have anyone left around getting access to something that they shouldn't.”

The board can affect information security by using a corporate information security policy, as a tool to communicate with and direct management activities in the organisation. Two-way communication is then required back from management to report to the board and executive on progress. StatGov1 shared “I either sign off or present all policies that apply to the organisation. By present, I mean to the board for approval depending on whether or not it's a board-level policy.”, continuing “I don't think information security policy would be something the board would sign off on. It'd probably be me. ... That's it in terms of accountability.”

Governance became difficult when outsourcing business functions to external supplier organisations. Customers for example rely on organisations to safeguard their personal information when buying from them and have no visibility into supplier agreements that the organisation might engage in where their information might be exposed. As FinCo2 stated, “The customer doesn't care that it wasn't this
organisation that lost their data. They trusted this organisation, not the third party.”

MgtCo2 agreed, stating “it doesn’t matter if it’s stored within … their systems, or if it’s outsourced into other systems. The accountability of securing that information is still back into that organisation.” EduCo1 summed up with

“I’m still accountable. … I am engaging the third-party to be able to store that credit card information. So, at the end of the day, I’m still accountable … to the customer, while the third-party is responsible to me to ensure good protection of that information.”

5.2.1.4 Information Platform

An information resource has previously been defined as a receptacle that holds information (Denning, 1999). This definition conflicts with the data from this research however which views an information resource or asset as a business resource used by an organisation towards achieving its vision and mission. AvCo1 was very conscious of this, stating “there’s a good degree of information assets across the company that, if our competitors were to get access to that, would compromise us.” FedGov2 took the time to identify these resources, stating “We’ve done a whole bunch of work on modelling our high value information assets. That includes … our general business management systems.”

Information turns into a resource when security controls are applied to it, so that it becomes ‘ruggedised’ and durable. In its durable state, it can be relied upon to provide utility for the organisation towards the achievement of its goals for many years to come. Without security controls being applied to protect information, it can degrade in value, lowering the potential for it to be used a resource by the organisation. FedGov2 used an example of their public website to illustrate, with

“we have a rather large public-facing presence for a number of different reasons, recruiting information, interaction with business, business to
government, etc. ... We have tools that we’ve developed to maintain the integrity of our external facing websites. If they ever get compromised or defaced, then they get taken back to a last known good state immediately, ... And we’re very heavily engaged in ensuring that that public presence is maintained in a good state.”

Many receptacles support or hold information, which can include servers, databases, networks, paper and cognitive media (employee’s brains) (Ahmad et al., 2005). All these platforms can be internal or external to an organisation, as TelCo1 noted “people don’t get the fact that data can be stored on different hard drives and offshore, onshore, and whatever else.” The type of platform, its conceptualisation and classification, informs the type of security controls that are used to protect the information. ResCo1 articulated the main platforms and gave an example, with

“For example, if it is digital, my remit is predominantly only for digital data, not hard copies, physical data, so the levels of controls, whether we want to do encryption, whether it’s stored in a certain place, we have repositories that are allowed, specifically based on classification.”

Cloud-based storage was a concept that many research participants were concerned about. Interestingly, the choice of cloud-based platform was important to them. For example, Dropbox was not popular amongst the research participants, and Google Drive or Microsoft OneDrive were the preferred options instead. FedGov1 stated “we're very concerned about Dropbox”, ITCo1 stated “We don't have any business Dropbox deliberately … because it's insecure”, and FedGov2 stated “We don't allow instances of … Dropbox” When asked about their use of cloud-based storage, StatGov1 answered “Not personal Dropbox, but corporate cloud, yes … OneDrive.” RetCo1 stated “we use the Google Drive platform extensively … and they
[employees] can access it from anywhere in the world" and FedGov1 uses “OneDrive [to] provide a much more protected environment.”

Additional security controls were often implemented to supplement the standard security controls associated with the cloud-based storage, as FinCo1 shared “We’ve got visibility all the way to cloud-based storage [using] CASB (Cloud Access Security Broker) solutions” and MgtCo1 shared “We do monitor cloud monitoring in place, like … CASB and a Data Loss Prevention.” When asked about protecting cloud-based information, ITCo4 shared “we enforce protection of the information, [using] encryption, rights management.” As well as technical controls, policies were used to restrict the use of cloud-based storage, as StatGov3 stated “it definitely would be against policy” and TelCo2 stated “we have policies on that.”

Protection of information stored on mobile devices can be problematic and is affected by an organisation’s policies (typically a Bring Your Own Device policy) and technical security controls. FedGov1 confirmed “our organisation-issued mobile devices are all protected, but we do have issues with people bringing in their own” Organisations often protect business information held on mobile devices, whether the devices were organisation-owned or employee-owned, by taking full control of the device when it was being used for work purposes, as FinCo3 stated “the personal devices that are BYOD [bring-your-own-device]… we take full control over”. Modern technical security solutions include mobile device management products that can fully segregate organisational information from personal information, as FinCo2 shared

“The tools and the mechanisms we use for distributing data out to mobiles means that when it goes out to a mobile, it’s actually held within a secure enclave. It can’t actually be stored on the device outside of the protected environment that we manage on the device.”
Relying on mobile device management technical products is not a perfect approach however, as information can be displayed on screen and recorded using a separate video or photographic recording device, and ITCo2 confirmed “I would propose that it’s all, broadly speaking, pretty highly ineffective.”

Organisations restrict sensitive business information being held on social media platforms. As MgtCo2 confirmed, “Most organisations are quite aware of the social media challenges to their information assets.” ResCo1 took active steps to address this challenge, stating “part of our cyber intelligence program ... looks at external platforms where the company’s material is – ... the goal is to look for leaked information.” As an example of information being inappropriately shared on social media, FinCo1 perceived that disclosing certain details about the type of financial systems that some of their employees worked on created vulnerabilities, so mitigated the risk of a targeted attack by sanitising sensitive information on public-facing social media platforms, stating

“I'll give you an example. In the wake of the SWIFT breach in the Bangladesh Bank, there was increased awareness around people across the world being targeted for understanding or working in SWIFT environments. So that's when we go through social media and LinkedIn and find anyone in our organisation that works, or purports to have worked with SWIFT, and we go through and work around what that means and help them with that.”

AvCo1 took a preventative approach by educating employees on the risks of posting sensitive information on social media, stating “A lot of our education ... focuses on what we share on social media platforms, of risks in terms of what could exploit the company.” FinCo1 shared that monitoring of organisational information on social media platforms did not only occur sporadically in response to a threat, but regularly
in a preventative practice, stating “we have a full-time social media team that look out for the other stuff as well. We can feed some security stuff into there.”

Most research participants were either monitoring social media for sensitive information or planning to begin soon. StatGov2 offered “No, we haven’t started [monitoring social media], but we are thinking of doing that.” In a unique variation of this concept, ITCo4 was within its rights to monitor social media platforms for sensitive information but chose not to, stating

“Lots of information is published in social media, but as a general rule or modus operandi, we don’t monitor social media accounts of our employees. For business intelligence or other purposes, that would be considered an invasion of privacy and wouldn’t be appropriate, even though it actually is within the contract that you sign with my organisation when you get employed to say that you potentially could have your social media accounts monitored for the purposes of protecting the business.”

ITCo1 was conscious of one of the properties of paper being that it can degrade over time, affecting its availability and integrity, stating “we’ve now scanned all our old paper records, and everything’s stored online … and as a consequence, it doesn’t degrade.”

5.2.1.5 Decision to Hold Valuable Information

Organisation may take an active approach to deciding whether to hold valuable information internally or not. FedGov2 offered “it’s around setting your information strategy about what’s the important data, what are your high-value assets, and how much do you want to protect them?” FedGov2 continued

“what businesses need to do is … understand the risk of that [valuable] data being released into the public domain or compromised, and that's where they
can start to make informed decisions about … whether or not that data's now able to be lowered in sensitivity.”

StatGov1 gave an example on why organisations might not choose to hold valuable information, with

“\textit{I've reviewed all of my own files to determine if there was anything there that related to third-party information, which we've got a policy around not storing in a cloud environment without the authority of the person we've collected it from, or anything that was particularly sensitive. Not that I'm afraid of security in the cloud, but it seemed easier just to move it or delete it.}”

ITCo1 also decided not to hold valuable information, stating

“\textit{we've taken the deliberate approach of devaluing the information that we have. What I mean is, by taking away the risk, taking away the importance, taking away the impact … we don't keep a lot of valuable information.}”

Sometimes the decision on whether to hold valuable information was not one that could be taken by the senior security executive and escalation of approval is required. TelCo1 shared

“I send it up the tree, the Chief Legal Counsel and the CEO would both have the power of veto, as would the board. But ultimately, I don't expect them to know … all of the issues that would impact on that decision. They would expect me to actually come up with a recommendation and justify why.”

\section*{5.2.1.6 Decision on Whether to Outsource}

Different definitions of outsourcing are apparent and affect an understanding of the concept. Depending on the research participant, outsourcing could mean simply
using cloud-based infrastructure through to outsourcing entire business functions to business process outsourcing suppliers. RetCo1 began with

“You need to be very clear about what you mean by outsource … for me, outsourcing is I go to somebody and say manage my environment on my behalf. Outsourcing is not going to the cloud. Cloud is just a different hosting platform.”

However, there are different definitions of outsourcing used by research participants, which causes conflict and confusion. EduCo2 “I have a very broad definition that ranges from the more traditional managed services style of outsourcing through to … moving to the cloud as a form of outsourcing.” FinCo3 stated that

“For me, I’d probably default to something like the CPS 231 definition, which is where a material business activity is undertaken by a third party on your behalf, where either you have a business activity which you would otherwise have to do being completed by a service provider, and then, there’s a reasonable amount of debate about whether you include resource augmentation in outsourcing.”

In examining the APRA CPS 231 document to cross-reference, the exact definition of outsourcing used there was

“‘Outsourcing’ involves an APRA-regulated institution, or an institution within a group that is not an APRA-regulated institution, entering into an arrangement with another party (including a related body corporate) to perform, on a continuing basis, a business activity that currently is, or could be, undertaken by the institution itself.”

The APRA CPS 231 document also provided a definition of offshoring, with
“For the purposes of this Prudential Standard, ‘offshoring’ means the outsourcing by an APRA-regulated institution of a material business activity associated with its Australian business to a service provider where the outsourced activity is to be conducted outside Australia. Offshoring includes arrangements where the service provider is incorporated in Australia, but the physical location of the outsourced activity is outside Australia. Offshoring does not include arrangements where the physical location of an outsourced activity is within Australia but the service provider is not incorporated in Australia.”

On offshoring, TelCo2 understood organisational decisions about whether to outsource versus a desire to maintain control over their information, sharing “we are passionate about data jurisdiction and the exposure of having sensitive data stored offshore”, continuing “we’re always mindful of the Patriot Act and … in today’s day and age, … unless you absolutely know where your data is at any time, you cannot be absolutely sure how secure it is.” For ResCo1, this obfuscation of information location and lack of ability to maintain close control would preclude them from outsourcing valuable information, illustrating with

“We would take a risk for little or no value information … But if it’s highly-sensitive information, merger/demmer, board level strategy documents, then it will have to go into a very special repository where we have management control or visibility.”

Organisations manage conflicting priorities when deciding how to outsource the storage of information whilst remaining secure. StatGov1 shared their conflict, stating “we insource, although we’re starting to play in the cloud. … we’re … deciding how we do that in a way that allows us to comply with legislation around privacy.”
Organisations need to remain cognizant about what their core competencies are and what their informational needs are to support these competencies. There is a prevailing view that information used to support these core competencies should not be outsourced due to the loss of control and potential negative strategic impact on organisational success. When asked about the conditions that might prevent outsourcing some information-based business functions, ITCo1 answered “there's a lot of reasons you wouldn't put some things out. One of the main reasons would be it's a core competency … You don't outsource some things.”

Any decision to outsource requires careful preparation and due diligence checks, especially from the security perspective on the informational aspects. FinCo1 confirmed “Any partnering or sourcing that we do, we go in hard from a security perspective … we’ve got pretty robust third-party security risk assessment.” Organisations also need to assess exactly what they're considering outsourcing, as an IT system often includes the application, middleware platform, physical infrastructure and database, where some components can be separated for outsourcing and some can't. FinCo1 considered

“We’ve never gone … we want to outsource the database. We’ve gone, we’re going to outsource this application which has this database, and then the conversation is where should we store the data? What controls should we put around it? Is it the partner? Is it on premise?”

When making the decision on whether to outsource or not, organisations often took a risk-based approach and considered the future effects of a security breach in the event the information was compromised or disclosed. When asked about the decision to outsource or not, ITCo2 stated “I think it all boils down to simple questions like would it be problematic … Would it cause you harm if this information were made public?” AvCo1 also had considered the future effects of a security breach and the
impact that might have on an outsourcing arrangement, stating “if the database of information about our customers … should be compromised, then [that] would be catastrophic.” Although a mature user of outsourced services, when asked about whether their highly-valuable customer database resided on outsourced infrastructure, AvCo1 replied “No, that doesn’t. That particular one, no.”

In a variation on the level of effort expended in making the decision about whether to outsource or not, EduCo2 was more relaxed, stating,

> “I’m reasonably sanguine about what information goes out … because, typically, the degree of security they can bring to their data centres is better than we can achieve ourselves just because of their scale.”

Organisational decisions on whether to outsource are affected by a large range of constraints and enablers, to gain the advantage of several potential benefits, and these concepts are discussed in other sections.

### 5.2.1.7 Information Security

This section reports on findings about the concept of an organisation engaging in information security practices to protect its information. Key concepts within information security are origination and direction of the drive to secure information, the motivation for same, the influence of security leadership, and key areas of information security controls such as risk management, security culture, security education, training and awareness, security policies and technological controls.

One key property of organisations is their ability to conduct effective information security, with dimensions ranging from ineffective to effective. Information can never be perfectly secure due to the existence of unknown threats. Zero-day exploits, which are newly-discovered vulnerabilities that could be used to conduct an attack, serve to highlight the existence of unknown persistent threats. An organisation’s inability to
perfectly convert unknown threats into known threats affects confidence levels in its security leaders, and TelCo1 believed organisations need to take a pragmatic approach to balancing security needs with business decisions, explaining “Take a balanced approach on a commercial basis … you can’t be a security purist because you might as well shut the shop and lock the doors and walk away.”

When moving towards the goal of achieving the best state of information security that they can, organisations naturally seek to understand where they are now, so they can improve their posture based on gap analysis towards a desired future state. Measuring information security at the strategic level however was perceived as problematic. The reason for this is because of the uncertainty around effectiveness of operational security controls to counter threats, due to the unknown nature of threats. If the number of security attacks detected at an operational level suddenly increases, organisations are unsure whether that was because their detection tools have become more effective at turning unknown threats into known threats, or because the volume of external threats has increased. This measurement problem was exacerbated when attempting to measure information security at the strategic level not the operational level below it. On strategic measurement of information security, FinCo2 agreed “It’s a difficult question. There’s no single silver bullet.” To collaborate using a dashboard with metrics, some of the research participants used the US National Institute of Standards and Technology framework to guide security measurements, as ITCo3 commented,

“It’s a very challenging question. Most of the metrics are pretty bad. The reason being that there’s no direct correlation between the amount you can spend and the likelihood of getting hacked. So, you end up with a lot of quantitative numbers that don’t really tell you anything … we generally will use a [US National Institute of Standards and Technology] cyber security
framework, identify, protect, detect, respond, and recover, and come up with scores for each of those domains."

The main problem with information security in organisations is the uncertainty about whether threats will eventuate into security breaches or not. This then causes other problems such as deciding how much budget to allocate towards information security programs. The only rational action available to date is to assess known threats, understand the location and value of their information, and implement security controls to prevent and respond to known threats in a manner consistent with the value of information held. When threats eventuate into successful security breaches, in spite of large security budgets, organisations have been left without the language to explain why the breach occurred.

Threats are mostly known so can be prevented, but there are some threats that are unknown. Information is generally stored in known repositories within the organisation however some valuable information is unknowingly stored together with non-valuable information, making it vulnerable. Finally, security controls are generally selected and implemented according to sound heuristics and frameworks, however their effectiveness is unknown, given threat actors routinely impair their functionality. So, some threats are unknown, some valuable information is unknown, and the effectiveness of security controls is unknown. These three areas of uncertainty combined make it impossible for information security to be completely effective. ITCo3 continued with an example serving to highlight the problem with measuring information security, stating,

“As an example, people often bandy around spam numbers. We blocked 600 email-based attacks this month, and then next month you say we blocked 700 attacks this month. Great, is that a good trend, or is that a bad trend? Then the next month you block 400 attacks. Does that mean you’re blocking fewer
attacks or there were fewer attacks and you blocked just as many of them? And is that something that you’ve actually affected, or is that just a random variation in attackers going after whoever they’re going after?”

The volume of unknown threat vectors might be small but they’re still there. Therefore, organisations cannot claim to have 100% protected their information. The clear majority of potential attacks can be identified so preventative security controls can be implemented to mitigate the risk of an attack. FedGov3 confirmed “these days, you can never know whether something is completely safe or not, but you can have a clear indication.”

There were other ways for organisations to measure their information security at a strategic level. These included benchmarking themselves against industry competitors, tracking successful breaches, and monitoring process maturity levels in discrete areas of information security. StatGov3 conducts a “a bit of benchmarking”, and also measures “incidents, like near-misses and actual incidents, and you would be hoping that they would be coming down.” StatGov2 revealed,

“we have used … maturity measuring for our … information security processes, and the state government digital information security policy has over 12 parameters by on which we have to report on our maturity of those processes.”

The significance of the problem with measuring information security at the strategic level is that without measuring information security, a commensurate security budget cannot be appropriately allocated. StatGov3 commented “I think CISOs or cyber security people have to be able to communicate a good story to the board.” This was highlighted by EnerCo1, who quoted a board director he had met recently who stated, “the problem we have about security is no board of directors actually knows … what [monetary amount] we should be spending.”
By their very nature, most security professionals perceive that they must maintain control over the organisational environment to work towards preventing adverse outcomes. In a variation on this concept however, TelCo1 put the security framework in place to support good decisions being made by business people but did not attempt to control responsibility for outcomes, explaining,

“I don’t own the problem. Too many [people] in security think the world is going to fall on their head if something bad happens after they’ve called something out. Well, I’m totally the other way. Here’s all the information you need to make the decision. Here’s my recommendation. It’s your call.”

TelCo1 always made this transfer of control over outcomes explicit however, by collecting a signature on a Delegation of Risk form from the business person overriding the security recommendation, with TelCo1 declaring “I will not sign off on the delegation of risk. That’s how you survive long term in these jobs.”

Transparency and respect for the authority of business executives to make business decisions is key. If security professionals impede the operational decisions of the business people in their organisation, then the business people often procure software-as-a-service IT products and services without informing the IT department or security function, in a procurement model known as shadow-IT. TelCo1 stated,

“If you run around and make it really hard for people to do business … they go around you. They run projects without having you give advice and do a risk assessment. That’s even riskier because when you don’t know about it, you haven’t been involved and something bad happens, then it is your fault because you should have been across it.”
5.2.1.7.1 Origination and Direction of Motivation

A key property of organisational information security is the origination and direction of the motivation to improve security, with the two dimensions being top-down and bottom-up. The two opposing dimensions had various levels of support from within the research participants, with 14 research participants stating top-down, three stating bottom-up, and eight participants stating both. The reasons for top-down included the senior leaders, who were accountable for security within their organisations, being risk-adverse. FedGov1 stated “It’s the executives and the boards who are trying to push it down, and we’re reasonably risk-adverse because we’re a regulator.” An increasing number and severity of sanctions being imposed in the event of a security breach was also helping to motivate organisational leaders. ITCo3 recognised this, stating, “As much as anything, it’s about the board trying to protect themselves as protect the organisation.” Some research participants recognised that motivation had changed over time, where IT staff had identified key security risks some time ago but in modern times, risks to organisations were becoming more publicised, so leaders were taking more interest. ITCo2 stated

“It used to be, 10 years ago, bubbled up from IT, but now there are enough examples of where people have been decimated because of [security breaches] that, … with mandatory data breach notification laws happening here, you now have boards who are starting to say, are we legally liable? The last thing they want is be legally liable.”

AvCo1 agreed, stating,

“the boards have a duty of care and are accountable, ultimately, so they are driving change as well. We’re definitely seeing a shift, whereas I think you go back 10 years, for example, it would have been the technology team saying we’ve got a technical vulnerability that we need to close, and if we don’t, it will
be impacting in some way. I think it has definitely changed, changing to more of business discussion.”

One reason for a bottom-up approach was a lack of accountability in senior levels within the organisation which left the burden of compliance on the lower ranks. FedGov2 commented “you generally end up ... with a bottom up push because everything flows down to the point where you implement systems and controls, and they're pushed from the bottom up.” FedGov2 continued,

“How do you change that dynamic? You make people accountable. ... Give [senior people] the role of being the risk steward or the risk owner, and you make them responsible for accepting the risk of things happening below them in their business space.”

TelCo1 agreed with a bottom-up direction but for a different reason, believing a good security culture should mean that “security is everyone’s responsibility”, continuing “Bottom line is, the guy on the factory floor, the girl at the front desk ... it’s their responsibility to be asking us to drive the decision around security.”

The reasons for both directions were that boards are often uncomfortable with having to accept extreme levels of risk, and staff are closer to the action allowing them to spot deficiencies in security more easily. FinCo2 summed up with,

“The board is pushing down for treatment of risk. Regulators are pushing to see that a good standard of practice is applied, and risks are under control, under management. Staff very often do identify the gaps and issues and raise those for awareness, so they can be addressed, whether it’s localised or systemic.”

The maturity of organisations when addressing information security was another reason that both directions of motivation may be found. If the board of directors is
sufficiently skilled and experienced in information security, then they propagate
security strategy and security policies more effectively within their organisations,
whereas if they are not, then they are dependent on staff to report issues up to them.
ITCo4 confirmed,

“The organisations that are well-advanced and quite mature in this tend to
find that their boards and their executives are fully across and aware of
security. For organisations that are much less mature, or are just branching
into this, or are just starting to get it, what you'll see is that it's actually the IT
team or the IT security team that’s pushing for the implementation of security,
and they're having to put up business cases and arguments to the executive
on why they should invest in security. So, in a lot of cases, it just depends on
the maturity of the organisation.”

5.2.1.7.2 Security Leader

The research participants in this study all had a sense that they were responsible or
accountable for information security within their organisations. ITCo1 stated “anything
with information security ultimately involves me. I'd be the ultimate decision maker.”
StatGov1 also added “I've got responsibility for security within my own organisation …
and secondly, I've got responsibility for security around the services that we offer
to our customer base.” FedGov2, as a security leader within his organisation, was
required to set strategy as part of the role, stating “I'm engaged in the upper tiers of
the strategic direction setting for ICT security, having recently been a co-author and
publisher of my organisation’s ICT Security Strategy.” EnerCo1 went one step further
by not only setting the strategy but managing its operational implementation, being
responsible for “everything from building the strategy, implementing the strategy,
updates to the board (six monthly), … audit committee, general board, and the
executive team.”
In large and complex organisations with multiple divisions, each division may have a different risk appetite, which all need to be considered within the context of setting one information security strategy. AvCo1 explained,

“I'm responsible for the overall strategy, at group level, for my organisation, looking after three distinct businesses in the operational environment which are all very different in terms of their risk appetite. My role is to pull together a group security transformation program, … developing policy, key controls, … strategy and architecture, business engagement and awareness, … security operations, and … security programs.”

Maintaining relationships with key stakeholder groups was a recurring theme when analysing security leadership. RetCo1 named a few, with

“Ultimately, the whole information security strategy for my organisation rests on my shoulders, so everything to do with the 12, 24, 36-month planning is my remit. If you talk about what it means, strategic level information security, to each of the group executives and the board, I’d report to the risk manager on a quarterly basis around our security program and how it works and what we’re doing in that space.”

5.2.1.7.3 Risk Appetite and Management

By way of an introduction, this section analyses the concept of risk appetite within organisations and its properties. This section does not analyse how risk appetite can affect business decisions within organisations as this discussion is left to the Outsourcing Constraints section. This section also reports on findings from the data on risk management and its relationship to risk appetite.

Most organisations would have their board of directors or equivalent define a risk appetite so that operational teams can then make decisions within a risk
management framework, providing proper governance and reporting. StatGov1 stated “risk appetite guides all of the decision making that you do in running a business”, continuing with an example of “your risk appetite would guide the choice of [outsource] providers.” ResCo1 clarified the components of a risk appetite, stating, “we look at financial, productivity, as in operational impact, … brand and reputation together, health and safety is another one.”

The risk appetite then guides operational decisions, including major ones, as FinCo1 stated

“in my organisation, there’s always a big focus on risk appetite. Every time we make a sourcing decision, we do a materiality assessment. We do an impact around appetite, and we decide whether it’s in appetite. We cover country risk. We cover service risk. We cover data risk, so that’s quite a mature process.”

As well as guiding the direction of major decisions, the risk appetite guides appropriate accountability for ownership over these decisions, as FinCo2 stated,

“risk appetite drives us to focus on risk reduction to an acceptable level. We have very well-defined risk appetite statement, and … if the risk can be managed down to a medium level … risk according to the rules for risk definition, then the local business unit can decide whether to accept the risk or not … but if we find that … it can only get down to a high or an extreme risk rating … then needs to be raised to … an executive operating risk committee, to decide if that’s an acceptable risk or not.”

In a variation of this concept, although a common approach was for boards to define a risk appetite so that organisational subdivisions could then make business decisions based on risk versus reward, it is hard for these units to quantify the
boundaries of the risk appetite. ITCo3 saw issues with measuring risk appetite so that decision could be made within its boundaries, stating,

“Risk appetite is a phrase that gets used a lot, but when you actually push people on what it means, there is ... virtually no ability to actually quantify what risk appetite is. Risk appetite makes sense in an insurance, actuarial context where you have really good data ... and you can come up with really nice numbers. Risk appetite in a cyber security context is just really hard. The story that’s been in the press today – I think it’s the Maersk shipping line – I think it cost them $300 million or something for their NotPetya infection earlier in 2017. Their ability to have quantified that beforehand is nearly zero. ... So, if someone had said beforehand tell us what your risk appetite is, well, you’ve got all these systems that haven’t been patched in 60 days or 90 days. Is that within risk appetite? That’s a very different question to - your patching process is going to lead to a $300 million loss. Is that within your risk appetite? Of course, it’s not. ... So, it’s only in retrospect that anyone sees that either they were or were not within risk appetite.”

A well-defined risk appetite supports the implementation of robust risk management processes throughout the organisation, as StatGov1 stated “risk appetite guides all of the decision making that you do in running a business.” FedGov1 confirmed, “if you’re ... lowering your risk, no matter what risk it is, it's got to be a better way to run your business.” Risk management processes extend to the management of information to increase its security. FedGov1 used a few approaches to reduce the risk of holding information, stating,

“The only way you can actively decide is to look at what information you've got now that you're collecting, classify it, see what risk you're running, and then decide how you can either migrate that risk by getting rid of the
information, if that's possible, or not collecting it, and/or put the mitigation in place.”

5.2.1.7.4 Security Culture

A strong security culture is the result of repeated employee actions which can be shaped through education, training and awareness programs, as well as policies and procedures which must be followed by staff. ITC1 stated that on “culture … it's one thing to put things in policies and procedures; that's useless if you don't manage it.” Some organisations had a strong security culture, and some didn’t. FinCo1 admitted “We're not defence. We're not government, and we'll never have the luxury of the culture that they have when it comes to understanding and treating classified data.”

To create a strong security culture however, FedGov2 compared the creation of a ubiquitous security culture with the permanency of an employee’s DNA, with,

“you need to have really good controls around document handling, marking, and labelling standards, and you need to have that embedded into the DNA of the psyche of the end users, so when they create that documentation, they're doing the appropriate labelling and handling at the very lowest level.”

The reason that a strong security culture is important is that humans generally do not make reliably-repeated actions and shaping culture is a way of controlling that. Humans can make erratic decisions, based on how distracted, busy or emotional they are at the time. Humans are a vector that attackers can focus on in social engineering attacks that attempt to conduct a security breach by enlisting the aid of an unwitting employee. FinCo2 was clear when stating,

“the common denominator on a lot of compromises is people. Social engineering is what a lot of attackers rely on to get in the door, and so the general acceptance is that people are the weakest link.”
ResCo1 observed the, “impact of culture on protecting data. … You can have all the frameworks, but … you’re relying on the guy at the end of the keyboard to decide that this is the right thing to do”, continuing, “culture … of security is a company-wide continuous improvement activity that should exist. You actively shape it.”

A security culture begins at the top and organisational leaders must set and shape the culture with their own actions, as AvCo1 stated “culturally, the tone from the top is crucial”. TelCo1 observed “The culture of board and Executive Committee … and the ability to actually morph and change the culture in a business to meet the changing and evolving technologies and innovations.” Culture comes with its challenges however and to avoid core rigidities within an organisation that prevent it from adapting to change, TelCo1 stated “You’ve got to have a culture of change and adaptability to manage the evolution of technology and innovation.”

5.2.1.7.5 Security Policies

Security policies are the levers by which the governing body of an organisation, such as a board of directors, can direct employee behaviour from their position and in line with their strategy. FedGov2 had an entire framework of policies imposed upon them, stating “Our general governance is driven through Attorney General’s department who publish the PSPF, the Protective Security Policy Framework.”

At the governing body level, two concepts are shaped, which are strategy and policy. There are many different types of policies, as StatGov1 gave an example of “a policy around not storing [third-party information] in a cloud environment without the authority of the person we’ve collected it from” and EnerCo1 gave an example of “we’ve got an acceptable usage policy.” Policies are used to govern employee behaviour and within an information security context, policies can be coupled with classification of information to align information value with security controls. ResCo1 stated, “Anything that is classified … will default into a certain retention policy, and
the only way you deviate from the retention policy is if it's required as part of litigation.”

ITCo1 made the distinction that simply setting a policy and forgetting about it does not have any impact internally within the organisation, stating “it's one thing to put things in policies and procedures; that's useless if you don't manage it.” It was also difficult to change policies once they had been set because employee behaviour had already been set and changing the policy meant changing the behaviour, which requires effort to learn. TelCo1 confirmed “Always remember, it’s far easier to implement a new policy than it is to remove access or an old policy … [because] … people get used to it. It takes change.”

In a variation on the policy concept, FinCo2 saw merit in adopting a principles-based approach to shaping employee behaviour rather than strict adherence to a list of policies, stating “One of the things I often wonder about is whether policy needs to be as rigid as it is because I think a more agile way of working is actually more principle based than policy based”, continuing with an example of the, “principle of least privileges” and “Centralisation is another principle, so do things once rather than multiple times.”

5.2.1.7.6 Security Education, Training and Awareness (SETA)

SETA programs are the tools used within an organisation to implement security policy. SETA programs are reflective of the range of policies that an organisation has set and intend to shape employee behaviour. The result is that repeated actions that have been actively shaped by security leaders should result in a strong security culture. AvCo1 stated,

“one of the most important things is … education and awareness from the board all the way down, and if you can’t affect that in some way, then that impacts your entire program.”
Education, training and awareness programs are necessary not just for general, end-user employees but the IT security staff as well. FinCo2 noted,

“A lot of attention actually needs to be put into security culture, training, and awareness programs. That needs to be a strategic imperative. If you’re going to do security in house, then you’ve got to invest in your security personnel and staff. You need to make sure they have the latest, greatest current skills because it’s an ever-changing landscape ... Security skill-sets are really important.”

EnerCo1 gave an example of increasing user awareness of potential misuse of information via a data-loss-prevention tool installed on workstation desktops, stating

“All it does is when someone tries to [copy data], it just comes up with a dialogue box, and they accept that it’s actually in line with the policy. If they push yes, then it goes, okay, no problem ... If they say no, then that just closes everything off ... Gets rid of most of the cases.”

5.2.1.7.7 Security Technological Controls

Technological security controls are used to defend against threats and are deployed appropriately to protect information with different values. RetCo1 stated there were “thousands” of controls, continuing,

“We use a tiered structure [of controls] ... if it’s just internal information, we’ve got a base level of a number of security controls expected to implement ... If you have sensitive information, there’s a different level of rigor and additional security controls ... and you need to apply those. We actively test and monitor those controls.”

The technological security controls that are used to protect information in an organisation can become outdated or obsolete very quickly however. FinCo2 stated,
“Investing in cyber security controls to also be current then follows on. You cannot deploy a firewall, turn on all the switches, and say good, that job is done. That’s not the way it works. You need to stay very current, understand how that needs to evolve over time to address the evolving threats, and in order to keep on top of those evolving threats, you need to be very engaged with the community.”

5.2.1.8 Organisational Resources

Organisations use resources in daily operations to achieve their vision and mission, and these resources are sourced from several areas within the organisation. For example, StatGov1 used their cash resources to improve their product mix, stating “if we generate a surplus … that surplus is turned into reduced prices, investing in new products, new services, [for example] beefing up our security.” However, RetCo1 discussed how information can also be used as a resource in an organisation, stating “Depends on how and where it’s used in the business. If it’s used real-time [then] stale data that’s a day or two … old, it’s less valuable than data that’s needed at this point in time. It just depends on how it’s used in a business process.”

5.2.2 Outsourcing Constraints

To summarise this section, numerous conditions can constrain organisations from outsourcing. If even one condition affects an organisation, then outsourcing may not be an option.

Several constraints were identified in the data that impeded an organisation’s decision about whether to procure outsourced services or not. These included a requirement for continuous information availability, country risk, economic factors, the external threat environment, industry factors, inertia, threat intelligence, lack of trust, lack of understanding about what outsourcing is, legal factors, loss of control and uncertainty about the outsourced environment, a perceived lack of quality, a
perceived lowering in productivity, political factors, potential loss of business resilience, privacy concerns, regulatory compliance, risk appetite, and holding valuable information. These factors are all discussed in the following sections.

A number of these concepts, for example political factors or regulatory compliance, are important because their existence affects how the organisation decides to approach its information, including storage, use and security. Given all these concepts negatively affect the approach to information security by an organisation, relationships will be collectively termed P5 in Figure 7.2.

5.2.2.1 Continuous Information Availability

Modern upward trends in digitisation of organisational products and services means there is increased risk of customer service degradation should an outsource provider cause service interruptions. For some organisations, this risk was too much. FinCo2 was firm when stating, “It’s definitely a constraint. Our expectations are on availability from the provider. If they can’t provide the level of availability we need, then we can’t use them.” For an island like Australia, this is particularly pertinent, as FedGov2 explained,

“depending on where your data is held, it only takes one undersea cable to go down for your whole business to be degraded. And there’s a lot of web-only-based businesses now, you know, the Ubers of the world, etc., that if they have a major cable problem somewhere, then half of their customers are cut off indefinitely”

FedGov2 then summed up with, “considering [there are] maybe two or three major undersea cables connecting our fragile little nation with the rest of the world, we’re very exposed.” Other research participants thought ahead to what the impact from a lack of information availability to key stakeholders such as customers, might be on their public reputation. FinCo1 stated,
“Availability, absolutely, it’s one of our key tenets, is availability. Not from security or technology, but more ways on principle. So quite often decisions around sourcing are around availability and uptime. If our internet services are offline for two minutes, it’s in The Age [newspaper]. So that’s a key factor for us.”

Other research participants considered the financial cost from a service outage causing an interruption to information availability, with ITCo2 stating that for an organisation which, “has got several thousand call centre reps, if their systems aren’t available, tick tock. Cha-ching. For every 5-10 minutes, 30 minutes, two hours is millions of dollars.”

In a variation on this concept however, some research participants thought that the requirement for continuous information availability was a driver to use outsourced services, not a constraint. ITCo3 stated, “No, I mean I would think that’s the reason why you would outsource it. You’d outsource it because it’s much easier to get 24/7 operation and continuous monitoring when it’s outsourced, and you’ve got around the clock support and follow the sun and everything else, than it is do that yourself.”

StatGov3 agreed, stating, “If anything, you’d probably get better availability out of an outsource service provider than internally, so that might be a driver for wanting to outsource rather than a constraint.”

5.2.2.2 Country Risk

Country risk is the risk of procuring outsourced services from vendors based in one country over another country that might be deemed more or less risky. FinCo1 gave a brief explanation, with, “Country risk is … what we call it specifically, but that aligns to economic, political, and all that kind of thing.” FedGov1 confirmed “We’re looking
at something now where it won't be hosted in Australia, but we've got the choice of where it will be hosted. But if it was in China or Uzbekistan then we wouldn't do it.” EduCo1 agreed, stating “If it’s a third-party organisation that sits in a communist country … Or in an organisation which does not abide to human rights, we might not consider doing business with them.” TelCo1 gave an example, stating,

“I mean, today in the paper, there is this … suggested premise, that the White House is considering in North America building their own nationalised 5G network, which they’re doing to counteract the national security threat of international organisations backed by countries that may very well be at loggerheads with the US. … national security issues will definitely come into the decision to outsource and what that means to the company and the country going forward.”

5.2.2.3 Economic Factors

PharmaCo1 explained that different economic models affect an organisation’s decision on whether to outsource IT infrastructure only or entire business processes, stating,

“Well, there are two types of outsourcing. There’s what I call IT Outsourcing, and then there's business process outsourcing. IT Outsourcing is basically outsourcing infrastructure. We have a saying here in the US, it's like, your mess for less. The business process outsourcing is like payroll, you outsource the entire payroll process to a third party, and it's really in their interest and yours for them to improve on the process to make it more efficient, and that's a very different kind of a relationship. And they all have economic models where it makes sense to either outsource and not outsource. So, economics do play a role.”
Thinking ahead, a country’s economy may determine the success of an organisation’s outsourcing arrangement because it might have a downturn which negatively impacts on the outsourcing vendors. ITCo3 stated,

“the reality is that some of the outsourcing deals we’re looking at now, particularly in the cloud environment, really involve organisations putting core parts of their operating business into someone else’s hands. And given that a lot of the tech industry is not profitable and nowhere near being profitable, we’re only a dot com crash away from a lot of these companies disappearing. I’m not sure that anyone really knows what happens when one of these cloud service providers disappears, and they’re just no longer there to actually run your systems.”

In a variation on this concept, when examining the cost-benefit relationship, ITCo4 thought economic factors might actually be a driver to outsource, stating that organisations which own their own data centres,

“will reach a point where all of the IT infrastructure inside of that data centre will end-of-life. You’ll need to go through a technology refresh process. And that's when you start to say, okay, if I've got to refresh this technology, I've got to go through a major hardware acquisition, I've got to go through a major project, I've got to go through all of the cost of migrating to new hardware ... That's potentially then that opportunity where you look and say, okay, instead of operating this data centre and then refreshing the technology every three to five years, am I better off to just go to an outsource arrangement?”

5.2.2.4 External Threat Environment

The external threat environment might affect an outsourcing decision because the outsource facilities have security frameworks installed that might appear vulnerable. StatGov1 stated, “You would be unlikely to engage an outsource provider of data
storage if they had a history of being breached.” This vulnerability might be due to variability in the maturity of security frameworks implemented at various outsource facilities, as ITCo4 explained “Some will have only a baseline level of security and ability to protect against modern threats. There will be other providers who … have a whole range of additional capabilities.” Another source of threats, that could affect an outsourcing decision, presents when co-locating information in an external outsource facility alongside another customer that is storing very high information there. ITCo3 explained,

“one interesting aspect of that is the contagion risk, or in fact, the collateral damage risk in my threat profile. If I’m outsourcing to an organisation that is also the outsourcer for very, very high-risk organisations, then, in a sense, I’m going to be taking on some of their risk as well.”

As well as determining threats that arise from outsource facilities being located in high-risk countries, organisations should also consider threats that arise from the external outsource facility being in an unsafe part of a city. PharmaCo1 considered “There are certain parts of the city where you wouldn’t want to have your information assets stored, if only because it’s difficult for employees to operate there effectively.”

Research participants began with a risk assessment of the external threat environment. FinCo4 stated, “We take a risk-based approach to protecting our information and this starts by assessing external threats. We … identify as many risks as possible.” Some organisations looked for specific threats, with EduCo2 stating

“We constantly look at our [control] settings based on the external threat environment. The biggest one, from our perspective, is probably state-sponsored threats because they’re typically well-funded, quite sophisticated, and quite targeted in what they’re looking to steal.”
AvCo1 however took a broader view, stating,

“The threat environment plays a significant part in our risk assessment. … We … look at the specific threat actors that might want to gain access to that information, whether that be for criminal use. Is it credit card information? Is it sensitive information that could be sold on the web for monetary value? Is it something that we could be held for ransom on? So, you look at the threat actors around that, is it criminal, is it government, is it a political agenda?”

In a variation on this risk assessment approach, one research participant used a threat model to gain an understanding. ResCo1 explained the term, stating,

“Threat model is let’s say you take a solution or technology environment, you do an analysis of what all can go wrong with it, all of the different types of threats to that environment, the threat actors, and what are the implications of those and what controls are needed.”

Within the organisation, external threats then affect the organisation in two ways. The first is that organisations assess the external threat environment and then implement a set of security controls in a preventative program designed to mitigate risks arising from those threats, as AvCo1 stated, “We operate in a high threat environment, so we take that as given and then increase the controls based on the value of our information.” RetCo1 summed up by stating “The higher the classification of the data, the higher the threat to that particular dataset, the more controls you need to apply.”

The second is that then organisations monitor their information and threats, and detect and respond to attacks when they occur. ITCo3 clarified,

“There’s the theoretical part of it and the reality. I think the theoretical part of it is that organisations go through this lovely process of understanding their assets and understanding their information, and they’re looking at the threats to that information and coming up with risks and designing controls to address
those risks and everything else. In practice, it doesn’t work that way. In practice, it is much more reactive, and so threats influence it”.

One consequence of information having value is that value can change depending on who is assessing the value. An organisation might assess the value of information differently to a threat actor. This can affect the level of controls put in place to protect the information which can affect the success or otherwise of a security attack. FinCo3 explains, with,

“there can be an asymmetry between what the organisation thinks is valuable and what the threat actor thinks is valuable. … That then means that organisationally you have to decide to protect it consistent with how valuable it is to the attacker, rather than how necessarily valuable it is to you.”

Although all research participants agreed that threats affected the security controls they implemented to defend the organisation’s information from a breach, most did not perceive that the value of their information was also affected by threats. PharmaCo1 stated,

“Companies are going to create information that has varieties of different value levels. The fact that somebody wants to steal it is a given. I mean, I don’t think that’s going to stop businesses from operating or innovating because that’s what they do. It’s our job to figure out a way to make sure that bad guys don’t get that stuff.”

Organisations did not raise or lower the value of the information dynamically in response to threats, but it’s possible that they should be, according to MgtCo2 who stated, “in my personal experience, they’re not that mature”. ITCo3 explained,

“I think most organisations are determining what information they hold based on the business need for that information or the value of that information. … I
don’t think organisations, yet, are mature enough to say that … because of the threat environment, holding that information is bad for us, so we’re not going to. I don’t think anyone’s mature enough to have that discussion yet.”

5.2.2.5 Industry Factors

What industry an organisation operated in affected their decision on whether to outsource information, as some industries had a higher level of threats than other industries. MgtCo2 gave some examples with,

“the manufacturing industry, given their immaturity in the technology space, especially in the cyber space, and the retail sector will have a different view on security and outsourcing and cloud sourcing as compared to the banking sector or to the tech industries in general.”

ITCo1 gave the specific example of a financial organisation to illustrate, stating,

“I can think of some industry factors and they would be – there’s some trading applications that need to be super-fast. So, you’ve got applications that actually do automated trading and speed makes a real difference. They spend a lot of money getting a bed of fibre networks to the trading centre so that they can execute faster trades. That would be a situation where storing something offsite, or information offsite, would slow them down, and that would be an industry factor. So, it would be a valid argument for storing it all in-house to get it as fast as possible.”

FinCo3 extended the conceptualisation of industry factors to include three factors, which were regulatory requirements, commercial requirements, and community expectations, stating,

“It strikes me that industry factor is probably a proxy for some combination of regulatory requirement, your upstream commercial requirements, so whether
your customers require you to only do business, or at least store data, in some parts of the world, and community expectations, in that order. So, the regulatory compliance would be very strong, then contractual requirements would be slightly weaker, but very industry specific, and then community expectations the weakest direct transmission, but over a long enough time period, is a very strong constraint. Then those three things would then factor into whether or not your industry is more or less likely to outsource and where it’s likely to outsource to.”

PharmaCo1 pointed out that their industry was becoming more highly regulated, which extended beyond them to include their suppliers. The corollary to this is that if an outsource facility is not up to standard, then they cannot be used, stating,

“we’re a highly regulated industry and the various drug agencies are now taking an interest in cyber. And by transference, they also take interest in the folks that operate systems for us. So, in as much as we have to be validated by drug regulatory groups, so do our vendors.”

In a variation to this concept, ITCo4 pointed out that if participation in an industry made an organisation a bigger threat target, then use of an outsource facility could make them more secure, stating,

“a lot of organisations that work in either highly-regulated or high-security arrangements and environments, … can potentially get better visibility, better security, better ability to do compliance and regulatory compliance within an outsourced arrangement, depending on the provider they choose, than what they can do in their own on-premise environments.”

StatGov3 agreed, stating,
“Maybe industry factors, instead of constraining, could encourage organisations to want to outsource. If I think of financial services … sometimes you can respond quicker, and … cheaper, if you’re outsourced.”

5.2.2.6 Inertia

Fear of the unknown can cause inertia, preventing organisations from using outsource facilities. FedGov1 confirmed “there is a bit of inertia … because it's the unknown”, continuing, “there is inherent nervousness about it.” In some instances, inertia can be caused by employees who might fear for the loss of their jobs if information is moved externally, as ITCo1 stated,

“We’ve certainly got clients where we’ve offered offshoring some of their work, and they don’t want to do it because it’s too hard. It’s only too hard because the lower level people make it hard because they don’t want to lose their jobs, and they’re worried that if you make it easy, then with price points that are competitive, they won't be able to do the job anymore.”

FinCo2 agreed that process and fearful staff can cause inertia in the transition to an external facility, stating,

“Going through a process to obtain the right level of certification and approval that actually an outsource provider is safe enough to use. … The process can be too onerous, or it's just too hard, and maybe that's somehow linked to the internal politics.”

StatGov3 thought that rather than employees experiencing the inertia, the management layers could cause it based on their drive, experience and maturity, stating “Probably lacking strong leadership. You can have paralysis by analysis … You can have nobody prepared to put their hand up and take responsibility for it.” MgtCo2 agreed, stating,
“management appetite and management knowledge. So, I think appetite and knowledge, ... mature buying patterns is something that could either enable or dissuade organisations from outsourcing.”

Overall, the employees and management both needed to embrace the use of external outsource facilities and this required a shift in mindset and therefore the culture of the organisation. EduCo1 gave an example, stating,

“The culture of the organisation. ... We have adopted a cloud-first strategy. We were a centralised inhouse all service managed organisation. We’re moving away from that now. ... There is a level of change that is required within the organisation because ... of retraining; ... we have approximately 370 IT staff here. That doesn’t mean we’re gonna do them out of a job. We’re going to retrain them on other things. But there’s a level of cultural change the organisation … needs to adopt to be able to embrace our path.”

5.2.2.7 Threat Intelligence

Organisations need to engage in surveillance of the external environment for threat intelligence and the presence of some targeted and concerning threats may affect a decision to outsource information. FinCo1 was adamant when stating “We watch the threat landscape”. FinCo2 engaged heavily in gathering threat intelligence from as many channels as they can, stating,

“we engage with over 120 different organisations on our intelligence sharing networks and programs through about a dozen different formal organisations, using both formal and informal communications mechanisms to share intel. That includes levels of law enforcement and government, through our peer financial services sector, and other non-sector industry bodies that also have cyber as a primary focus or risk, telecommunications and utilities and so on.
Information sharing is incredibly important to be able to stay current, stay alive.”

5.2.2.8 Lack of Trust

Trust in an outsource facility vendor appeared to be a significant concept for the research participants. AvCo1 stated, “I think that probably the most important part of moving to cloud is being able to determine that cloud provider is somebody you can trust.” Trust however was not easy to define. FinCo4 thought that the modern conceptualisation of trust was changing, stating,

“I think the notion of trust is changing. Innovation in technology is driving a rethink to the way we approach trust. It’s incredible to think that blockchain technology in a trust-less environment could be considered more trustworthy than a 100-year-old organisation such as the one I work for.”

FinCo1 defined trust as,

“Trust. The … ability for us to assure ourselves that the provider does the things that they say they will, their willingness to give us visibility and control, and right to audit. The simple test is: if we can’t do with the provider what we would do for ourselves, is it the right thing to be doing?”

The type of outsource facility that was being used by an organisation made a difference to the level of trust placed in it. An outsource vendor that shared partial control for the management of unencrypted information off-premises was viewed as very different to an outsource vendor that provided only external ICT infrastructure. RetCo1 disclosed their level of trust in an outsource vendor that managed their information, stating

“I would be very hesitant to hand my data to somebody that tells me they’re going to store my data securely on my behalf. That’s not a service I would
consume in any way, shape, or form, and I can’t see the benefit of that, to be honest with you.”

However, RetCo1 had no issue with consuming the services of an external ICT infrastructure supplier, stating “I would have no hesitation to … put sensitive data into the public cloud. With the right level of controls, I would.” RetCo1 balanced this however by disclosing that they only deal with ethical cloud suppliers, asking “Are they ethical organisations?” FinCo1 recognised the disparity between buyer power and supplier power affecting trust, stating,

“If you think about the AWSs and the Microsofts of the world, they’re not going to be as open, so we have to work a lot harder to get visibility. It’s not good enough for AWS to tell me they’ll do something. They need to show me how they do it. And if they can’t, then I need to build a control to mitigate the fact that I can’t say for sure.”

PharmaCo1 observed that outsource facilities may have perverse incentives to decrease the security controls used to protect information, stating,

“You have to trust your outsourcing partner to ensure that those employees are not criminals. We have a saying here in the US, trust but verify. So, if you don’t put it in the contract, odds are the outsourcer is not going to do anything about it. Look at it from their perspective, it costs money.”

EnerCo1 stated, “you can’t outsource governance, so … make sure the organisation that’s doing it for you is actually abiding by what it’s saying it’s doing in the contractual controls”, continuing, “a right to audit … just doesn’t work in the contract.” The problem was scale, as EnerCo1 elaborated “if they have like 100 customers, and every customer says, I want a right to audit, well, that [is too hard].” Instead, EnerCo1 posited a different approach, stating, “if you come up with a monthly reporting matrix and say … just report on these key metrics … like, how many times do you check the
admin passwords”, then with enough metrics, this can have the same effect as if the organisation went in and performed an audit.

5.2.2.9 Lack of Understanding of Outsourced Environments

Another constraint that may constrain an organisation from deciding to outsource is that they don’t have the skills or expertise in employees to understand it. This ignorance is different to taking a fear-based approach to resisting outsourcing. FedGov2 stated,

“The other factor, I think, that prevents some organisations from outsourcing is they don’t understand it. There’s a lot of buzz words out there. There’s a lot of sharks who are happy to sell you an Amazon Web Services instance, but not actually tell you what the benefits are, and how you manage it, and how it works. They’ll just give you the smoke and mirrors component.”

5.2.2.10 Legal Factors

Research participants gave different answers about legal factors that may constrain an organisation from deciding to outsource, which related in two main areas. First were environmental conditions such as statutory and common laws of the country, regulatory bodies, and ordinances that regulated organisations. Second were specific contractual conditions between two parties seeking to provide and consume products and services.

On the existence of legal factors being a constraint to outsourcing, StatGov1 confirmed, “Legislative compliance would be [a] reason you may not do it”, continuing, “we’re starting to play in the cloud. … we’re … deciding how we do that in a way that allows us to comply with legislation around privacy.” As a supplier of ICT outsource services, ITCo3 was required to “sign contracts that require us to only host
things in Australia, or not subcontract any hosting." On whether legal factors can constrain outsourcing decisions, TelCo1 stated,

“Yes, because there are caveats around what we can do as a GBE (Government Business Enterprise). There's the new critical infrastructure office under AGs (Attorney-General's office), and I think with all the TSSR (Telecommunications Security Sector Reforms) that will be coming in, there will be requirements under that, that will obviously impact on what we can and can’t do.”

When it came to negotiating contracts with external outsource providers, StatGov1 was concerned most with a “Loss of control. Inability to establish contracts that give you the level of control that you want or that you think you need.” FedGov1 confirmed “if we can't get the contractuals right and the protections right then we can't do it”, continuing, “they're either not complex enough or too complex. It depends. I've seen examples of both.”

StatGov1 gave an example of a time when they could not gain agreement on the terms and conditions they were after, requiring an escalation to the board of directors for risk acceptance, stating,

“We are attempting to negotiate a contract with a cloud vendor … and I'll be taking that to the board … because there are some risks associated with that contract that we simply cannot mitigate because the cloud vendor have negotiated as far as they're willing to negotiate. … One of the things that they won't commit to, for example, is advising us if there is a breach of their security around our systems or data. Now that's not to say they wouldn't tell us, but they won't sign a contract saying that they must.”
Reaching agreement on liability between parties was also a key consideration when negotiating outsourcing contracts. FinCo2 shared, “The big concern regarding outsourcing is liability”, continuing with an example,

“Lawyers are always worried. Liability becomes the number one issue. If a provider says, yeah, if we have an outage for more than five days, maybe we'll give you a free month of our service. No, you may have just caused us $10 million worth of lost business. So, $1,000 worth of your service is not really going to compensate.”

In a variation to the concept that it is necessary to negotiate favourable terms and conditions in outsourcing contracts, ITCo4 stated,

“I think some of that needs … a culture shift. This idea that an organisation needs to … make changes to a contract, … when you start to talk about subscription-based services or outsource-based services, most of the contracts are pretty standard”, continuing,

“Once they get … legal advice, … in the past, they were tied-in for a certain number of years and a certain amount of money, and it was really difficult to get out of the contract. With subscription-based services, … there’s no such thing as minimum spend. They're not locked into a contract. They can cancel it with 30-days’ notice.”

5.2.2.11 Loss of Control / Uncertainty About Environment

The concept that organisations lose full or partial control over their information or ICT environment emerged from the data as a major concern. StatGov1 was concerned about, “loss of control over things that you feel you need to have control over … if somebody else gets in and sees it, … who wasn’t authorised, you'd want to know that.” FedGov1 agreed, stating,
“rightly or wrongly, in my experience there’s a perception that outsourcing is risky, and I’m not talking necessarily about service levels and all those sorts of things, but moving it out of the known space into something else is inherently more risky.”

RetCo1 flatly refused to even consider partnering with an outsource vendor to manage their information, stating, “I would be very hesitant to hand my data to somebody who tells me they’re going to store my data securely on my behalf. That’s not a service I would consume in any way, shape, or form”.

There might be some valid business reasons that organisations don’t want to lose control of processes or information, including that they form a core competency for the organisation. ITCoo1 confirmed, “there’s a lot of reasons you wouldn’t put some things out. One of the main reasons would be it’s a core competency.” EnerCo1 gave an example of a time when an organisation lost control of their information, citing,

“I remember years ago, someone … outsourced something to Florida, and then the Florida company went bust, and they found that the data was outsourced to a place in Bahamas, which meant the whole systems, and everything were gone. It’s around … contractual controls.”

5.2.2.12 Perceived Lack of Quality

Organisation have a concern that the quality of services in external outsource vendors may not be up to the same level of quality as what is adhered to internally. On their decision whether to engage in outsourcing services or not, FedGov1 stated, “the factors that would affect us are inability of the proposed vendors to provide for our information security requirements, our privacy needs.” On a similar theme, StatGov1 stated, “the sanctity of the data, for example, if somebody else gets in and sees it, … who wasn’t authorised, you’d want to know that.” ITCoo4 gave examples of customer questions about the level of quality in their outsourced services, stating,
The traditional [questions are about] shared infrastructure, using shared infrastructure. They don't have dedicated infrastructure, so then they have to talk about, so what are the logical isolation mechanisms and what level of assurance can they get? … being a multi-national, how does that work, and where are the services supported by? … There are questions around, are you on the certified cloud services list? At what level are you on the certified cloud services list? How do we meet Information Security Manual compliance?"

5.2.2.13 Perceived Lowered Productivity Due to Security Controls

A few research participants held a perception that increased security controls can decrease productivity in organisations. Increased security controls in outsourced environments could be related. StatGov1 confirmed, stating, “there's a limit to how much security you can … put in place …, and you also have trade-offs from a usability productivity perspective if you put too much security in place”, continuing with an example,

“So, this morning I got mail from the Auditor General's office. The Auditor General doesn't just send you mail; they send you a mail message to say that they're sending you mail, and to get access to it, you enter your email address and a password. And since I don't get that much mail from the Auditor General's office, I always have to seek a new password. So, something, to my way of thinking is particularly necessarily very highly sensitive, takes ten minutes to get instead of ten seconds, which is frustrating.”

5.2.2.14 Political Impact

Another key concept that emerged from the data as a constraint on an organisation’s decision about whether to outsource or not were political factors. ITCO1 thought that “government organisations are going to worry about protecting the minister’s
reputation." ITCo2 confirmed, “I would see most government organisations wanting to stay away from outsourcing if … if they are going to have our data offsite somewhere in another country.” StatGov1 stated that political leaders need to engage with more security education, training and awareness programs to fully appreciate the potential opportunities for outsourcing information, stating,

“The challenge, politically, is a lack of understanding. Politicians are sometimes motivated by fear. There may be a degree of uncertainty around outsourcing of data on the basis of a sense that that makes that data more likely to be inappropriately accessed, and that's generally not based on a good understanding of what security mitigations have been put into place to ensure that doesn't take place. So, it’s a perception issue at the political end.”

StatGov2 thought that an outsourcing decision can be affected the destination country hosting the information, stating “If you’re outsourcing in a country where there's political instability, you will not.” MgtCo2 considered that political factors included a nation’s intent to surveil other nation’s information and that cyber capabilities were linked to these political intentions, offering,

“Politics always plays a role, but … with how cyber is now high on every countries’ agenda, there’s establishment of cyber commands all across the place. What’s happening across US, Europe, China, Australia. I don’t think cyber is something that is now in the shadows. I think it’s very much mainstream, and there is a large political agenda behind it as well. So, politics does play a role.”

ResCo1 considered that outsourcing decisions were not affected by political factors but that the outsourcing vendor was, offering,

“If you’re operating in a certain jurisdiction, and the number one outsourcing provider there is not on good terms with a particular countries' political
environment, it may not be a good thing to outsource. It won’t affect the outsourcing decision. It would affect the selection of the provider.”

In a variation on this concept of political factors constraining an organisation’s decision to use outsource services, ITCo4 stated,

“In Australia, for example, within government there’s a cloud-first policy. So, we’re actually seeing a shift, … they're more inclined to do that because there's less risk. … You're not investing multiple millions of dollars into a project, which goes and buys a whole bunch of infrastructure, which then doesn't work … I think we’re seeing more of a shift to outsource services from the politicians, not less.”

5.2.2.15 Potential Loss of Business Resilience

The concept of business resilience covers a range of areas in an organisation including disaster recovery. FedGov2 had a strong business resilience program that included management of their public-facing websites and protecting them from breaches, stating,

“We have tools that we’ve developed to maintain the integrity of our external facing websites. If they ever get compromised or defaced, then they get taken back to a last known good state immediately … And we’re very heavily engaged in ensuring that that public presence is maintained in a good state.”

StatGov2 gave an example of their entire organisation suffering an outage, with,

“AWS has … an acceptable use policy, and if that is breached, they have the right to terminate the service, which is okay except it's not clear that they'll just terminate the service of the organisation who has breached their acceptable use policy or an individual in that organisation who has done that,
and they may terminate the service for all of us. That wouldn't be a good thing.”

Sometimes organisations were focussed on ensuring resilience in key parts of the business instead of the whole organisation. FinCo2 gave an example, stating,

“Materiality is how critical this process is to the organisation. … So, if it’s a real routine thing like HR records, then people aren't too concerned. … But if there’s $5 billion in payments that didn’t get done across the country or internationally because there was an outage, that’s a totally different thing.”

On ensuring resilience in parts of the organisation to maintain ownership and control on information shared in outsourced settings, FinCo4 shared “there is a potential loss of data if they go out of business”, and ITCo3 commented on portability, stating,

“data portability. So … if I sign up with Outsourcer A, will I ever actually be able to move, or is my data in some proprietary format on some proprietary system that, if I move, I basically have to start again, and I lose it all.”

5.2.2.16 Privacy Legislation Compliance Concerns

Privacy concerns affected organisation's decisions on whether they could outsource quite strongly. StatGov1 shared, “we're going through the throes of deciding how we [outsource] in a way that allows us to comply with legislation around privacy.” Although the privacy legislation was very clear to most research participants, FedGov2 related a story about colleagues in other organisations not being as aware, stating,

“A lot of them aren’t considering the privacy factor. I’ve spoken to some industry partners around similar things, and as soon as you mention the Privacy Act, they go the what? And they’re not even aware that some of the factors that could or would prevent you from going to cloud services is
actually the Privacy Act, not your own internal strategies or your own internal business decisions. It’s just the protection of that personal data going into those hosted environments.”

5.2.2.17 Regulatory Compliance

Regulatory compliance was a concept that attracted significant concern from research participants when considering its impact on decisions to outsource. On considering outsourcing options, FedGov1 was emphatic when stating “If it doesn’t meet regulatory compliance, we can’t do it. It’s off the table.” ITCo3 stated that the most common regulations were “data sovereignty requirements around privacy, GDPR, the Privacy Act.” If an organisation discovers that their outsource partner was non-compliant with regulations, that can lead to termination of the relationship, as PharmaCo1 stated, “data residency and sovereignty laws … We have had situations where we have had to end agreements with outsourcing partners due to the security concerns.” ITCo4 extended compliance from not just assessing the outsource supplier, but their customers as well, as part of an ecosystem, stating,

“what they do need to do is take into consideration that regulatory framework and ensure that not only does the outsourcer meet their obligations underneath the regulatory framework, but can the customer, can the organisation, also meet its own regulatory obligations within that service?”

ResCo1 identified that specific regulations can drive different behaviours. Privacy regulations for example affected outsourcing decisions related to sharing of information only, not infrastructure as well, stating,

“It depends on if it’s privacy related stuff. … So, if it’s outsourcing our infrastructure services, then it’s not so much of an issue. But if it’s outsourcing in terms of going into a [Software-as-a-Service] solution, then that would be a little bit of a concern because then you need to look at is this a multi-tenanted
environment? How do we know when stuff happens because some of the requirements around notifying within a certain timeframe? How do we make sure these things happen? Who owns the risk if that happens? … so those kinds of things come, then you start losing the value of outsourcing.”

On maintaining a good working relationship with the regulator, FinCo2 saw regular two-way conversations and updates with regulators as the path forward to preventing a negative experience with compliance, stating,

“Anything we’re looking at doing …, we’ll talk to the regulator in advance, and say we’re thinking of doing this, letting you know it’s coming. And as we go there’s constant dialogue so that we don’t turn up and say, oh, look what we’ve done, and they go, oh, we’re not happy with that.”

StatGov3 raised an interesting perspective on risk appetite, stating, “I think most organisations would have zero risk appetite for legal or regulatory compliance breaches.” Most boards or equivalent have formally defined a risk appetite statement, that is used by executive and management to guide decisions within the organisation. It is incumbent on them to include a reference to regulatory compliance in the risk appetite statement, so that it is clear for all employees, and they can make clear decisions on outsourcing.

5.2.2.18 Risk Appetite

The board of directors or equivalent in a public organisation will typically set a risk appetite as part of their risk management and governance processes. The risk appetite sets the limits of risk that the whole organisation will tolerate, and delegated levels of authority for approving risk below that by executives and management. ITCo4 confirmed,
“risk appetite should absolutely form a fundamental component of all the assessment of whether you should or shouldn’t use an outsourced arrangement … The challenge for most organisations at the moment, particularly in government and in smaller enterprise, small to medium enterprise, is how do they effectively assess that risk and then determine whether or not it is within or outside their risk appetite.”

As ITCo4 identified, the challenge for consumers of outsource services is that the storage of information and the protections put in place to secure the information are obfuscated from the customer, stating,

“The challenge … is a lack of understanding of … how they’re secured, operated, supported, maintained, and run. And being able to make an informed decision about … what is the residual risk, what are the mitigations and compensating controls to then feed that into that decision around risk appetite.”

Measurement presented as a property of risk appetite and was a challenge to most. StatGov3 stated,

“If there was PROTECTED or … TOP SECRET information, I expect that the risk appetite for putting that out in a general cloud would be not high. Yet I come from financial services where they’re actually able to quantify risk appetite pretty much down to a dollar level, so then that’s really making an informed risk decision. I think risk appetite is a really useful lever to have in trying to look at what your options are.”

StatGov1, a CEO, gave an example of a time when a risk was identified within the organisation and exceeded StatGov1’s level of delegated authority for approval, requiring an escalation to the board, stating,
“We are attempting to negotiate a contract with a cloud vendor, ... and I'll be taking that to the board ... because there are some risks associated with that contract that we simply cannot mitigate because the cloud vendor have negotiated as far as they're willing to negotiate. ... So, in that sense I'd be taking that ... to the board to say here's a risk that I'm gonna be willing to sign off. What do you think? And we'll see.”

5.2.2.19 Valuable Information Ownership

Within the context of deciding about whether to outsource information, the ownership of information with high value impacted the decision to outsource.

StatGov3, being a government organisation, stated, “if there was PROTECTED or ... TOP SECRET information, I expect that the risk appetite for putting that out in a general cloud would be not high.” FinCo1 perceived that information value was the foremost concern, stating, “really, that’s key. Before we even look at those other factors, the materiality or the value of information is important.” FedGov2 also perceived that an outsourcing decision was contingent on the value of information, stating,

“A lot of the big banks are going to cloud services for a lot of things that they do, but that really sensitive information, you know, the user names, passwords, credit card details, etc., they’re generally keeping very tightly secured in their own data centres.”

In a variation to this concept however, StatGov1 thought that an external outsource facility may be a better repository for organisational information if it offered higher security, stating “if the data is super valuable you may want to put it someplace outside because it’s more secure to do so.” ResCo1 gave an example, stating,
“For example, board documents or cyber strategy documents could stay in an outsourced provider facility that we have full visibility and assurance that it’s being protected to our standards or higher. And in some cases, we might have to use an outsource provider because we probably are insecure internally.”

ITCo4 agreed that assessing information based on classification and using an external outsource facility can be more secure, stating,

“[If] an organisation [is] looking at [a] classification scheme and looking at outsourcing, they just need to look at, okay, based on a certain classification of information, what are the controls that need to be put in place to be able to store and process that information, irrespective of whether it’s in an outsourced environment or on-premises? And then, in the discussion about an outsourced environment, can they actually deliver or meet those controls and those obligations that need to be in place to protect that information using that service. If they can, then they should crack on.”

Information might have such high value that it is irreplaceable. Security controls such legal patents give the information owners the right to legal recourse to defend against infringing the patent however the information is made public as part of the patent process. ITCo3 perceived that irreplaceability of unique information could affect the decision to outsource, stating,

“I guess if you look at … look at Space X in the US. Space X doesn’t patent anything, basically, because their belief is it’s really hard to invent what they’ve invented. If they patent it, they’re basically giving it away. The people who would likely be knocking off their IP are nation states who aren’t going to care about the patent anyway. So, they’re better off just not patenting it. I would guess they are not hosting that in some random cloud environment on
the internet. If your IP is genuinely that much of – if you lose it, then it’s over
kind of scenario, then, yeah, it’s going to be like the recipe for Coke and the
recipe for Big Mac sauce and keep it locked in a vault and systems that are
not internet connected, so that can rule out outsourcing."

Pharmaceutical organisations generate revenue by developing new drugs and
bringing them to market, so the formulas for the new drugs are highly secret, and the
target of industrial espionage. PharmaCo1 had found a method to outsource
irreplaceable information used by an outsource partner yet keep it secure, by
compartmentalising and devaluing the information via tokenisation, sharing,

“In our world, we do outsource clinical trial information. In terms of handling
that, it's something called CRO (Contract Research Organisation). The
organisations that do this are clinical CROs, but that information essentially is
tokenised and anonymised when it's processed. And even the compounds
that we're testing, those are tokenised as well, so the risks are relatively low
to work with those individuals or those kinds of companies.”

5.2.3 Outsourcing Enablers

To summarise this section, numerous conditions can enable organisations to engage
in outsourcing. Their existence makes outsourcing a viable option for organisations.

As well as a sizeable number of outsourcing constraints, several outsourcing
enablers also became apparent after the research data was analysed. These
included due diligence, inclination to reduce complexity, money, preference for
operational expenditure (OpEx) over capital expenditure (CapEx), the presence of
security controls, and the size of the organisation. These are all discussed in the
following sections.
A number of these concepts, for example money or organisational size, are important because their existence affects how the organisation decides to approach its information, including storage, use and security. Given all these concepts positively affect the approach to information security by an organisation, relationships will be collectively termed P6 in Figure 7.2.

5.2.3.1 Due Diligence

Moving information outside the confines of a network boundary of an organisation into cloud-based storage is not straightforward and there are many factors to consider from many different sources. FedGov1 stated,

"when we first moved our infrastructure out, I had to get all the assurances I could about the business case, RFP … I got an independent review from KPMG. We did a privacy impact assessment. We had to go to a couple of board meetings".

ITCo4 considered that due diligence had to be extensive and coined the term SOS to describe their approach, stating,

"[SOS means] Security of Supply. The first thing I do is actually make sure the company that we rely on has got a strong history, and your due diligence looks at not just the organisations and its financial viability but those that control it. There’s any number of companies … around the world in IT services, particularly cyber security services, who are backed by foreign nationals"

The significance of due diligence is that ITCoo4 thought that conducting an appropriate level of due diligence then allowed the organisation to negotiate better terms and conditions in an outsourcing agreement, stating,
“You have to do your due diligence so you understand how it's configured and how it's supported, maintained and secured, but ultimately, then what you do is devise a contract that says, okay, on the basis that you've told me this is how it's supported, maintained, configured, and secured, I expect you to do all of those things, and if you don't, you're in breach of that contract.”

MgtCo1 agreed that having a right-to-audit in the terms and conditions of a strong Service Level Agreement was crucial, stating,

“If you're outsourcing certain things, make sure you have a right to audit and a strong service-level agreement with them. And before onboarding, do a proper third-party security assessment on them, ask ... how they manage data, where are the data ... who [has] access to it, which of the clients have the same storage, always know where your data is. ... Do your proper due diligence when outsourcing. Based on that, you make your decision.”

5.2.3.2 Inclination to Reduce Complexity

Organisations perceived that, unless it was related to core business, the burden of hosting information in-house can seem like a waste of time if their primary purpose is to focus on something other than IT. Hosting information in-house requires employees and physical parts, such as a dedicated floor space, a secure physical environment, server hardware, operating system expertise, and database administrators. Instead, RetCo1 stated that they use an outsourcing partner because,

“There’s obviously cost benefits, potentially, in that I only pay for what I use. ... I don’t have to worry about ... operating system patching and general IT of maintenance. ... I can focus on protecting the data which is the only thing I really care about. Honestly, I don’t care about anything else apart from data. It’s menial tasks to maintain a server appropriately, it’s really painful. It’s much easier to let somebody else do it, who does it very well.”
5.2.3.3 Budget

Budget or the lack of it can affect the decision on whether to outsource or not, as confirmed by MgtCo2 “It depends on how much money they have to spend on it”. Financial resources are limited within any organisation and constrained budgets affect the prioritisation and commencement of strategic and operational initiatives. Sometimes an organisation’s board of directors or ministerial equivalent engages in budget setting decisions and sometimes they don’t, leaving these decisions to executives. FinCo2 related an example of a board active in budget-setting, where,

“in a budget discussion that we had last year, there were budget cuts that were imposed that meant that some risk treatments that were treating extreme risk were going to be delayed. So, when that message was taken to the board, funding was restored. That’s at board level.”

5.2.3.4 Preference for OpEx over CapEx

A predilection for OpEx over CapEx affected outsource purchasing decisions within organisations. Organisations may not need to own the IT infrastructure that is used to host their information, especially if they can lease the same platforms, so the need for capital expenditure to purchase and own the infrastructure is diminished. ITCo1 stated, “The nature of our business … doesn’t require any capital expenditures. We’re all operational expenditures. Our costs are our staff, and every other cost is irrelevant to business.” EnerCo1 thought that environmental conditions might cause preferences to change, stating,

“In the security space, we’re pushing a lot of cloud tools because then it keeps current with all the rest of it, but that affects OpEx, whereas if you go in onsite, then it’s CapEx, but sometimes, going CapEx is more attractive than OpEx and vice versa.”
5.2.3.5 Security Controls

Security controls protect information from threats, and ITCo4 gave a few examples such as “multi-factor authentication, ... role-based access controls for staff, and the ability to do things like, for email, implement ... Dynamic Tag Management”. A key concept was equivalency of controls between organisations. In an outsourced arrangement, the security controls in an outsource partner must be equivalent or better than what is used within the organisation. PharmaCo1 stated,

“... the outsource partner should be mapped into the security process, the policy standards and procedures of the contracting company. So, when we talk to an outsource partner we want to make sure that they at least are, a) aware of our policies and standards, b) that they can comply to them”.

PharmaCo1 perceived that over time, outsource vendors are maturing and getting better at applying security controls to protect information, stating “outsourcers now are very security aware. ... outsourcing partners have better security controls than we have because it's their core business.” Flexibility may be required to bring outsource partners up to standard when comparing equivalency of security controls, and an organisation should have the option to demand that certain security controls be implemented by outsource partners. ITCo4 stated “Inevitably, their own risk appetite ... might mean that there are additional things that they need to have implemented. This service should actually make that available.”

When implementing security controls, it is important to focus on the overall outsourcing goal to guide implementation efforts. MgtCo2 stated,

“... most organisations try and layer their security controls for multiple standards. I think there needs to be a fine balance between technology controls that are strategic and outcome-based versus prescriptive controls that are very technology-specific because in large outsourcing contracts, that has often
been an issue, where organisations get caught up and end up spending too much money because they were prescriptive at the time.”

Identifying the controls used by an outsource partner however can be problematic because either the outsource partner refuses to allow visibility into the current state of their security controls, or because they use their own outsource suppliers in back-to-back agreements and don’t have visibility themselves into what security controls are used. This reassurance as to the level of security controls used may sometimes be provided, not directly by inspection, but by high-level attestations. ITCo4 noted,

“when you outsource … you lose the ability to implement technical solutions … what they should be looking for when they do their due diligence and their risk assessment process [is] which ones actually provide them the visibility and the ability and the tools to be able to do exactly that.”

The key concept is building trust, where an organisation must be able to trust that an outsource partner has equivalent or better security controls and commits to using them to protect the organisation’s information. Another way that an organisation can gain this trust is to rely on independent assessments made by third-parties. AvCo1 illustrated with,

“The key concept is building trust, where an organisation must be able to trust that an outsource partner has equivalent or better security controls and commits to using them to protect the organisation’s information. Another way that an organisation can gain this trust is to rely on independent assessments made by third-parties. AvCo1 illustrated with,

“We have used criteria from the Cloud Security Alliance to help define which cloud providers meet a certain level of criteria. You know, all cloud providers aren’t created equal, so rather than saying what is the information that you’re going to put in the cloud, for example, we first ask the question, what is the level of trust associated with that cloud service provider?”

There is advice available from many government regulators, consultants, and vendors, on how to deliver assurance over third parties. To sum up, FinCo3 stated,
“at the highest level, the key thing you need to consciously build if you are outsourcing … material business activities, is a third-party security program. That, ideally, consists of two pieces. One is a risk assessment activity at the beginning of the relationship with a third party … And … the second thing is a control and assurance program that scales to reflect that risk.”

After time, the relationship with the outsource partner may come to an end for a variety of reasons. Backups of an organisation’s information made by outsource partners are an important control in a security program as they aid in ensuring availability of information. Backups must be made available to the organisation, to allow data portability and the capability to respawn a website, database or application that uses the information, as part of a disaster recovery program. Disaster recovery is an important component of an overarching business resilience capability. ITCo4 noted that organisations must,

“be able to take back-ups, and to have data portability so that if something happens inside the outsourced environment, they can potentially bring that data back into their on-premise environment, or some other service provider, and get it up and running again really quickly.”

StatGov2 agreed, stating “one of the very important control clauses in the contract should be the exit clause, [where] you should get your information back, and it should be in a form which you can use.”

5.2.3.6 Size of Organisation

The size of an organisation does not affect the number of security attacks it suffers, as TelCo2 confirmed “There’s plenty of reporting about data breaches, security breaches, in SMEs, medium-sized and large businesses”. The size of an organisation does however influence the human resources organisation-chart
structure, because larger organisations require and can afford extra employees and layers of management. ITCo3 reflected on roles and responsibilities, commenting,

“So, it largely depends on the size of the organisation. So, for the largest organisation, that’d be the Chief Information Security Officer or Head of Cyber Security. And then, as they get down into the sort of mid-size, it tends to be more Information Security Manager or Information Security Officer.”

The size of an organisation also affects the allocation of resources within it, as smaller organisations with limited resources need to direct these towards higher priority activities first. FedGov3 commented on the benefits of using outsourced infrastructure, stating,

“You don’t have to maintain those skills inhouse, and you don’t have to pay for it. You’re paying someone else to do all that, organise the expertise and carry the risk. … why should a medium-sized organisation that specialises in building car widgets … also need to be experts in securing their systems because this is something that’s common to absolutely every business and organisation, but that’s not what they specialise in. That’s clearly the benefit of outsourcing.”

This recognition of asymmetry in size between the organisation and an outsourcer partner means that efficiencies in scale and scope can be realised, thus conserving precious organisational resources. FinCo3 stated,

“You could get someone else to deliver that capability for you [and] because they operate on a much larger scale, they could be dramatically better at it. Particularly where you’ve got that asymmetry in size.”

5.2.4 Organisational Context Summary

There were several concepts discovered from the data after analysis of the categories Organisation, Outsourcing Constraints, and Outsourcing Enablers, with
the conceptual model in Figure 5.1 depicting the major concepts together with their relationships. Models include definitions of concepts but do not fully justify their relationships or boundaries, and are often the basis for developing theory (Wiesche et al., 2017). In all, the student researcher created 35 different versions of this diagram after integrating memos and analysing, before settling on Figure 5.1 as offering the best explanation of the concepts involved and their relationships.

![Conceptual Model of Core Organisational Concepts](image)

**Figure 5.1. Conceptual Model of Core Organisational Concepts**

### 5.3 Chapter Summary

This chapter describes the findings from analysis of the data, providing a rich description of the concept of information security strategy, analysed for its properties and dimensions, noting any variations throughout. After the data were analysed, related analyses were aggregated into categories, which were integrated and then interpreted in relation to the overall research question.
Chapter 6: Findings – Approach and Impacts

This chapter continues on from the findings on information used within an organisation and findings about what context organisations operate within, to describe findings about what approaches organisations take to secure information, and finally what benefits or consequences impact organisations.

6.1 Chapter Aim

The aim of this chapter is to describe the findings after analysis of the data, providing a rich description of the concept of information security strategy, analysed for its properties and dimensions, noting any variations throughout. After the data were analysed, the analyses are aggregated into categories, integrated, and interpreted in relation to the overall research question.

6.2 Information Approach

To explain the heading, taking an “approach” to securing information is an in-vivo term that was adapted from ITCo1, who stated “we've taken the deliberate approach of devaluing the information that we have.” Information can be approached in a few different ways. It might be stored internally within an organisation’s private data centre, or its management might be outsourced to a trusted managed services provider. There are situations where an organisation might decide to not hold the required information, instead using information held by an external third party. In a similar way, an organisation can decide the value of the information that it owns, from low value up to high value. The previous section has outlined the relationships where antecedent concepts affect the approach to securing information within an
organisation, labelled from P1 through to P6 in the conceptual model depicted in Figure 7.2.

In this section, four distinct approaches to securing information are identified in the data, which are securing valuable information, evading trouble, getting help, and accepting the risk. These concepts relate to approaches taken when securing information within the organisations that were studied in this research and are italicised in the relevant research participant quotes to highlight them. Relationships where these four concepts affect strategic impacts on the organisation are collectively labelled P7 in Figure 7.2. A description of these four concepts follows.

6.2.1 Securing Valuable Information

To summarise this section, if information is valuable, then it must be secured well, and is often stored internally for added control.

Generally, valuable information must be secured, which affects where it gets stored. The first step is to identify valuable information. FedGov2 offered, "you have to look at all your data holdings and make very conscious business decisions about what is the most highly protected data that you have and then control access to that".

The next step that organisations take after they have identified valuable information is to secure it. This protection is information-dependent rather than a universal organisation-wide approach, as StatGov1 reflected "we look at classes of information and determine whether or not that information needs to have additional protections because of the nature of the information", and ITCo3 added “organisations are trying to create a sensitive data environment so that they can keep all their sensitive data in a relatively restricted set of systems and environments that they can apply more controls to". StatGov1 agreed "you would have greater levels of security around it, greater controls in terms of access". ITCo1 believed that protecting valuable information required secure infrastructure with security controls, because “to store
valuable information, you probably have to fortify your defences, fortify your infrastructure”.

As well as securing valuable information, organisations increased control over their information by storing it internally. ITCo1 agreed with the next step being to store valuable information internally, stating,

“You could obviously put it in a secure area. You can have various privileges setup by password security. You can use encryption on accessing it, so you can't access it through unencrypted means. ... You've got to be inside the office on a local network. You can't be outside the office.”

ITCo3 agreed and extended by stating that information storage systems should not even be connected to the internet, to reduce the risk of a security breach, stating,

“If your IP is genuinely that much of — if you lose it, then it's over kind of scenario, then, yeah, it’s going to be like the recipe for Coke and the recipe for Big Mac sauce and keep it locked in a vault and systems that are not internet connected.”

FinCo4 kept their valuable information internally and identified budget as an enabler for this, stating,

“why wouldn’t I store my valuable information in an outsourcer’s secure environment? ... Our internal data centres are more secure than what can be found in the market as we have the funds to make this possible.”

When asked whether protection of high value information makes an organisation more secure, ITCo3 answered, “Yes.” This relationship between fortification techniques positively affecting the security of an organisation is important and is labelled P7a in Figure 7.2.
6.2.2 Evading Trouble

To summarise this section, removing value from information reduces impact if there is a security breach. There are three mains to achieve this reduction in information value: avoid, tokenise, and delete.

Information held by organisations can be reduced in value, by avoiding possession of valuable information in the first place, tokenising it, or deleting it, which results in reduced costs and increased security of the organisation. ITCo1 confirmed “we’ve taken the deliberate approach of devaluing the information that we have. What I mean is, by taking away the risk, taking away the importance, taking away the impact”. ITCo3 also agreed that devaluation made organisations more secure, stating, “in the same way that a bank that holds no money is a less attractive target to rob, yes”. This relationship between devaluation techniques positively affecting the security of an organisation is important and is labelled P7b in Figure 7.2.

The findings revealed three clear techniques that organisations actively use to reduce the value of their information. First, ITCo3 reduced information value through tokenisation, “you tokenise [information], so you don’t actually have the data anymore; you have tokens that effectively refer to the data”. Second, organisations often make the deliberate choice to avoid holding valuable information in the first place, as is the policy of StatGov1, “we don’t deal with anything that is PROTECTED”. Third, FinCo1 found that lowering information value can also be achieved by deleting old information, as “purely by removing volume, you’re reducing surface area, reducing risks in lots of ways”. These three main approaches to securing information are discussed in the following sections.

6.2.2.1 Avoid

Organisations can actively decide to avoid holding valuable information to reduce the risk of impacts from a security breach. ITCo3 confirmed that avoiding holding
valuable information was a valid approach to improving regulatory compliance, stating,

“The bigger element is organisations just trying to avoid having the information at all. And again, [Payment Card Industry] is another example of that, which is rather than take payments yourself, use PayPal or just outsource the whole thing. Just get rid of that function so you don’t have that data that brings with it a regulatory burden.”

6.2.2.2 Delete

The volume of information held can sometimes be reduced to lessen the impact of a security breach, as StatGov1 offered “not that I’m afraid of security in the cloud, but it seemed easier just to move it or delete it.” ITC02 agreed, stating, “I have taken a number of exercises, … where I go through our shared drives of client work and remove that … to reduce the risk of that being out.” FinCo1 also noted that reduction of volume of information reduced the risk of a security breach, stating, “Just purely by removing volume, you’re reducing surface area, reducing risks in lots of ways.” PharmaCo1 was a strong proponent of this deletion technique, stating,

“I'm actually a firm advocate of destruction of unnecessary data. First of all, it’s costly to store. You have compute, you have storage costs, you have processors that need to be maintained just to archive that stuff. If you can destroy it, well, you don’t have those costs either, so there’s a win there as well. Companies should actually delete a whole lot more data than they do.”

FedGov1 was bound by law to retain information for various periods of time but agreed that not deleting information increased risk of a security breach, stating,
“we have Records Acts, for example, we've got to keep some information for a certain period of time. So … to be really quite honest with you, we just tend to keep everything, which comes with a risk and a cost.”

Internally within the organisation, the person responsible for deleting information is the data owner. ResCo1 commented, “All of the data that we have electronically, the data owner has responsibility for it. One of the responsibilities of being a data owner is to manage the life cycle of it."

6.2.2.3 Tokenise

When asked whether lowering the value of information makes organisations more secure, ITCo3 responded affirmatively, stating,

“[Payment Card Industry Data Security Standard] is the classic example of that. I mean that whole standard is built around that very concept, which is if you hold credit card data you’re going to be in for a world of pain protecting it. Whereas if you tokenise it so you don’t actually have the data anymore, you have tokens that effectively refer to the data, then your life becomes much, much easier. So that concept is very common now. That concept of tokenisation is really how that fits together.”

When asked whether tokenisation makes their organisation more secure or not, StatGov2 replied, “Yes.” This relationship between tokenisation as a devaluation technique positively affecting the security of an organisation is important and is labelled P7b in Figure 7.2.

6.2.3 Getting Help

To summarise this section, securing valuable information can be more effective when organisations take advantage of increased security controls and maturity of security processes by procuring services from specialist outsource partners.
Essentially, outsourcing is an economical way to get help by utilising external skilled experts and current technology infrastructure to securely host information. Its use depends on risk appetite and trust in the vendor. Outsourcing has numerous benefits and has gained popularity, as StatGov1 found “contemporary services, availability anywhere, these are the advantages of the cloud, evergreen environment, so we’re not having to upgrade things ourselves”. FedGov1 believed the investment required for in-house infrastructure made outsourcing attractive, as “it’s economies of scale. You should be able to get something that's better than what we can provide with a bunch of five or six people”. Organisational considerations for outsourcing included the level of competence and hence trust in the outsourcing partner, with FedGov1 sharing “the factors that would affect us are inability of the proposed vendors to provide for our information security requirements, our privacy needs”.

Counterintuitively, in a variation to this concept, concerns about trust did not prevent outsourcing being a viable option for improving security, as StatGov1 shared “I'm almost certain that Microsoft's environment is going to be more secure than anything I can do internally”. FedGov1 pragmatically considered “there's economies of scale for large providers to provide much better services than we can ever provide. And in some of that I include information security as well”. This perception extended to information with high value, as StatGov1 agreed “if the data is super valuable you may want to put it someplace outside because it's more secure”. When asked whether outsourcing information storage can make an organisation more secure, ITCo3 answered “it can”. This relationship between outsourcing techniques positively affecting the security of an organisation is important and is labelled P7c in Figure 7.2.

However, outsourcing is not always appropriate. In a variation of this concept, all research subjects agreed unanimously that regulatory compliance, economic factors, legal factors, and the external threat environment can be constraints on the decision whether to outsource. Most subjects (80%) agreed that industry factors, political
factors, valuable information and the requirement for continuous information availability also constrain decisions to outsource. The sensitivity of the information being stored outside the organisation was also a major factor, as StatGov1 stated “third-party information, which we’ve got a policy around not storing that in a cloud environment without the authority of the person we’ve collected it from, or anything that was particularly sensitive.” ITCo3 extended to address irreplaceability of information being a barrier to outsourcing, stating

“If your intellectual property is genuinely that much of – if you lose it, then it’s over kind of scenario, then, it’s going to be like the recipe for Coke and the recipe for Big Mac sauce and keep it locked in a vault and systems that are not internet connected, so that can rule out outsourcing”.

6.2.4 Accepting the Risk

To summarise this section, low-value information can be secured using minimal efforts only, which conserves security budget for securing more valuable information.

Information may of such low value that its storage and protection can be accomplished with simply a minimal amount of resources, as ResCo1 stated “controls around it are … very minimal”. ITCo3 explains,

“the information is low value so don’t worry about protecting it. We have this concept in our company of minimum viable security. Minimum viable security is: what do we need so that if something goes wrong we’re not seen as being horribly negligent?”

ITCo1 added “we put decent precautions in place. ‘We’ve been so sad that this information got stolen, but we gave best efforts.’ I wouldn’t really get into trouble with any government organisation because we’re taking precautions.” Under this approach, organisations did not leave information completely unprotected. There
were basic security controls put in place to defend information against ubiquitous threats. RetCo1 argued, “You would have a base level of controls that proliferates throughout the organisation that’s non-negotiable.” FinCo3 also took this approach but slightly increased the base level of protection around low-value information, stating

“Great examples of [low-value information] are email and file storage … We actually do a reasonable bit to protect all of those things as if they were mildly, but not extremely, sensitive, so with a reasonably strong baseline set of controls. We’ve got a very strong perimeter, as you’d expect from a large organisation.”

The reasons for this are twofold, one is increased productivity by reducing the effort expended by data owners in attempting to determine the value of information and correctly classify it, and the other is generally increased security, as FinCo3 stated,

“It reduces the amount of energy that a user has to put in to working out how to protect information because we’ve done the work for them. I think, too, it helps hold the rest of the environment to a higher base level of hygiene than would otherwise be the case.”

AvCo1 refined the approach by explaining that the security budget should be used initially for protecting high-value information and then the residual budget should be expended on protecting low-value information. StatGov2 also reduced the amount of effort taken to protect low-value information, explaining “I’m saving money … and resources”. RetCo1 also took this approach, stating,

“Everybody’s got limited resources, and you want to make sure that you apply the appropriate level of security and resource allocation to securing data based on the value of the data. If the value of the data is very low, you don’t want to spend a lot of money in securing it.”
This reduction in resources results in a proportionate reduction in capabilities but this was perceived as acceptable given the low value of the information, as StatGov3 explained “if it’s got little value, it would be more palatable to have a longer delay in being able to recover it or retrieve it [from backups].” Pragmatically, AvCo1 accepted that this prioritisation towards high-value information might mean that there are situations where all the security budget is expended on protecting high-value information with no residual budget left over for low-value information, stating,

“The most valuable information changes so it’s constantly moving and shifting. … You have to constantly shift your control prioritisation to an environment rather than it being static. … You may not get to it just because you’re focusing all your efforts on the most valuable information. In an ideal world, you’d have 100 percent controls across everything based on your policy, but you’re just not going to get to it in time. You wouldn’t get to it from a cost perspective.”

When asked whether their organisation perceived that minimal efforts to protect low-value information made their organisation more secure, RetCo1 answered, “Yes, I do, because then you can actually put the resources where the valuable information is.” This relationship between minimisation techniques positively affecting the security of an organisation is important and is labelled P7d in Figure 7.2.

6.3 Strategic Impacts on Organisation

A range of business benefits can be achieved should the organisation take an appropriate approach to securing its information to avoid a security breach. These benefits are largely strategic in nature, relating to the organisation, not of a security nature. The benefits are grouped according to whether they benefit the organisation, a relationship with stakeholder in its environment, or were the result of engaging in
outsourcing. An explanation of all these concepts, which have been identified from analysis of the data, follows alphabetically.

6.3.1 Environmental Benefits

The following are a number of benefits that organisations enjoyed which affect external stakeholders and the relationships with them. They include maintaining customer trust, public reputation of the organisation, maintaining regulatory compliance, reducing the risk of litigation, and avoiding share (stock) price fluctuations.

6.3.1.1 Customer Trust

To summarise this section, a security breach can affect customer trust, although customers are forgiving.

StatGov1 took a pragmatic view of the impact from a security breach on customer trust, which in the context of government organisations would be citizen trust, stating, “it would have an impact on public trust, that is assuming that the public trusts government anyway … It certainly wouldn't enhance trust, that's for sure.” FinCo2 thought that the size of the breach affected customer trust, stating, “It depends on what the breach is …, but if [it was] significant, if we had a Yahoo-sized breach, customer trust will be totally killed.”

In a variation to this concept, ITCo1 did not view the impact from a security breach on customer trust that seriously, stating,

“They expect us to look after the data reasonably carefully. Is it going to be life-threatening? No, as long as we took reasonable precautions. It's not something that we need to go overboard about, but as long as we take reasonable precautions we should be fine.”
StatGov3 agreed, giving the reason as repeated security breaches inuring customers to loss of trust, stating,

“I think people are starting to become almost conditioned to the fact that there will be data breaches. I would have said, probably five years ago, it would’ve been high, but now, there’s kind of even a little bit of an expectation that it’s gonna happen.”

FinCo3 agreed that customer trust was important but noted that it was resilient, and history has shown that it can withstand the impact from a security breach, stating,

“Customer trust is the heart of a financial services business, so financial services organisations, particularly retail organisations, exist because customers trust them. If anything ever seriously damaged that trust, that would be very bad, and certainly that’s a significant underpinning of regulators’ public view about why financial services regulation is so important. The long-run lesson of the last 10 years of data breaches in the US, though, suggest that in the general economy, customer trust seems to be affected quite strongly in the short-term around a data breach. For example, Target saw a material reduction in revenue right after their data breach became public, but that cut isn’t typically sustained. The long-run experience of organisations like TJ Maxx in the US, and I think Target as well, is that after a reasonable period, their customer trust, in fact, returns to the prior levels despite having had a material data breach.”

**6.3.1.2 Public Reputation of Organisation**

*To summarise this section, a security breach can affect an organisation’s reputation, which can affect revenue if the breach is large enough.*
As well as customer trust issues in the event of a security breach, organisations often suffered damage to their public reputation. FedGov1 acknowledged this impact, stating, “one of our risks is reputation, a huge reputational risk, ... if we have a breach, it affects people's livelihoods because it's their work or their health”. EduCo2 placed significant emphasis on the impact to their public reputation in the event of a security breach, stating,

“The big one for an organisation like us is reputational damage, particularly if you’re dealing with research partners who have certain expectations that your collective information is safe.”

PharmaCo1 shared that being highly ethical had an impact on their decisions, and acknowledged the potential effect of a security breach on their public reputation, stating,

“It's very high. We're a highly ethical company. ... We are very concerned about breach and what that would do to our brand, and especially the nature of the breach. So, whether it's patient data or it's donor data, or it's loss of intellectual property, or denial of service, all of those things would have an impact.”

FinCo2 perceived that the size of the security breach made a difference in the impact on reputation, stating,

“It depends on the severity and the type of breach. When it comes to reputational impacts, we talk about things that are visible for a day to a week in the local press. What impact is that going to have? Negligible ... If it's a really big thing, ... and we're in the press for months, that's a different thing. That then has consequences where customers are starting to question if they're with the right organisation".
6.3.1.3 Regulatory Compliance

To summarise this section, a security breach causing non-compliance with regulators can negatively affect productivity or finances, although regulators are usually not too severe. A non-adversarial relationship with regulators is recommended.

Often organisations are required to maintain compliance with regulations, and a security breach can sometimes affect that compliance. PharmaCo1 took compliance very seriously, stating, “That’s very significant. A deviation with the drug agencies could result in a plant shut-down. It could be really serious.” MgtCo2 however thought that regulatory sanctions were perceived as insignificant, stating, “In Australia, where we have had privacy breaches, the biggest fines … that were imposed were on Telstra … and they were sub-million-dollar fines.” RetCo1 perceived that the significance of non-compliance with regulations depended on the information that was breached, stating,

“If we breach [customer] privacy or PII information, we’ve now got a regulatory stick associated with the Mandatory Data Breach Notification 2017 scheme, and if we don’t comply with that, there could be compliance issues”.

Reassuringly, most organisations recognised the importance of compliance with regulators, as StatGov3 stated, “I don’t think any organisations I’ve worked for have a risk appetite for doing something that’s illegal or in noncompliance with regulations”. TelCo2 advised that organisations should simply involve regulators as soon as possible in the event of a security breach, stating,

“We take that very seriously, and we work very closely with the regulators. So, if there was a data breach, my experience [with] what the regulator’s looking for is the early declaration, early advice of a data breach.”
6.3.1.4 Risk of Litigation

To summarise this section, risk of litigation can potentially have a severe impact on an organisation although cultural differences can mean the risk is low.

Although not top of mind for most research participants, there was a risk of litigation that could affect the organisation in the event of a security breach. FinCo3 explained, “litigation itself isn’t a primary concern for us. It’s more a side effect of all the other things that have gone wrong.” FinCo2 perceived that the risk of litigation was low, and questioned, “Whether it’s litigable … Are there grounds for litigation? So, terms and conditions tend to protect us [in] how we provide our services. I’d say [the risk is] low.” ITCo1 also thought the risk of litigation in the event of a breach was quite low, stating,

“we’ve been going 12 years and we haven’t been sued once, and it’s extremely unlikely that one of our clients is ever gonna sue us. They’d just sack us if they don’t like us or ask for their money back”.

FedGov2’s experience however was quite different, stating, “If you leak even one person’s information into the public domain, generally, they go and find a really good lawyer and take you to the wall.” PharmaCo1 had also noticed an increase in litigation, stating, “Yes, we’re seeing a lot more activism on the part of attorneys who are suing companies for breaches because of the effects on either individuals or share price.” ITCo2 thought there might be cultural differences between countries in attitudes towards risk of litigation, stating, “In North America, without a doubt, it’s significant, … and not that high here [in Australia].” RetCo1 agreed, stating, “Australia’s not a very litigious country the way America is”.
6.3.1.5 Share (Stock) Price Fluctuations

To summarise this section, a security breach can negatively affect the share (stock) price of publicly-listed organisations, also affecting internal employee incentive schemes, but generally it recovers.

Although privately-held organisations were incorporated, and the owners held shares, the research participants from privately-held organisations had no interest in share price, as ITCo1 confirmed, “We’re a private company, so the price of the shares is irrelevant”, continuing, “It’s relevant if we sell, but in the short-term it’s not relevant”. TelCo2 agreed, stating, “we’re government-owned, if we go to a listing, it would be high, but at the moment, it doesn’t affect us.”

Only research participants from publicly-listed organisations were concerned about their organisation’s share price being affected by a security breach. FinCo1 confirmed, “A security breach could affect our share price, absolutely it could.” FinCo3 gave some context about why a security breach affecting share price would be significant to the board and key executives, stating,

“Share price is a factor in the sense that, as far as I’m aware, the CEOs of all publicly-listed companies have total shareholder returns somewhere in their scorecards and weighted quite strongly”.

TelCo1 noted the alignment between a security breach, those directors accountable in the boardroom, and share price fluctuations, stating, “This whole data security, data breach, is so pervasive, which is why it is one of the hottest topics on board agendas at present.” FinCo2 was circumspect however on how much of an impact a security breach would have, stating, “Evidence says that share price takes a short term hit and then recovers in a relatively short time frame.”
6.3.2 Organisational Benefits

The following are a number of benefits that organisations enjoyed which were internal and related directly to the organisation itself. They include avoiding bankruptcy, maintaining the confidentiality, integrity and availability of information, reducing expenses, maintaining the reputation of individuals, avoiding loss of life, maintaining operational productivity, organisational security, probable loss mitigation, and protection of trade secrets.

6.3.2.1 Bankruptcy Avoidance

To summarise this section, a security breach can affect an organisation's reputation so much, it goes bankrupt.

On some rare occasions, organisations can be involved in a security breach that is so significant, they go bankrupt. This can be for a few reasons such as reputational damage or loss of IP, but overall StatGov2 agreed with the effect of a major breach, stating, “You’ll lose the business, go bankrupt”. On loss of IP, ResCo1 stated, “If you had a very competitive environment, where your IP, your bread and butter, is all in electronic format, and if you lose that, then you’re going to run out of business.” On whether a security breach could severely affect an organisation's public reputation, StatGov3 cited the story of Cambridge Analytica misusing Facebook data and then filing for insolvency, agreeing that reputational damage from a security breach can be so severe that it leads to bankruptcy, stating,

“[one] of the impacts could be that the organisation could go out of business. If I think of the recent Facebook one with Cambridge Analytica firm in the UK. Maybe the reaction to that would mean that nobody would want to deal with them as a service provider anymore.”
6.3.2.2 CIA of Information

To summarise this section, a security breach affecting confidentiality, integrity, and availability, of core information can be catastrophic.

The confidentiality, integrity, and availability (CIA) of information was perceived as a key concern by almost all research participants. FedGov2 was clear when stating,

“"I'm an old-school security guy. I started with the CIA, the towers of security, and if you talk about the CIA, towers of security, then I'm right up there: confidentiality, integrity, availability of information. Definitely ... the core tenants of protecting your environments, your data, your people.""

RetCo1 agreed, stating,

“"By the nature of a breach, it'd mean the confidential information that I didn't want public is now made public, so the confidentiality has been breached. ... The integrity of the information can no longer be trusted as well because we know that somebody was there that might have changed something, and it could impact the availability because they might have deleted the database. So, a breach, by nature, could impact all of those.""

EnerCo1 clarified that the importance of CIA on information however depended on its utilisation within the organisation, as not all information has the same value, stating,

“"It depends on the system because some of them can be low, but if it was a breach of our [energy] generation plant, for example, that can actually be very high, catastrophic.""

6.3.2.3 Expenses Reduction

To summarise this section, lowering the value of information can reduce an organisation's expenses.
Organisations should always be keeping a focus on minimising expenses when considering deploying initiatives in a security framework. StatGov1 believed that taking steps to lower organisational risk by lowering the volume or value of information resulted in cost benefits, stating,

“It would benefit the organisation – it may be that there would be a way to lower the inherent risk that would be more cost-effective than other ways of mitigating that risk. So, for example, destroying anything over seven years old, meaning that data no longer exists, may be a less expensive option than storing it offsite in someplace secure for a long period of time. So yeah, there could be a cost benefit there.”

6.3.2.4 Individual Reputation

To summarise this section, a security breach can affect an employee’s or customer’s reputation, which would have a consequential effect on the organisation’s reputation.

A distinct theme that emerged from the data was the idea that as well as affecting an organisation’s reputation, a security breach can negatively affect an individual’s reputation. PharmaCo1 confirmed, stating, “It could quite frankly affect individuals negatively.” FedGov1 regulated practitioners in an industry and noted the potential impact from a security breach on a practitioner’s ability to practice, stating,

“If information got out, there could be personal harm to people. Not only reputation to us, but people’s reputation... it’s not just our reputation, it's people’s reputations as well, and their livelihoods, potentially.”

StatGov1 also took the view that a security breach could have a devastating impact on the reputations of individuals whose information they held, stating,

“The information we store for our customers is highly sensitive, so health information, child protection information, justice information. The release of
that kind of information could have a very, very detrimental impact on individuals whose information it is”.

FedGov2 noted the impact of a security breach on the employee in charge of security at an organisation, stating,

“in the actual security world, if you’re in an organisation that’s had a major breach, and you’ve been at the helm when that’s happened, you generally find it really hard to find another job anywhere else, not in security, at least.”

6.3.2.5 Loss of Life Avoidance

To summarise this section, in the modern age, a security breach can kill people.

In one of the most serious consequences from a security breach, people can suffer health problems up to and including death. All research participants agreed this concept was serious. AvCo1 was clear in stating, “if you look at the ASX top 50 [stock market], we're the only one that operates with threat to life from a cyber security perspective. We’d take that, obviously, seriously in that respect.” EnerCo1 agreed, stating, “if it affected, health and safety and environment. … that would be a problem for us.” StatGov2 gave a range of examples, stating, “loss of life, someone can die. In a hospital … if they crashed the operation theatre, somebody can die. Maybe they can hack into a plane and make it crash.” ResCo1 pointed to the recent example of Stuxnet being used to manipulate an environment, to show that the precedent had been set and that in this modern age, it was now possible to target people, stating,

“People. Operational technology control systems that manage physical things, … where people are working. Those things can be affected. It can cause physical harm to people. The equivalent of Stuxnet. It does harm to people.
That harm machinery causing the failure that impacts other things in the environment."

For-profit organisations weren’t the only ones concerned with loss of life, as this had a bearing on some government organisations as well. FedGov2 elaborated, stating,

“I think we’re in a unique situation where we do put people in harm’s way, so we take the risk component extremely seriously. When you look at the cost of losing some personal information that might allow a person to be targeted for a phishing attack versus losing personal information to the degree that those people in harm’s way are compromised and could potentially be put in a really dangerous situation or lose their lives, it’s a completely different risk assessment to undertake.”

PharmaCo1 took the view that poor planning could have disastrous security consequences, with an example being the location of a security operations centre, stating,

“high-risk countries, or even locations in a city. There are certain parts of the city where you wouldn’t want to have your information assets stored, if only because it’s difficult for employees to operate there effectively. They also have personal risk as well for the staff operating centre.”

**6.3.2.6 Operational Productivity**

To summarise this section, a security breach can disproportionately affect operations, lowering productivity.

Organisational productivity can be negatively affected in the event of a security breach, as employee resources are often redeployed internally to remediate the situation. FinCo2 explained, stating,
“Productivity. If we had a serious incident, there’s a serious breach, we would end up assigning a significant workforce to work out what happened, and respond and recover from that sort of activity, and that would require engagement of media outlets, our regulators, our technology teams, our business teams to go and talk to customers. It would be a massive hit on productivity. Instead of working on new things, we would basically go into holding pattern for a period of time while we suffer the storm.”

EnerCo1 identified that various resources can have their productivity affected, not just employees, such as their manufacturing plants, stating,

“I’d say generation sites is probably the big thing. I suppose … if [Supervisory Control and Data Acquisition] SCADA systems got ransomwared … stopping our manufacturing plants, where we manufacture electricity, that’s a big thing.”

6.3.2.7 Organisation Security

To summarise this section, organisations can increase their security by protecting information, reducing the value of information held, gaining access to security controls in an outsource partner, and minimising efforts to secure information to prioritise budget towards valuable information.

FinCo2 held a lot of high value information so for their organisation, security was commonplace and a high priority, stating, “We’re fairly mature as an organisation, in terms of protecting data and our information security safety, so for us, the bar is very high.” ITCo3 agreed that protection of high value information could make an organisation more secure, however equally thought that lowering the value of information held made the organisation more secure, “In the same way that a bank that holds no money is a less attractive target to rob.” ITCo4 thought that most
organisations would be more secure by outsourcing the management of their information to an outsource provider, stating,

“For most organisations, I think storing any information in an outsource provider, provided they’ve done their due diligence and understands how that provider protects their information and their services, is going to be more secure.”

RetCo1 believed that taking minimum efforts to protect low-value information made their organisation more secure because that allowed the redistribution of limited security budget towards higher priority initiatives, stating, “Yes, I do, because then you can actually put the resources where the valuable information is.”

6.3.2.8 Probable Loss Mitigation

To summarise this section, organisations can avoid huge clean-up costs after a security breach by preventatively implementing security controls and purchasing cyber insurance.

Probable loss mitigation involves the preventative actions that organisations can take to reduce the risk of incurring significant sums of money on remediating ICT systems after suffering a security breach. According to FinCo1, it is probable that all organisations will suffer loss from a security breach, stating, “it’s not if, but when.” In the words of ITCo4, preventative actions help to avoid future costs, stating,

“things like clean-up, marketing, and forensics, and security, and a range of other activities that they potentially would not have had to spend on should they have done baseline security and delivering a range of other things upfront.”

PharmaCo1 acknowledged that the direct cost of responding to a security breach can be significant, stating,
“Just the clean-up of a major breach is very disruptive. So, there's the initial breach, there's the loss of information, and then there's the clean-up. And then, there are the preventative controls that have to be put into place afterwards. You can do all of this in a planned way, but what tends to happen is a breach causes you to rethink everything. You've seen the papers where XYZ company’s been hacked, and now, they're spending $150 million to remediate.”

RetCo1 agreed, segmenting the impacts into three separate areas, stating,

“Depending on what it is, the cost of recovery could be significant because the tail could be very long. As soon as you suffer a public breach … you're going to have 25 million regulators, auditors, and everybody else and their dog on you, and the associated costs with responding to all of those … Secondly, the tail of this in terms of how long people are going to complain or blame you for something that’s happened to their personal life … could be a couple of years. There’s also potentially litigation from a class-action lawsuit … that could take years to solve as well.”

ITCo3 thought that financial loss in the event of a security breach would likely result in a small sum, however acknowledged that some larger organisations had spent considerable sums on restoring ICT systems, stating, “the direct cost of responding to [a breach is] generally going to be low. Unless you’re Maersk and managed to torch $300 million somehow”.

So, if the cost of responding to a security breach is acknowledged as significant, the question then becomes, how can organisations prevent this situation? ITCo4 described it as, “things like unexpected costs associated with a security incident that … they would not otherwise have had to spend if they'd done the right things in the beginning.” RetCo1 pointed to cyber insurance as a possible option for mitigating the
risk of clean-up costs, stating, “elements of that you can obviously insure for”, continuing,

“The only thing I advise my organisation to insure against is the costs associated with getting people in to come and help contain or mitigate or investigate the particular breach because that could be significant, and it could be unbudgeted, which could have an impact.”

6.3.2.9 Protection of Trade Secrets / Intellectual Property / Competitive Advantage

To summarise this section, organisations can suffer significant financial impacts from a security breach to trade secrets, requiring excellent security to protect them.

The loss of trade secrets or IP can lead to a loss of competitive advantage and market position, through leakage of trade secrets to competitors or a decrease in revenue. MgtCo2 gave an example, stating,

“For example, if there is a data breach … in the mining sector, information around their digging, their next geospatial data, where the next multiple years of millions of dollars of mining revenues are going to come from then, yes, it does have an impact.”

StatGov3 acknowledged that a range of industries typically hold trade secrets, stating, “Pharmaceuticals put a lot of time into research and development, so IP theft there would be high [importance]. Even automotive industry and definitely defence industries as well.” FedGov2 had experience with the effects of organisations losing trade secrets to well-prepared competitors, stating, “We’ve certainly seen in the past, organisations who’ve suffered some sort of breach, lose a lot of business to a competitor who’s got a rock-solid security model.”
6.3.3 Outsourcing Benefits

To summarise this section, there are many benefits should an organisation engage in outsourcing.

There are a range of benefits should an organisation decide to outsource the storage or management of its information. These benefits include ability to work flexibly, access to contemporary services, agility and speed of consuming services, availability, evergreen infrastructure, economies of scale, increased capabilities / skills / maturity, increased collaboration, increased security, reduced cost, reduced workload on internal employees, redundancy and resilience, and reliability. They are all discussed in the following sections.

6.3.3.1 Ability to Work Flexibly

The nature of cloud-based ICT infrastructure means that users can access to these systems from anywhere in the world. StatGov1 clearly saw some of the benefits of moving information involved the capability for employees to work more flexibly, stating, “Contemporary services, availability anywhere, these are the advantages of the cloud”, continuing,

“I feel I'm going to be getting very significant business benefit as a result of moving into Office365 because it offers a range of services that we currently don't have that should allow us to collaborate better and work more flexibly than we currently do.”

ITCo4 contrasted traditional outsourcing where an external outsource facility hosts multiple organisation’s information and entire business processes, with ICT infrastructure as a service, stating, “the benefits are, you get scale, you get flexibility, you get the ability to dynamically scale up or down your storage requirements based
on your needs at the time”, continuing, “it’s really subscription-based services which gives you the ability to have that flexibility.”

6.3.3.2 Agility and Speed of Consuming Services

External cloud-based services are available to be consumed on-demand all-day, all-year. This increases the speed by which they can be accessed, which then increases organisational agility. FinCo1 acknowledged this was a key driver, stating, “the driver [is] the operational efficiencies and the agility of consuming services.” StatGov2 agreed, stating, “The benefits, number one, is … what you want, … you can get really fast”. StatGov3 perceived there were other benefits to high speed, stating, “you also are able to spin-up additional storage at a fairly minimal time delay. That can present a lot of benefits.” FinCo2 perceived that this speed improved the organisation’s time for bringing products to market, stating,

“When we start to use other people’s compute environments …, we are up and running with those functions a lot quicker. So, time to market, time to functionality, speed, agility.”

6.3.3.3 Availability

As well as external cloud-based services being available from anywhere in the world, services are also available for a higher percentage of time. StatGov1 agreed that benefits include services being available from any country, stating, “availability anywhere”. ITCo3 saw benefits in having skilled service personnel from the outsource vendor monitoring the service continuously, stating,

“You’d outsource it because it’s much easier to get 24/7 operation and continuous monitoring when it’s outsourced, and you’ve got around the clock support and follow the sun and everything else than it is do that yourself.”
6.3.3.4 Economies of Scale and Scope

Outsource vendors typically gain economies of scale and scope by specialising in outsourcing. FedGov1 stated, “I think it’s economies of scale. You should be able to get something that’s better than what we can provide with a bunch of five or six people, in my view.” ITCo3 explained how outsource vendors achieved economies of scale and scope, stating,

“So, the only way that this whole market works is if there is a lot of shared cost and shared infrastructure, and effectively, the best we’ve come up with out of that is outsourcing. The classic example being email. Anyone at the moment that is still hosting their own mail server is insane. Just give it to Office365, give it to Gmail, give it to Amazon WorkMail. It’s just completely implausible that you are going to be able do a better job than they are.”

AvCo1 identified that one of the motivations for outsourcing is difficulties with retaining skilled staff, and outsource vendors with their economies of scale could address this, stating,

“I mean, if you do it more cost effectively, that’s the key thing. … one of the biggest problems is having skilled staff who understand how to manage those environments and keeping them trained and everything else to manage those environments.”

ITCo4 identified a range of benefits including economies of scale, stating,

“the benefits are, you get scale, you get flexibility, you get the ability to dynamically scale up or down your storage requirements based on your needs at the time. And you don’t have to go buy a whole bunch of infrastructure. Therefore, compare that to standard on-premises-type environments, you don’t have to have extensive lead times while you get
funding, CapEx approval funding, projects established, lead times for the delivery and implementation of hardware."

EduCo2 expanded on a benefit of outsourcing to cloud being cost savings from the economies of scale and scope, stating,

“if you include the capital cost of having to renew your own environment added together with the operating expenditure that is typically required to maintain them yourself, over the course of the life cycle, there is an arguable cost saving in moving.”

FinCo3 noted that accessing outsource vendors with their economies of scale and scope improved process maturity, stating,

“In terms of service outsourcing, as opposed to resource augmentation, I think outsourcing can allow you to access service providers that operate at greater economies of scale, which benefits both in terms of cost reduction by comparison to doing it yourself, but also process maturity by comparison to doing it yourself.”

6.3.3.5 Evergreen Infrastructure

One of the benefits of using outsource cloud environments is that their maintenance patching for hardware and operating systems is constantly up to date. This eliminates the need for organisations to hire employees with necessary skills and patch systems themselves. StatGov1 used the term ‘evergreen’ to describe the nature of these current systems, stating, “Contemporary services, availability anywhere, … evergreen environment, so we're not having to upgrade things ourselves, … The cloud will give us that.” FedGov1 identified that aging internal ICT systems was a motivator for accessing the evergreen environment in cloud, stating,
“when I first took over the IT section – we had a lot of issues with our systems, very unreliable, so there hadn't been investment in the facilities. So, one of the reasons we outsourced our infrastructure facilities was to get business-grade facilities, to be quite honest with you.”

ITCo2 related an example from a historical personal story, stating,

“a little company …, and they had a server and never backed up the server. … If something ever happened to it, they were screwed. But by having that in the cloud, somebody was maintaining it, somebody was keeping the versions up to date.”

FinCo4 perceived that outsource vendors having many skilled employees keeping their systems evergreen meant that the vendors and customers benefited from the aggregated knowledge, stating,

“When it comes to using outsourced services …, some of the benefits are that it is evergreen, … and it is Microsoft’s core business, [so] there is a cumulation of knowledge that comes from having millions of customers.”

6.3.3.6 Increased Capabilities / Skills / Maturity

AvCo1 identified that a motivator for accessing outsource services was the latent pool of skilled resources, stating, “one of the biggest problems is having skilled staff who understand how to manage those environments and keeping them trained … to manage those environments.” StatGov1 agreed that a gap in internal skillsets meant that accessing outsource services was attractive in addressing that, stating,

“I feel I'm going to be getting very significant business benefit as a result of moving into Office365 because it offers a range of services that we currently don't have that should allow us to collaborate better and work more flexibly than we currently do. So yeah, I would pay a small premium for that.”
TelCo1 thought that security skills were in short supply and that using the services of an outsource vendor could address that, stating,

“Skill shortage in Australia is definitely [an] issue. And by that, I mean competent people to manage the capability required to reduce the security risk, skill shortage. The cost of skills here is highly significant, cost of labour.”

PharmaCo1 agreed, stating, “in cyber, there’s a real shortage of cybersecurity personnel with the right skills. You go to a consulting firm or an outsourcer really for two reasons: skills or bandwidth”, continuing,

“looking at available skills, let's take big data, Hadoop, MongoDB and the data lakes … You may want to turn to an outsource partner that specialises in the management of those kinds of environments, and even provides … access to data scientists who do basic analysis.”

ITCo4 perceived that the benefit of accessing skills externally was that internal staff could be redirected to focus on business functions, stating,

“An organisation needs skills in designing and building applications and how they … manage and handle their data. They don't necessarily need to have expertise in managing things like storage.”

FedGov3 agreed, stating,

“In one sense, why should a medium-sized organisation that specialises in building car widgets, why do they also need to be experts in securing their systems because this is something that’s common to absolutely every business and organisation, but that’s not what they specialise in. That's clearly the benefit of outsourcing.”
6.3.3.7 Increased Collaboration

Collaboration can be facilitated by cloud-based platforms to increase communication internally between employees but also externally with other stakeholder groups such as customers and suppliers. StatGov1 perceived that their employees and their customers would be able to collaborate better by using external outsource facilities, stating,

“I feel I'm going to be getting very significant business benefit as a result of moving into Office365 because it offers a range of services that we currently don't have that should allow us to collaborate better … than we currently do.”

TelCo1 perceived that collaboration advantages increased internally between partnered supplier organisations, as well externally between employees, stating,

“we don’t call it outsourcing. We call it team building. What we call it is, we are extending the team. If I’m going to use, hypothetically, Accenture, the Accenture contract is: come on-board, sit with us, and they don’t get separate lanyards. They are not identified differently. They are part of the team, not just professionally but socially.”

6.3.3.8 Increased Security

Given large outsource vendors trade on their reputation, ensuring the security of their cloud services is world-class was a primary focus. StatGov1 acknowledged the disparity in levels of security, stating, “I'm making an assumption, but I'm almost certain that Microsoft’s environment is gonna be more secure than anything I can do internally.” PharmaCo1 agreed that an outsource vendor should have better security, stating,
“In terms of a cyber risk, assuming you picked a credible outsourcer, you have essentially a similar risk profile. Often, an outsourcer can do a better job of protecting data than a business can.”

ITCo4 saw increased security as a benefit of using outsourcer services, stating, “Additional security for no extra cost.” StatGov2 agreed and added that often the customer can dictate the level of security required, stating, “you can … include in the contract what security you need, and they can provide you with all that.” EduCo2 acknowledged that outsource vendors weren’t perfect, but was certain they had world-class security, stating,

“more secure environments that the big outsourcers or the big cloud-providers can potentially provide. Now, … they’re [not] bulletproof because as much as they run … triple-redundant data centres with full encryption, there’s always the potential for someone to come up with some innovative new way of finding a way around their arrangements. … But broadly speaking, because of their scale, … we’re talking about multi-billion-dollar or trillion-dollar organisations who spend enormous sums each year managing their environments to make sure that they are secure because their business reputation depends on it. The main benefit I would point to, in terms of moving information to the cloud … is that … they are more secure environments than what we could possibly hope to run internally."

6.3.3.9 Reduced Cost

Most research participants perceived that use of outsourcer services was a cheaper alternative to operating an internal ICT environment. The problem with running an internal environment was that if an organisation was going to manage an ICT environment internally, then they had to do it well, which meant an exorbitant expense to commence. Organisations can take advantage of mature ICT
environments by purchasing cloud services based on how much they used the environment, not a fixed cost regardless of whether they used it or not. ITCo2 agreed, stating, "I think there can be considerable benefits … [like] lower cost". ITCo1 noted the lack of capital expense for ICT hardware, stating, “It’s cheaper. You don’t have to pay for hardware.” PharmaCo1 also perceived that organisations might want to avoid the capital expense of establishing an internal environment, stating, “Typically, outsourcing is done because of a cost issue. In terms of IT outsourcing, it’s done as a cost-avoidance issue.” FedGov3 insightfully noted that as well as reducing cost, using the services of an external cloud vendor reduced risk, stating,

“reducing the inhouse cost, both in terms of financial and human resources. I mean, you don’t have to maintain those skills inhouse, and you don’t have to pay for it. You’re paying someone else to do all that, organise the expertise and carry the risk.”

EduCo1 agreed with the reduced cost premise, stating, “Lower cost of service, obviously.” FinCo3 also perceived that accessing external ICT services could reduce costs, stating,

“I think outsourcing can allow you to access service providers that operate at greater economies of scale, which benefits … in terms of cost reduction by comparison to doing it yourself”.

6.3.3.10 Reduced Workload on Internal Employees

Often organisations can reduce ICT workload on internal employees by using the services of an outsource vendor. StatGov1 explained, stating, “Contemporary services, availability anywhere, these are the advantages of the cloud, evergreen environment, so we’re not having to upgrade things ourselves.” ITCo1 identified a large range of activities that are required to operate internal ICT environments, stating,
“It’s a hell of a lot more reliable every time than you doing it yourself. When something goes wrong, you’ve got it to get it fixed, you’ve got to get someone in, and you’ve got to find someone who’s got the expertise, which means you’ve got to have a relationship, whereas with something like Google, it just works. It works every time. And when it’s got an outage, if Google has a five-minute outage then it’s world-wide news. When I had an outage, we had a system and we had internal, and it was two weeks to fix it because we had to reboot the damn server and everything else, and our email was down for that period of time.”

6.3.3.11 Redundancy and Resilience

Large external outsource facilities often have mature disaster recovery plans and can restore services quickly, leading to greater redundancy and business resilience. StatGov1 agreed, stating, “greater redundancy in terms of data recoverability. The cloud will give us that.” FedGov2 had a primary focus on monitoring and detecting security breaches for their public-facing systems, stating,

“We have tools that we’ve developed to maintain the integrity of our external facing websites. If they ever get compromised or defaced, then they get taken back to a last known good state immediately … And we’re very heavily engaged in ensuring that that public presence is maintained in a good state.”

ITCo4 also had processes established to restore services quickly if their outsource vendor suffered an outage, stating,

“to have data portability so that if something happens inside the outsourced environment, they can potentially bring that data back into their on-premise environment, or some other service provider, and get it up and running again really quickly.”
6.3.3.12 Reliability

Since external ICT outsource vendors primarily focus on the availability of their services to generate revenue, the corollary is they are therefore more reliable. ITCo1 explained, stating,

“So, going with someone like Google just means it's a hell of a lot more reliable. ... and it just works. It works every time, and there's really no problems with it. And if there is a problem, they get right on it and you get it fixed within a heartbeat, so there’s just no comparison.”

6.4 Chapter Summary

This chapter describes the findings from analysis of the data, providing a rich description of the concept of information security strategy, analysed for its properties and dimensions, noting any variations throughout. After the data were analysed, related analyses were aggregated into categories, which were integrated and then interpreted in relation to the overall research question. “The quality and contribution of one’s work depends upon the depth and breadth of the investigation” (Corbin & Strauss, 2008, pp. 273). Table F.1 in Appendix F summarises the findings from the analyses of the concepts discovered. Table F.2 in Appendix F summarises the relationships that were discovered between the concepts.
Chapter 7: Discussion

The substantive theory put forth in this chapter\(^3\) is that, based on certain antecedent conditions, the appropriate selection and use of an information security strategy will guide the optimal storage and use of information held organisation-wide, leading to positive strategic organisational impacts. This section describes the generic strategies in the proposed theoretical model, the relationships between them and different strategic impacts on the organisation, and practical advice on how to select one. One definition of a theory is “a statement of relations among concepts within a boundary set of assumptions and constraints” (Bacharach, 1989, pp. 496). The theory is built around a core category, which in this thesis is “approach to securing information”, but “theory doesn’t just build itself; in the end, it is a construction built by the analyst from data provided by participants” (Corbin & Strauss, 2008, pp. 266).

This chapter constructs a theory on information security strategy based on the findings from the data collected and analysed previously in chapters two, four, five and six. To reiterate, the intent of this research program is to engage in theory building, not theory testing which is suggested as a future research direction for the completed model using statistical studies. Based on the principle of Ockham’s razor, building simpler theories is generally preferable, even though a fundamental trade-off between simplicity and fecundity of data must be made (Gregor, 2006; Weber, 2012).

\(^3\) Elements of this chapter are published in the following peer-reviewed articles:


7.1 Chapter Aim

The aim of this chapter is to combine findings from the literature review described in Chapter 2, with the substantive categories generated from the data collection and analysis described in Chapters 4-6, to advance to theoretical knowledge (Evans et al., 2011; Strauss & Corbin, 1990). It is this relating of concepts together instead of simply listing them that raises findings to the level of a theory (Corbin & Strauss, 2008). This chapter establishes a grounded theory on information security strategy based on combining the core category “approach to securing information” with other substantive categories. This theory on information security strategy argues that balancing the strategic nature of core information with constraining environmental conditions guides the selection of an appropriate information security strategy. This section explains the theoretical model of information security strategy including its various elements and describes them based on the structural components of a theory for explanation and prediction (Gregor, 2006). It continues by providing the contextual background, then proposes a theoretical model of information security strategy, with an overview, examination of theory type, assumptions, structural components, means of representation, constructs, statements of relationship, scope, causality, testable propositions and prescriptive statements.

7.2 Overview of Theory on Information Security Strategy

This theory involves the selection of one appropriate information security strategy to secure all of an organisation’s information-based resources so they can continue to be used towards the achievement of organisational goals. The selected strategy may then be used to inform a strategic plan guiding operational-level decisions about selection of usable ICT infrastructure and security controls for the protection of organisational information against threats. The strategy is chosen according to the strategic nature of the information to be protected and extrinsic organisational
constraints, including on outsourcing. The overall goal is to protect information according to its strategic value, with non-valuable information still being protected but potentially with less expensive controls. Strategically valuable information requires more comprehensive and expensive controls to protect it, which may be sourced externally.

7.3 Theory Type

There are five types of theory which include 1. analysis, 2. explanation, 3. prediction, 4. both explanation and prediction, and finally 5. design and action (Gregor, 2006). The theory on Information security strategy is a variance-type theory based on the fourth category, for explanation and prediction. An explanation and prediction type of theory describes "what is, how, why, when, where, and what will be" (Gregor, 2006, pp. 620). Contributions to knowledge embodying this type of theory typically offer predictions with testable propositions and causal explanations (Gregor, 2006).

7.4 Assumptions

The assumptions underlying information security strategy need to be stated explicitly to reduce any inferential errors that may result from using biased formative assumptions. By making assumptions explicit, their legitimacy can be debated and agreed upon prior to the utility of any proposed theoretical model being established. Failure to take assumptions into account threatens the validity of any resultant theoretical model (Roberts et al., 2012).

First, information security strategy depends on organisations being motivated to secure information. If an organisation is not motivated to secure information, then any processes protecting information will not be implemented. Some of the motivations include the ownership of trade secrets, obligations under regulatory compliance, and adherence to international standards for information security.
Second, the theoretical model of information security strategy depends on organisation choosing the least cost alternative. Given two competing alternatives for security controls that would achieve the same level of security to protect information, the cheaper of the two should be selected by an organisation. Cost reduction is a guiding principle that affects all procurement decisions for security controls.

Third, information security strategy depends on an organisation first identifying and classifying information according to its varying sensitivities and value. Without an understanding of whether the organisation holds trade secrets for example, an appropriate strategy cannot be selected. Information must first be classified to allow fidelity in a strategy selection.

7.5 Structural Components

Many researchers have formed a position on what a theory is and is not, and what the structural components of a theory are (Bacharach, 1989; Gregor, 2006; Grover, Lyytinen, Srinivasan, & Tan, 2008; Weber, 2012). Often researchers will describe the parts of a theory including constructs, relationships, conditions, actions, with a complete theory having significance, originality, succinctness, and the ability to be falsified (Weber, 2012). Given this theoretical model of information security strategy is designed for practitioners, this paper adopts the structural components of theory for an explanation and prediction theory, including diagrammatic means of representation, the primary constructs, some statements of relationships between constructs, scope, causal explanations, testable propositions and prescriptive statements (Gregor, 2006). These components are described in the following sections, beginning with a diagrammatic means of representation.
7.6 Means of Representation

One component of a theory that is required is a depiction of the theory in some way, such as a diagram, table, picture, narrative, or model (Gregor, 2006). In this thesis, the theory on information security strategy is represented diagrammatically (Gregor, 2006). Figure 7.1 offers a visual depiction of the four generic strategies included in this theory and the factors that influence their selection:

![Diagram showing four generic information security strategies: Devaluation, Fortification, Minimisation, Outsourcing, based on Information and Organisational Context]

*Figure 7.1. Generic Information Security Strategies*

*Information* is a category code indicating dimensions using an ordinal scale that refers to the value associated with information, which can be negligible or up to critical in the case of trade secrets. *Organisational Context* is also a category code indicating dimensions using an ordinal scale, that refers to external factors that might preclude an organisation from outsourcing the storage or management of its information, which either exist or don’t exist.
7.7 Primary Constructs

The phenomena of interest relate to the concepts identified during the open coding and reassembling of data about the approaches taken to securing information and include four generic strategies: Fortification, Devaluation, Outsourcing and Minimisation. The construct names are in-vivo codes adapted from statements made by research subjects during their data collection interviews and were subsequently employed during model formation (see Table 7.1). They map to the four main concepts discovered during data analysis that describe the ways that organisations typically approach securing information.

<table>
<thead>
<tr>
<th>Concept Codes</th>
<th>Category Codes</th>
<th>Representative In-Vivo Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing valuable info</td>
<td>Fortification</td>
<td>ITCo1: “to store valuable information, you probably have to fortify your defences, fortify your infrastructure”</td>
</tr>
<tr>
<td>Evading trouble</td>
<td>Devaluation</td>
<td>ITCo1: “we’ve taken the deliberate approach of devaluing the information that we have.”</td>
</tr>
<tr>
<td>Getting help</td>
<td>Outsourcing</td>
<td>StatGov3: “Well, outsourcing, generally, it can provide enhanced security.”</td>
</tr>
<tr>
<td>Accepting the risk</td>
<td>Minimisation</td>
<td>ITCo3: “Minimum viable security is: what do we need so that if something goes wrong we’re not seen as being horribly negligent? I think that is the baseline that gets applied to low-value information and rightly so.”</td>
</tr>
</tbody>
</table>

7.7.1 Fortification

The Fortification strategy applies where the value of information held by an organisation cannot be reduced and barriers to outsourcing it also exist. Barriers to outsourcing may include the irreplaceability of trade secrets, which should be termed strategic information due to its utility in the pursuit of organisational goals. The organisation must protect this valuable information by applying additional security controls to mitigate the risk of a security incident and typically cannot outsource its
management. The higher the information’s value, the greater the need for comprehensive security controls to reduce the likelihood of a security breach (McFadzean et al., 2007). The disadvantage of the Fortification construct is that it comes with an associated expense burden, both in financial terms and human capital.

### 7.7.2 Devaluation

The Devaluation strategy intends to increase security by lowering the value of the information held, either by (1) avoiding holding valuable information in the first place, (2) tokenising information, or (3) expunging old information. Tokenising information refers to the practice of substituting valuable information with a non-sensitive identifier, referred to as a token, which has no exploitable value. By not holding valuable information, the organisation becomes more secure against threats because there is less impact on operations from security incidents. Organisations also avoid the expense associated with the protection of valuable information. This is a novel, almost counter-intuitive aspect to this thesis.

An illustrative example that might be used to explain the Devaluation phenomenon is where retail shops put an empty cash register till in their front windows overnight along with a note stating, “No Cash Held on Premises”. This causes the shop to be more secure and the reason is the deterrent effect, where attackers may read the note through the window, then decide to pass the shop by and not force entry. This is due to a perceived imbalance of required effort versus potential gain, where the attacker may perceive that too little will be gained from too much effort. An interesting implication in this example is that there is a feedback loop to the attacker (i.e. the note in the window) to let the attacker know that there is nothing worth stealing, without which this technique may not work. The threat emanates from a human source, where the motivation to attack and decision-making is arbitrarily controlled.
This differs for example from a bushfire, where the threat has no decision-making capability. Combining emptying the till with the message helps cause the deterrent effect, rather than simply emptying the cash register alone. It cannot be said to be true in all cases however, as the attacker might assign value to other items in the retail shop, so from a causality perspective, this deterrent can be said to reduce the likelihood of an attack due to the perceived lack of financial reward. By devaluing the information held, organisations can reduce the impact from a security breach.

### 7.7.3 Outsourcing

The *Outsourcing* strategy aims to increase security by leveraging storage infrastructure and security controls from external vendors. Benefits include gaining access to more highly skilled or qualified staff, an external provider’s larger security budget, and providing latent capacity and scalability. Outsourcing ICT infrastructure can take the form of secure and resilient ICT infrastructure, managed by a third party, with scalable security controls. A robust business continuity plan with cyber insurance to cover the costs of response to security incidents is required. Information hosted externally is perceived to be held more securely because vendors offering outsourcing services often have the advantage of scale and scope. Outsourcing comes with a loss of control however, and therefore, a possible increase in risk. There are several barriers to outsourcing (e.g. regulatory compliance, external threat environment) that may prevent the outsourcing of information externally.

Benefits that may be obtained include gaining access to highly skilled or qualified staff, external provider’s larger security budgets, and providing latent capacity and scalability. Outsourcing ICT infrastructure can take the form of secure and resilient dedicated ICT infrastructure, managed by a third party, with scalable security controls such as distributed-denial-of-service protection tools available. Information can be held securely by outsourcing its management because vendors that offer outsourcing
services have an advantage of scale and scope. A metaphor might be people who keep cash under their mattresses beginning to believe that banks can keep their cash more secure than they can.

Outsourcing comes with a loss of control however. For example, public cloud vendors that offer the use of shared computing resources have data centres that are typically located all over the world. Information stored in a data centre in one country can be backed up to a data centre in another country. In global vendors, technical support staff who work on the cloud infrastructure originate from many nationalities. Public cloud vendors often co-locate their computing and networking infrastructure in data centres that are owned by other companies and employ contractor support staff. Any one of these staff or organisations could pose a threat and they should all be considered during a vulnerability assessment.

An organisation’s contextual environment factors include both internal and external factors such as governmental laws and regulatory compliance (McFadzean et al., 2007). As stated previously in Section 2 Background, other contextual factors that could constrain the outsourcing of information include regulatory compliance, industrial, political and legal factors, external threat environment and the existence of valuable information (Baets, 1992; Banker et al., 2010; Baskerville, 2010; Beebe & Rao, 2009; Kayworth & Whitten, 2010; Kelly, 1999; Kim et al., 2012; Posthumus & Von Solms, 2004; Tutton, 2010). Any of these constraints may preclude the use of outsourcing.

7.7.4 Minimisation

The Minimisation strategic goal is to provide the minimum viable security for non-valuable information so that an organisation cannot be said to have been completely negligent in the event of a security breach. It provides a plausible defence for those responsible for organisational security controls from accusations from information
owners that insufficient protection was provided for the non-valuable information. It may take the form of hosting on cheap and efficient external public cloud and takes advantage of the security controls put in place by vendors with large security budgets and mature processes.

7.8 Statements of Relationship

Generic constructs have relationships amongst them that are labelled associative, compositional, directional and causal (Gregor, 2006). This theoretical model of OrgISS explained in the following passages includes causal relationships, not simply directional or associative (Gregor, 2006). This type of causal relationship describes where a change in one factor increases the likelihood of something else being affected and is best suited to the social sciences because of the open system of environmental conditions in an organisation that could affect the relationships, not all of which can be controlled for (Gregor, 2006). The statements of relationships described in this theory are not explained using operators of first-order predicate calculus (per the Once-Received View), as it would be a mismatch due to this theory’s alignment to social science not natural science (Craver, 2002).

In analysing the findings from data analysis, the properties of information and the way it is used, combined with organisational contextual conditions, both influence the approach to securing information within an organisation, and this has a variety of effects on the organisation’s success or otherwise. After conducting selective coding on categories, only the concepts that affect outcomes are depicted in Figure 7.2. Appendix G provides a summary of all the coding, moving from open concepts to axial categories, depicted as a data structure, with format adapted from Gioia et al. (2013). Integration of selective coding allowed for the focus of the model to be on core concepts and only the relationships that demonstrably affect the selection of an information approach (Glaser & Strauss, 1967; Wiesche et al., 2017). For example,
within the Information category, there were seven concepts and properties discovered from the data (i.e. asset, value, control, access to functionality, classification, location, ownership), however only value, control, and access to functionality appear in the final model, due to the existence of data that supported their relationships with an information approach (i.e. P1-P3). After conducting theoretical coding, Figure 7.2 offers a diagrammatic representation of the main relationships discovered from data analysis. To note, although all relationships depicted are uni-directional, real life is complex and after theory testing, some may actually be bi-directional, as noted in Future Research Directions in Chapter 8.

![Figure 7.2: Conceptual Model of Organisational Information Security Strategy](image)

See Table F.2 in Appendix F for a summary of concept descriptions and evidence of the relationships between concepts as depicted in Figure 7.2.

### 7.9 Scope

The scope of the theory on information security strategy in this thesis is a substantive theory, in that it is focussed within a specific area of inquiry of information security strategy and can be applied under varying conditions (Glaser & Strauss, 1967;
Urquhart et al., 2010). It is defined by the generalisability of the modal qualifiers used to describe the relationships between constructs (like all or some) and clarifications about boundaries (Gregor, 2006). In terms of statements that define scope, all organisational information must be protected by some controls. What this statement does not do is distinguish between lower-classification information and higher-classification information, which may require additional forms of security controls.

The boundaries of this theoretical model of information security strategy include all the infrastructure, networks and platforms where information is stored, organisational information and the people who work on the infrastructure and information. Protection of staff, infrastructure, networks and platforms is also known as computer security, information security or cyber security (Siponen & Oinas-Kukkonen, 2007). This theoretical model is designed to be used at the strategic or organisational level of an organisation, not the individual, group or inter-organisational levels.

7.10 Causal Explanations

Theory building depends on the detailed development of categories and their eventual integration to explain causality (Corbin & Strauss, 2008). This section gives causal reasoning statements about the relationships among the phenomena of interest. Causality can be explained in varying ways and the following list, with four types of causal analysis, supports causality in the information systems discipline (Gregor, 2006, pp. 617):

i. Regularity (or nomological) analysis, i.e. ‘A causes B’;

ii. Counterfactual analysis, i.e. ‘If not A, then not B’;

iii. Causal analysis, i.e. ‘A increases the likelihood of B’;

iv. Manipulation or teleological causal analysis, i.e. ‘If A, then B’;
Use of the terms *explanation* or *causal explanation* in this paper refers to the third type of causality, termed causal analysis, which is more suited to the social sciences (Gregor, 2006). This is due to research participants being employed at organisations, which lack the properties of a closed system such as identifying all variables and controlling for them in experiments.

The causal explanations for the patterns of decision-making observed by research participants are based on combining multiple concepts and relationships from *information* and *contextual conditions* categories, with different concepts from the approaches to securing information category and a description follows.

In this section, the seven concepts related to the core category *Information* are examined for not only their properties and dimensions, but the way that they interrelate. This understanding begins by identifying the goals of the organisation, as evidenced by the business strategy in their strategic plan. For the sake of edification, the term *business* is used here for a public organisation as well, using the understanding that government departments are in the *business* of providing services to citizens. Business goals are influenced by the vision and mission of the organisation, as well as any resources the organisation owns. The goals of the organisation are achieved through using resources which can include information assets. These information assets can take the form of trade secrets, intellectual property, or a customer database for example. The goal of these information assets then becomes to support the achievement of business goals. Identification of key information required to support the achievement of business goals is a key tenet in the evaluation of an information security strategy.

Organisations must then consider whether the goals for the use of information can be achieved without accessing the functionality or utility of an information asset. An illustrative example is the use of credit cards to facilitate a financial transaction
between the organisation and a customer. An organisation may gain surety about the efficiency of this transaction by holding the credit card details, by using an outsource supplier to hold the credit card details, or by not holding the details and accessing an external service such as PayPal to gain access to credit card details on demand. The functionality that the organisation desires is the use of the credit card details on demand to conduct a financial transaction. However, another viable option to conduct the financial transaction without accessing the credit cards on demand is to ask the customer to present their credit card during each purchase transaction. In this scenario, no credit card details are held by the organisation, an outsource supplier, or a specialist service provider such as PayPal, because the customer continues to hold (and secure) the credit card details. The customer may then decide to not present their credit card and the organisation must decide whether this risk is worth taking. In this example, the information goal of facilitating a financial transaction can be achieved without the organisation securing access to the functionality of the credit card on demand. This is representative of the Minimisation strategy.

Often, achieving the information goal without safeguarding access to the functionality of the information asset on demand is not possible so organisations must explore other options. Moving on, if an information asset is held by an organisation, then it must have an owner identified, as this person will be responsible for the lifecycle management of the information, i.e. its creation, protection, use, and eventual destruction (Tallon & Scannell, 2007). Decisions made about whether management and control of information can be shared with an outsourcing provider must be made in consultation with the information owner, as that person remains ultimately accountable. Decisions made to engage the services of an outsource partner will affect the location of the information, as the outsourcer may be required to hold and secure the information externally so that it can use the information to provide a service or benefit back to the organisation. The organisation must be able to trust
that the outsource provider can manage the lifecycle of information as well or better than the organisation, and if it cannot, then it must retain management of the information. This retention of information lifecycle management would be representative of the Fortification strategy. The decision to engage an outsource partner is also influenced by a range of potential constraints on outsourcing that may potentially negatively affect the organisation. If constraints exist, then an organisation will probably not be able to engage in outsourcing. There are also a range of enablers that can positively affect the decision to engage in outsourcing. A decision to engage an outsource partner is representative of the Outsourcing strategy.

Information does not always need to be owned by an organisation to derive benefit from it. From the earlier example, PayPal owns and stores credit card details and organisations can pay a small fee to access this service and achieve informational goals. This reduces the requirement for an organisation to own high-value information, which in turn reduces the possibility that high-value information is disclosed during a security breach. Reducing the impact of security breaches results in the maintenance of productivity in organisations. Organisations can also enjoy a range of other benefits at strategic level from a reduction or avoidance of security breaches, including environmental, outsourcing, and internal organisational benefits. Use of externally-owned information to achieve an organisation’s information goals is representative of the Devaluation strategy.

7.11 Testable Propositions

The following propositions relate to construct relationships that could be tested, although testing is outside the scope of this thesis. They form the basis of understanding the relationship between a generic information security strategy and strategic benefits to the organisation:
P7a: Fortification: If strategically-valuable information and constraining antecedents exist, and an organisation increases security controls, then the perceived security of the organisation will be higher.

P7b: Devaluation: If non-valuable information and constraining antecedents exist, where an organisation stores information externally or otherwise reduces the value of all internal information, then the perceived security of an organisation will be higher.

P7c: Outsourcing: If valuable information and no constraining antecedents exist, and the organisation procures externally-managed outsource services with adequate security controls, then the perceived security of an organisation will be higher.

P7d: Minimisation: If non-valuable information and no constraining antecedents exist, and the organisation stores information externally, then the perceived security of the organisation will be higher.

7.12 Prescriptive Statements

The following prescriptive statements in this section offer recommendations for practice, specifying the steps by which practitioners can assess the varying nature of information and organisational contextual factors, and then select a suitable information security strategy (Gregor, 2006). The following steps depend on eliciting relevant information from a business strategy document, which typically articulates the growth path for an organisation over the coming five years. It follows then that should the business strategy document be rewritten in five years’ time, then the information security strategy should also be rewritten, to ensure alignment with goals. This means that information security strategy development is a cyclical process to
produce a strategy which is documented in a plan, to facilitate enhanced understanding and distribution amongst stakeholders.

The practical application of this substantive theory requires that it be highly related to information security, that laymen employees can read and follow the steps, it must be general enough to apply to a wide range of organisations, and must allow practitioners partial control over everyday changes in their situation (Glaser & Strauss, 1967). The prescriptive steps adhere to these four principles and are explained in the following sections.

7.12.1 Step One: Information Discovery, Profiling and Classification

As part of an information discovery exercise, an audit should initially be carried out to identify all information that an organisation knowingly and unknowingly stores or uses. Organisations should use any of the auditing frameworks available to practitioners, to ensure integrity in the search for information.

The information audit catalogue should contain the name of the information, a description, whether it is a structured asset or unstructured data, its value and sensitivity, what systems and people have access to the information, what the information is used for, the information’s classification, its location, and its ownership.

With regards to classification, all information should be profiled and classified, for example into a classification system such as one that military organisations might use: UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. Alternatively, if the choice is available, a simpler classification system using PUBLIC, CONFIDENTIAL and SECRET is intuitive and easy to understand for stakeholders who interact with the information.
7.12.2 Step Two: Analyse Information for Strategic Purpose

The organisation’s current 5-year Strategic Plan or equivalent should be obtained and examined in detail to determine what information is required to achieve the organisation’s vision and mission. Every initiative in the strategic plan that potentially requires information to be achieved should be identified. Other factors to be identified include what the goals of the organisation are, what industry it operates in, whether the organisation owns intellectual property, and what the main resources owned by the organisation are.

7.12.3 Step Three: Assess Outsourcing Constraints and Enablers

The next step is to decide whether any constraining or enabling antecedents exist and are relevant to the organisation. Constraining and enabling antecedents for information security strategy originate internally or externally and are those conditions that may prevent or enable an organisation from outsourcing its information, people, processes or ICT infrastructure. There are quite a few conditions that may exist, and Table 7.2 illustrates some of the more common constraints.
Table 7.2. Common Constraining Antecedents for Outsourcing

<table>
<thead>
<tr>
<th>Constraining Antecedent</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory compliance</td>
<td>An organisation’s products or services may have national security implications as defined by federal regulations, increasing restrictions</td>
</tr>
<tr>
<td>Legal factors</td>
<td>Data sovereignty laws constraining information storage to on-shore facilities attempt to ensure a successful prosecution in the event of a security breach</td>
</tr>
<tr>
<td>Industry factors</td>
<td>Organisations competing in new and emerging industries may find it difficult to outsource operational aspects of their businesses. Organisations in the medical industry may hold patient information</td>
</tr>
<tr>
<td>Economic factors</td>
<td>Economic sanctions against nation states may preclude the storage of information there</td>
</tr>
<tr>
<td>Political factors</td>
<td>A political decision at Ministerial-level may preclude government departments or agencies from outsourcing their ICT infrastructure</td>
</tr>
<tr>
<td>External threat environment</td>
<td>Organisations operating in the military, banking or finance industries compete in high-threat environments, even if they are suppliers and sell benign products or services as raw materials</td>
</tr>
<tr>
<td>Valuable information</td>
<td>Intellectual property may form the basis of an organisation’s competitive advantage and be too valuable to risk storing externally</td>
</tr>
<tr>
<td>Ubiquitous information availability</td>
<td>Vendors providing 99.999% uptime for ICT infrastructure shared services are rare in the market and high-availability may be unachievable</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>An organisation’s directors may simply regard outsourcing as too risky</td>
</tr>
</tbody>
</table>

7.12.4 Step Four: Select Information Security Strategy

The organisation is now able to select a strategy:

i. If the organisation holds strategically valuable information and constraining antecedents exist, then choose **Fortification**.

ii. If the organisation does NOT hold strategically valuable information and constraining antecedents exist, then choose **Devaluation**.

iii. If the organisation holds strategically valuable information and no constraining antecedents exist, then choose **Outsourcing**.

iv. If the organisation does NOT hold strategically valuable information and no constraining antecedents exist, then choose **Minimisation**.
As part of the process, the selected strategy should be approved by the governing body, for example the board of directors or the minister of a government department, and then used to guide the development of a strategic plan involving a set of initiatives (ISO/IEC, 2013).

7.13 Theoretical Integration

Grounded theorists have an obligation to relate their developing theory with other previously-developed relevant theories (Urquhart et al., 2010). The wider benefits of this are twofold, as (1) this contributes to theoretical integration throughout the information systems discipline, and (2) this increased understanding could support the development of formal theories (Urquhart et al., 2010). Another benefit is that this process could serve to “reformulate previously established” theories (Glaser & Strauss, 1967, pp. 34). This section improves theoretical boundary clarity because “any contest between insights and existing theory becomes a comparative analysis that delimits the boundaries of the existing theory while generating a more general one” (Glaser & Strauss, 1967, pp. 255). Accordingly, this section relates the theory on information security strategy to selected existing theories identified as part of Chapter 2: Research Background. As a reminder, the complete list of relevant existing theories can be found in Appendix B: Theoretical Background List.

7.13.1 Information Category

The theory of information warfare from Denning (1999) argues that information resources, which are defined by the author as the ‘containers’ that hold information, can increase or decrease in value based on warfare activities conducted by either the organisation or its enemies. Given the persistent nature of advanced threat actors, information warfare has a lot to offer in guiding the defensive and offensive approaches to be taken by an organisation. As a suggestion towards reformulating previously established theory, the main incompatibility with OrgISS is the naming of
ICT infrastructure as a ‘resource’. In OrgISS, the resource is information, after it has been secured by the myriad of security controls implemented within an organisation against threats. Resources can then be reliably used by the organisation towards the pursuit of its goals and exploited the same as any other asset owned by the organisation, as per resource-based theory. ICT infrastructure should be viewed as a platform that information resides upon and should be named as such.

7.13.2 Organisational Context Category

Dynamic capabilities theory as described by Teece, Pisano, and Shuen (1997) describes the linkage between changes in external environmental conditions causing an organisation to reconfigure internal capabilities based on resources. This theory is similar in some respects with organisational information processing theory by Galbraith (1974). These theories have implications for OrgISS whereby the nature of OrgISS cannot be static and must be process-oriented to allow changes in environmental conditions, for example national laws on data storage, to affect generic information security strategy selection. OrgISS has been changed to explicitly state that although the strategy is instantiated in written form, and its implementation is documented in a strategic plan, its state is a process aligned with business strategy renewal as a result of this insight from dynamic capabilities theory.

General systems theory originally described by Von Bertalanffy (1969) holds that business functions or departments in an organisation can be viewed as complete systems in their own right, and when they interact with each other, or with external organisations, they share information and can evolve and change their properties as a result. The interconnection of the individual systems links them into an entire ecosystem. This has implications for OrgISS when assessing outsource partners. Should an outsourced ICT infrastructure vendor for example use the physical premises of a data centre provider, then not only does the organisation have to
assess the security maturity of the outsource partner but any suppliers that it uses as well to check for vulnerabilities. OrgISS theory has already identified the requirement to assess outsource partners and their suppliers.

Stakeholder theory by Donaldson and Preston (1995) argues that stakeholders participate in organisational activities primarily for their own self-interest and the priorities of these interests are not immediately obvious. This has implications for the assessment of outsource vendors and the maturity assessment of their security controls. An organisation will want to ensure parity of security controls, where an outsource vendor’s controls are at least, if not better than, the security controls in use by the organisation. However, security controls cost money and the outsource vendor is pursuing a business goal of profit. It is conceivable that an outsource vendor may covertly reduce security controls to reduce expenses and increase profit, and the organisation must guard against this with a thorough assessment.

7.13.3 Information Approach Category

Contingency theory as originally espoused by Fiedler (1964) contends that there are a number of approaches to leadership within an organisation and that the different approaches are dependent on internal and external constraints. This linkage between internal and external conditions affecting the selection of the most appropriate option from a small set of options is consistent with the model design adopted by OrgISS. As a difference however, OrgISS goes further to explain in detail what the benefits are to an organisation from the optimal option selection. Contingency theory has been criticised for a lack of explanatory power however OrgISS has been careful to be grounded in the data to increase its trustworthiness and power of explanation.

Two of the generic information security strategies, Devaluation and Minimisation, guide an organisation that does not own valuable information that specifically supports the achievement of organisational goals. In the case of Devaluation, the
organisation requires on-demand access to valuable information held by other organisations, for it to achieve its goals. An example would be organisations accessing customer credit card details held by PayPal to transact a sale. The motivation to develop a dependence on information not owned by the organisation can be explained using resource dependency theory by Pfeffer and Salancik (1978). In this theory, actors lacking essential resources will seek them from others by developing relationships with them.

### 7.13.4 Strategic Impacts on Organisation

As identified in Chapter 6: Findings, one of the strategic impacts on an organisation that arises from an appropriate selection of an information security strategy is protection of competitive advantage. A relevant theory that explains this is the resource-based view of the firm theory by Penrose (1959), which argues that organisations own a number of resources that create sustainable competitive advantage if they possess four characteristics, being valuable, rare, inimitable, and non-substitutable. This theory explains why selecting a generic information security strategy for the protection of trade secrets, to be used as a resource, leads to competitive advantage.

Another strategic impact on an organisation should it select an appropriate information security strategy is regulatory compliance, as described in Chapter 6: Findings. Some regulatory bodies, for example the Payment Card Industry Security Standards Council, enforce an uplift in security controls within organisations that hold valuable information such as credit card data. Compliance as an outcome, from adopting technological security controls in response to demands from regulators, can be explained by technology-organisation-environment theoretical framework by DePietro, Wiarda, and Fleischer (1990). These authors argue that technologies relevant to the organisation, characteristics of the organisation such as its size, and
the environmental context such as its industry, affect the process by which an organisation adopts technology.

### 7.14 Chapter Summary

This chapter combined concepts discovered during a review of the literature with findings from data collection and analysis, to propose a set of four generic strategies for securing information. This theory on information security strategy advances understanding of how to secure information from a strategic perspective. The theory gives decision-makers guidance and options for the organisation-wide protection of information, which has been a gap in research to date.
In this chapter\(^4\), I summarise the research program and draw several conclusions based on the discussion chapter. I revisit the research question and sub-questions posited in chapter one and answer them. I list and describe the key findings from the research, and separately list the contributions to knowledge. No research program is perfect, so I identify key limitations and offer suggestions for future research directions. The thesis is closed with a list of references and several appendices which contain data relevant to the study but due to their voluminous nature, would detract from the narrative if they were included in the body of the thesis.

### 8.1 Chapter Aim

The aim of this chapter is to draw strong conclusions from the arguments in the discussion chapter and to respond to the aim of the research as described in the introductory first chapter. To recap, the aim as described in Chapter 1 Introduction was to increase understanding of information security strategy in organisations.

### 8.2 Summary of Work

This thesis offers a theoretical model of information security strategy and advances understanding of how to secure information at a strategic level. I found that leaders of information security should assess their organisational information value and their key factors in their environment before making decisions about selecting one strategy.

\(^4\) Elements of this chapter are published in the following peer-reviewed article:

to secure all information. There are four main approaches commonly taken to increase the security of information. These are (1) to increase protection of valuable information through fortification, (2) to devalue sensitive information so that basic protections are sufficient, (3) to seek external assistance with the protection of valuable information through outsourcing, and (4) to provide a minimal level of security for non-sensitive information. Regardless of the approach taken, the common goal is to increase the security of information, which by extension increases the security of the organisation.

8.3 Conclusions from Discussion

All information systems-based research should develop an understanding of a phenomenon in a section describing the implications of the research (Zmud, 1998). The reason for this is to improve the academic community’s shared knowledge of the phenomenon and to act as the base for any future research (Zmud, 1998). Therefore, this section does not seek to summarise conclusions as the previous section has already achieved this, but rather identify the significance of each of the conclusions.

The following describes the implications of my research model in both theoretical and practical terms. The theory-based implications include aspects of the developed theoretical model that might be most appropriate for future empirical testing, and also some suggestions for what aspects of the model could be developed more with additional theorising (Zmud, 1998). The practice-based implications include prescriptive statements and contextual situations where the application of the model would be most relevant (Zmud, 1998).

8.3.1 Significance for Theory and Research

Theoretical significance includes the finding to reduce the value of information to increase organisational security, which is novel, almost counter-intuitive. As well, the
findings to engage in outsourcing, not to gain access to skillsets or reduce cost, but to increase security is also original in extant literature. Significantly, it is novel to offer strategic-level decision-makers options to protect organisational information as decisions about security have typically been left to executives and management.

8.3.2 Significance for Practice

Practical significance includes giving organisational decision-makers guidance for the strategic-level protection of information including direction for the selection of technological infrastructure, and cyber insurance, which has been a gap in guidance to date. The executive staff can identify appropriate strategic initiatives to implement the approved strategy, request adequate budget, and share responsibility with management for implementation.

The selection of an information security strategy then sets the direction for the organisation’s IT Strategy and the associated operational-level decisions about procurement of people, processes and ICT infrastructure. These strategies are:

i. Fortification: The information that was discovered as part of the analysis of information for strategic purpose exercise should be identified and that information earmarked for protection. The rest of the information that was discovered as part of the information discovery, profiling and classification exercise should be protected as well.

ii. Devaluation: Valuable information held within the organisation should be deleted or tokenised and linked to information held by another organisation. Organisations should partner with other organisations to hold the information, for example linking to PayPal to process credit cards rather than hold card details internally.

iii. Outsourcing: Strategic information can be stored on external cloud-based or shared-segmented servers however the organisation must ensure that
governance of adequate security controls is available. These security control services from the outsourcing vendor must be both preventative, for example information at rest in the cloud should be encrypted, or responsive, for example distributed denial-of-service mitigation tools should be automated and scalable. Public cloud has several benefits such as scalability, collaboration, flexibility, low cost, modern architectures and change management. Large vendors such as Microsoft, Amazon and Google also invest millions of dollars into security for their respective platforms. Procuring cloud takes advantage of these large security budgets and avoids the cost of direct internal investment in security.

iv. Minimisation: Organisations can find a way to not hold valuable information yet still achieve their vision and mission. This approach can significantly reduce the infrastructure and investment required to achieve organisational goals.

8.4 Research Question Answered

The research question from Chapter 1 guiding the conduct of this research body of work is:

*RQ: How can organisational leaders select an information security strategy that best benefits the organisation?*

This research question was broken down into the following sub-questions and an answer for each is as follows:

1. **What is an information security strategy?**

Information security strategy is an organisational-level model of conceptual elements, which is motivated by antecedent conditions that balance internal information needs
and external environmental factors, to yield information security benefits to the organisation.

II. How is an information security strategy selected by organisational leaders?

An organisation should select a single strategy for the entire organisation by following these rules:

i. If the organisation holds strategically valuable information and constraining antecedents exist, then choose Fortification.

ii. If the organisation does NOT hold strategically valuable information and constraining antecedents exist, then choose Devaluation.

iii. If the organisation holds strategically valuable information and no constraining antecedents exist, then choose Outsourcing.

iv. If the organisation does NOT hold strategically valuable information and no constraining antecedents exist, then choose Minimisation.

III. How can an information security strategy best benefit an organisation?

The selected strategy should be endorsed by the governing body, for example the board of directors or the minister of a government department, and then used to guide the development of a strategic plan involving a set of initiatives.

8.5 Key Findings from the Research

This research made several findings including identifying the antecedents that prompt or motivate the adoption of an information security strategy, the constituent components of an information security strategy, a range of benefits that can be enjoyed post-adoption, relationships between antecedent conditions and information security strategies, and an improved understanding of information security. These findings are described in the following sections.
8.5.1 Finding 1: A Set of Antecedent Concepts that Motivate the Adoption of an Information Security Strategy

The antecedent conditions were largely grouped into two main areas, with the first group including concepts that related to a core category, information. The four main concepts that emerged from the data were accessing the functionality provided by information, controlling information, information as an asset, and information value. A few other properties of information were also identified which were information classification, information location, and information ownership.

The second group related to the organisation. There are three discrete categories of concepts that relate to the information storage properties of an organisation. They are broadly labelled organisational conditions, outsourcing constraints, and outsourcing enablers. These three categories each contain a set of concepts with their properties and dimensions. Organisational conditions are those factors that describe the strategic and operational level aspects of an organisation that relate to information security. They include the organisation’s vision and mission, goals, governance structures, information resources, capabilities and performance. Outsourcing constraints are the conditions originating either externally or internally that affect an organisation’s ability to engage in outsourcing. Their existence may have an enormous effect on decisions made both in the director’s boardroom and operationally by management and staff. Outsourcing enablers also have an enormous effect, as often outsourcing decision cannot be made without them.

8.5.2 Finding 2: A Set of Constituent Concepts That Together Form the Body of an Information Security Strategy

During the literature review, a set of concepts were identified that form the constituent components of an information security strategy. These constituent components can be grouped according to the level of an organisation that they relate
to. The highest level, inter-organisational, included regulatory compliance, information warfare, information asset protection, and environment scanning. At the organisational level, components included boardroom accountability, quality improvement, information asset management, labour source, risk management, organisational agility, governance, business continuity, people and process, incident prevention, and policy. At the group level, components included knowledge leakage prevention, security budget, responsibility, controls, incident response, and ICT infrastructure.

8.5.3 Finding 3: A Set of Concepts That Are Benefits Yielded from The Adoption of an Information Security Strategy

The benefits include avoidance of bankruptcy, maintaining the confidentiality, integrity and availability of information, maintaining customer trust, protecting an individual's reputation, avoidance of loss of life, operational productivity, organisational security, a range of outsourcing benefits, performance reporting, probable loss mitigation, protection of trade secrets, public reputation, reduction in expenses, regulatory compliance, reducing risk of litigation, and reducing share price fluctuations.

8.5.4 Finding 4: Causal Relationships Between Antecedent Conditions and Approaches to Securing Information

Several key relationships were identified where an antecedent construct affected organisational approach to securing information. For example, high value information causes an organisation to increase the volume and type of security controls. Also, an organisation can maintain partial control over high value information yet increase its security. As well, information can form the basis of a core competency which negatively affects whether it can be stored externally.
Organisational concepts such goals and strategy affect how the organisation decides to store, use and secure its information. As well, constraints such as the existence of political factors or regulatory compliance requirements affects how the organisation decides to store, use and secure its information. Enablers such as budget or organisational size can also affect how the organisation decides to store, use and secure its information.

8.5.5 Finding 5: Causal Relationships Between Approaches to Securing Information and Strategic Impacts on an Organisation

Fortification techniques, including improving the security controls used to protect information, have been shown to positively affect the security of an organisation. As well, devaluation techniques, such as avoiding holding information in the first place, tokenisation of information, and deletion of unnecessary information, positively affects the security of an organisation. Outsourcing, to take advantage of the scale and scope of an outsourcing partner’s specialism and security controls, positively affects the security of an organisation. Also, minimisation techniques to avoid ownership of information and to reduce the value of any information held and positively affect the security of an organisation.

8.6 Contributions to Knowledge

This thesis makes several contributions to towards the body of knowledge on why organisations should adopt an information security strategy and how organisational leaders should take steps to evaluate and select a strategy in practice. Specifically, the contributions to knowledge are:
8.6.1 Contribution 1: A Definition of Information Security Strategy in Organisations

Based on the literature review, I construct a definition proposing the meaning of information security strategy:

"Information security strategy guides the achievement of organisational goals and objectives using IT infrastructure and information resources to achieve them, is motivated by antecedent conditions that balance internal information needs and external environmental factors to yield information security benefits to the organisation, and is selected from a small set of generic strategies to guide decision-making when implementing operationally."


The literature review from this research involved thematic analysis which identified a set of core concepts organised by level and relationship. The levels included individual, group, organisation and inter-organisation. The relationships included antecedents, constituents, and yields. The examination of extant literature in information systems identified several concepts and these were expanded quite significantly after data collection and analysis.

8.6.3 Contribution 3: A Conceptual Model of Information Security Strategy

The conceptual model of information security strategy depicts all abstract concepts and their relationships, generalised from the data. The relationships are proposed ones only without explanations. This model was then used as a representation of reality from which to base the development of a theory on information security strategy.
8.6.4 Contribution 4: A Theory on Information Security Strategy

The theory on information security strategy states that there are four generic strategies that guide the security of information within organisations. The depiction shows how core categories, their relationships, including properties of information, along with organisational and environmental conditions, affect selection of the most appropriate approach to securing information, which in turn offers a wide array of strategic-level organisational benefits.

8.6.5 Contribution 5: A Set of Practical Steps to Select an Information Security Strategy

This research provides guidance for practitioners in identifying all structured and unstructured information owned by the organisation, evaluating environmental challenges with securing that information, and selecting a strategy to secure it. The governing body then approves the most appropriate strategy, which can then be used to guide executives and management when making operational decisions to secure information.

8.7 Limitations

No study is without limitations, so this section identifies a range of limitations to the data in this research. All research studies are bound by time and resources and this doctoral thesis is no different. The following are some limitations that apply to the study.

8.7.1 Limitations of Review into Information Security Strategy

The OrgISS construct developed so far is potentially of great benefit to organisations seeking to adopt an overall strategy for their information security. It demonstrates (1) the precursor conditions which when met, cause organisations to consider the use of OrgISS; (2) the constituent elements of an OrgISS for operationalisation; and (3) the
benefits that can be enjoyed by an organisation upon successful implementation. Given that, there are still have limitations impeding an understanding of OrgISS.

First, a significant amount of research conceptualises OrgISS as a plan, which identifies the construct as a static document, bereft of dynamic processes to ensure its validity when responding to immediate changes in the external environment. This gives rise to possible construct validity issues as having a plan is important, but not a precondition for an organisation to vary its OrgISS based on persistent incident detection and response (Straub, Boudreau, & Gefen, 2004).

Second, the information systems literature contains analysis on OrgISS from various levels within an organisation, largely focusing on the organisational perspective. This stratified perspective has its own properties and varies from an inter-organisational level, for example in terms of complexity and focus on external factors. Therefore, the nomological network of terms will be different for each level.

Third, measurement issues arose in this study when I found that information systems researchers either did not adequately explain the dimensions with which to measure the elements of the OrgISS construct at each level or defined theoretical measures for one level and then operationalised them at another (Baskerville & Dhillon, 2008). Additionally, tangible aspects of OrgISS such as the use of technical controls were perceived to be very measurable through reporting but intangible aspects such as employee attitudes towards security less so.

8.7.2 Limitations of Research into Information Security Strategy

Although this study collected data from 25 research participants from 25 different organisations, the sample is Australian and so precludes generalising directly to other organisations worldwide. However, this study identifies and discusses concepts and propositions that improve understanding of OrgISS concepts, and this
understanding is applicable to a wide variety of other organisations seeking strategic direction to secure their information (Yin, 2011).

This study utilised deeply subjective questions, and the answers that were given in response by the participants were also subjective. Although the student researcher went to some lengths to remain open to findings and bracket biases away from the study, it is probable that some persist, which is not a bad thing (Corbin & Strauss, 2008).

The research questions and resultant answers often used imprecise measures for the constructs depicted in the conceptual model. This could not be avoided for the purposes of developing the phenomenon of information security strategy based on limited data, and it is hoped that future research might improve measurement.

The conceptual model remains untested empirically. The relationships identified in the model are propositions not hypotheses because formal testing was never within the scope of this study. This research program focuses on increasing an emerging understanding of the phenomenon of information security strategy.

### 8.8 Future Research Directions

This thesis develops an extensive set of concepts related to information security strategy but is far from an exhaustive explanation of how OrgISS is applicable to all organisations. There are a few interesting directions that future research could take to build on the findings and contributions from this thesis. The following is a list of suggested directions to move towards a better understanding of OrgISS.

Moving away from strategy to look more broadly at the field, this thesis advances understanding of information security properties and their dimensions, including assets, controls and threats. Could this be investigated further with a view to developing a theory on information security?
Given the strong links from OrgISS to organisational strategic theory apparent in the literature, what are the links between business strategy, IT strategy, and OrgISS? How can OrgISS be integrated more fully with business strategy or the IT strategy? Is there a dependence on OrgISS to achieve organisational success, and if so, how is this success defined or measured? Are there avenues to generate additional competitive advantage through OrgISS?

How would OrgISS be operationalised within an organisation, using a strategic plan? To what extent would compliance culture influence the effectiveness of OrgISS operationalisation (Shedden, Ruighaver, & Ahmad, 2010; Tan, Ruighaver, & Ahmad, 2010)? How does OrgISS relate to strategic information systems? What is the role of the individual level in OrgISS? How do levels of analysis apply in the digital realm? Could the impacts on organisational outcomes from the setting of an information security strategy be empirically tested and measured? Could some concept relationships be bi-directional instead of uni-directional? What initiatives would form part of a strategic plan to implement the strategy?

There are a number of information systems scholars who have researched theories related to OrgISS, including for example deterrence, prevention, surveillance, detection, response, deception, perimeter defence, compartmentalisation and layering (Ahmad et al., 2014b; Beebe & Rao, 2009; D'Arcy & Herath, 2011). What would further analysis of other theories reveal about OrgISS? Could another researcher develop a similar data set, follow the same grounded theory procedures, and develop the same theory to enhance confirmability? Could the substantive theory on OrgISS articulated in this thesis be abstracted up another level to a formal theory, broader than information security and adaptable into other disciplines (Glaser & Strauss, 1967)?
How might organisations move from one information security strategy to another? Could organisations move from *Devaluation* to *Minimisation* to further lower the costs involved in protecting non-valuable information from threats and reduce expenses by providing minimum viable security via public cloud, to preserve security budget for higher priority security initiatives? In this case, there may be a loss of control involved, which may increase risks to the organisation’s information, so resiliency should be instituted with a robust business continuity plan (Dhillon, 2018).

Could organisations move from *Fortification* to *Outsourcing* depending on their security budget? Organisations looking for cost savings when protecting valuable information could look to identify irreplaceable trade secrets and protect them in-house but outsource all other valuable information and thus leverage the multi-million-dollar security budgets that large public cloud providers spend on securing their infrastructure. *Outsourcing* could then achieve the effects of *Fortification* but with reduced expenses, increased scalability and resilience, albeit with increased risk through reduced control.

Could organisations move from *Fortification* to *Devaluation* to reduce the cost of securing information by reducing the value of information held? Where valuable information exists, and ICT infrastructure and human resources are insourced as per the *Fortification* strategy, security controls and hence costs are increased which results in the valuable information held by the organisation being more secure. By moving to the *Devaluation* strategy, information value and classification would be reduced thus reducing risks, controls and costs. To reduce expenses, *Devaluation* would be the preferred option over *Fortification*, but its selection depends on information value being obviated.

Could organisations move from *Outsourcing* to *Minimisation*, assuming no outsourcing constraints exist? If information has value, then it should be outsourced
to the protection of external suppliers of services, such as cyber insurance agencies, cloud infrastructure, managed services, and security consultants. However, if information can be changed to have minimal inherent value, then it could be externally stored but secured using the cheapest, enterprise-grade quality, security controls available.

8.9 Postscript

Although formal testing of this theory on information security strategy is not within the scope of this thesis, some evaluation of this qualitative research has been performed to improve trustworthiness of the scheme. Upon completion of this research, the student researcher was contracted to provide consulting services to conduct an independent security review of a business client, which was a very large not-for-profit organisation headquartered in Australia. The scope of this review was to assess eight areas of the client’s technical security controls, evaluate the information security skills, qualifications and experience of the IT team, and write an evaluation to inform the recommendation of an information security strategy to the board of directors.

Adhering to the process for recommending a strategy (as set in Prescriptive Statements in Chapter 7: Discussion) led to the development of a list of 34 discovery-oriented questions to ask the client, a successful consulting outcome for all deliverables in a short period, and the work also resulting in some changes being made to the thesis. Specifically Table 2.3, which offers a thematic map of the concepts identified during the conduct of the literature review, was changed to delineate the antecedent concepts more clearly and distinctly, the prescriptive statements listed in Chapter 7: Discussion were changed to group related concepts such as legal, regulatory and standards together to improve efficiency, and future directions of this research were expanded to include identification of the initiatives that would form part of a strategic plan to implement the chosen strategy. Feedback
from the client was they thought they had been listened to and that the recommendation of an information security strategy was appropriate. The information security strategy was approved by their board of directors at a board meeting three months later and is currently being used to guide implementation of their information security strategic plan.
References


REFERENCES


REFERENCES


REFERENCES


Appendix A: Core Papers Analysed for Literature Review


Appendix B: Theoretical Background List

The following is a list of 34 theories in information systems, which relate to information security strategy based on the keywords asset, resource, threat, control, information, security, or strategy, that were found during a search and review of 104 extant information systems theories listed on a web-based resource maintained by Larsen and Eargle (2018).

Table B.1. Information Systems Theories and Information Security Strategy

<table>
<thead>
<tr>
<th>#</th>
<th>Theory</th>
<th>Search Term/s</th>
<th>Summary</th>
<th>Reference</th>
<th>Relevance to OrgISS</th>
<th>Limitations to OrgISS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Adaptive structuration</td>
<td>Resource</td>
<td>Adaptive Structuration Theory studies the interaction of groups and organisations with information technology. Groups and organisations using information technology for their work to dynamically create perceptions about the role and utility of the technology, which influences how technology is used, and hence mediates its impact on group outcomes.</td>
<td>DeSanctis, G., &amp; Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. Organization Science, 5(2), 121-147.</td>
<td>Interaction between groups and organisations via information technology includes some aspect of security.</td>
<td>Originates at the group level not organisation level. Does not assess interaction with threat actors external to the organisation.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2.</td>
<td>Boundary object theory</td>
<td>Information</td>
<td>A boundary object is a firm-level concept in sociology to describe information used in different ways by different communities. They are plastic, interpreted differently across communities but with enough immutable content to maintain integrity.</td>
<td>Star SL &amp; Griesemer JR (1989). &quot;Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley’s Museum of Vertebrate Zoology, 1907-39&quot;. Social Studies of Science 19(4): 387–420.</td>
<td>An OrgISS being different depending on the organisation using it fits, as does it being organisation-level.</td>
<td>The focus on describing information but not security controls does not fit with OrgISS.</td>
</tr>
<tr>
<td>5.</td>
<td>Five competitive forces strategy (Porter)</td>
<td>Threat, strategy</td>
<td>Five forces theory combines the bargaining power of customers, the bargaining power of suppliers, the threat of new entrants, and the threat of substitute products, with the level of competition in an industry.</td>
<td>Porter, M. E. (1980). Competitive strategy: Techniques for analyzing industries and competitors. NY, USA: The Free Press.</td>
<td>Examination of internal and external contextual conditions, and the inter-dependence on suppliers and customers.</td>
<td>The focus on potential and existing competition, and substitute products and services.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Complexity theory</td>
<td>Resource</td>
<td>Complexity theory is part of the theory of computation dealing with the resources required during computation to solve a given problem, the most common being time (how many steps it takes to solve a problem) and space (how much memory it takes).</td>
<td>Cook, Stephen A. May 1971. The complexity of theorem proving procedures. Proceedings Third Annual ACM Symposium on Theory of Computing: 151-158.</td>
<td>Utilisation of resources to achieve goals.</td>
<td>No link to strategy or approaches to securing the resource.</td>
</tr>
<tr>
<td>7</td>
<td>Contingency theory</td>
<td>Strategy</td>
<td>Contingency theory contends that there is no one best way of organising / leading and that an organisational / leadership style that is effective in some situations may not be successful in others. The optimal organisation / leadership style is contingent upon various internal and external constraints. There are also contingency theories that relate to decision making (Vroom and Yetton, 1973).</td>
<td>Fiedler, F. E. (1964). A Contingency Model of Leadership Effectiveness. Advances in Experimental Social Psychology (Vol.1). 149-190. New York: Academic Press.</td>
<td>Strategic approach to securing information needs to consider environmental conditions as well as internal management decisions.</td>
<td>Lack of explanatory power.</td>
</tr>
<tr>
<td>8</td>
<td>Dynamic capabilities theory</td>
<td>Resource</td>
<td>Dynamic capabilities are ‘the ability to integrate, build, and reconfigure internal and external competencies to address rapidly-changing environments, and are based on the resource-based view of the firm.</td>
<td>Teece, D. J., G. Pisano, and A. Shuen (1997) &quot;Dynamic capabilities and strategic management,&quot; Strategic Management Journal (18) 7, pp. 509-533.</td>
<td>Development of resources which are used to achieve goals. Links to org environment. Sustains competitive advantage.</td>
<td>Lacks a security perspective and focus on information as a resource.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>Game theory</td>
<td>Strategy</td>
<td>Game theory is a branch of applied mathematics that uses models to study interactions with formalised incentive structures (&quot;games&quot;). Unlike decision theory, which also studies formalised incentive structures, game theory encompasses decisions that are made in an environment where various players interact strategically.</td>
<td>John von Neumann and Oskar Morgenstern. (1944). Theory of games and economic behavior. Princeton: Princeton University Press.</td>
<td>Decision-making for strategic benefit.</td>
<td>Lacks a focus on security and the utilisation of information.</td>
</tr>
<tr>
<td>11</td>
<td>General systems theory</td>
<td>Control</td>
<td>Systems are open to, and interact with, their environments, and that they can acquire qualitatively new properties through emergence, resulting in continual evolution. Systems theory focuses on the arrangement of and relations between the parts which connect them into a whole.</td>
<td>Bertalanffy, L. von. (1934). Investigations on the Lawfulness of Growth. I. General principles of theory; mathematical and physiological laws of growth in aquatic animals. Arch. Development Mech., 131: 613-652.</td>
<td>Focus on interaction with other stakeholders such as customers or suppliers.</td>
<td>Does not use information as part of the interaction or secure the passage of information.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.</td>
<td>General deterrence theory</td>
<td>Threat</td>
<td>General Deterrence Theory (GDT) &quot;posits that individuals can be dissuaded from committing antisocial acts through the use of countermeasures, which include strong disincentives and sanctions relative to the act&quot;.</td>
<td>Straub, D. W., &amp; Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. Management Information Systems Quarterly, 22(4), 441.</td>
<td>Increasing security through the communication to a potential attacker of a disincentive being a lack of valuable information, meaning the reward for an attack will be low.</td>
<td>Does not focus on protection of information.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>15.</td>
<td>Information processing theory</td>
<td>Information, strategy</td>
<td>The idea (1) that short-term memory can only hold 5-9 chunks of information, and that (2) the human mind takes in information, performs operations on it to change its form and content, stores and locates it and generates responses to it.</td>
<td>Miller, G.A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63, 81-97.</td>
<td>Focus on information and its storage and location.</td>
<td>Disregards organisational context, strategic application and security of the information.</td>
</tr>
<tr>
<td>16.</td>
<td>Information warfare theory</td>
<td>Information, resource</td>
<td>The theory of information warfare is centred on the value of information resources that hold information and on “win-lose” operations that affect that value. Offensive and defensive information warfare is expressed in terms of actors, targets, methods, technologies, outcomes, policies, and laws. Information warfare can target or exploit any type of information resources.</td>
<td>Denning, D. E. R. (1999). Information warfare and security (8th ed.). MA, USA: ACM Press Books.</td>
<td>Containers that house information include people, paper, servers and databases. Defensive and offensive postures considered.</td>
<td>Primary focus is on protecting resources (containers) that house information, not the information itself.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>20.</td>
<td>Media richness theory</td>
<td>Information</td>
<td>Media richness theory is a hierarchy which incorporates four media classifications; face-to-face, telephone, addressed documents, and unaddressed documents. The richness of each media is based on four criteria; feedback, multiple cues, language variety, and personal focus.</td>
<td>Daft, R. L., and Lengel, R. H. “Information Richness: A New Approach to Managerial Behavior and Organizational Design,” in Research in Organizational Behavior, L. L. Cummings and B. M. Staw (eds.), JAI Press, Homewood, IL, 1984, pp. 191-233.</td>
<td>Classification of information based on perceived value.</td>
<td>Focus on security or strategic application.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>21.</td>
<td>Media synchronicity theory</td>
<td>Information</td>
<td>Media synchronicity theory is a predictor of communication performance, where communication will be enhanced when the synchronicity a given medium can support appropriately matches the synchronicity that a communication process requires.</td>
<td>Dennis, Alan R., Fuller, Robert M., Valacich, Joseph S. 2008. &quot;Media, Tasks, And Communication Processes: A Theory of Media Synchronicity.&quot; MIS Quarterly (32:3), pp. 575-600.</td>
<td>Focus on information and the platform it resides on.</td>
<td>Relates to group-level rather than organisation-level.</td>
</tr>
<tr>
<td>22.</td>
<td>Organizational information processing theory</td>
<td>Information</td>
<td>This theory identifies three important concepts: information processing needs, information processing capability, and the fit between the two to obtain optimal performance.</td>
<td>Galbraith, J. R. (1974). Organization design: An information processing view. Interfaces, 4(3), 28-36.</td>
<td>Focus on environmental conditions that affect at organisation-level and valuable information to support strategic decision-making.</td>
<td>Focus on security of information absent.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>Resource-based view of the firm theory</td>
<td>Resource, strategy</td>
<td>The resource-based view (RBV) argues that firms possess resources, a subset of which enable them to achieve competitive advantage, and a subset of those that lead to superior long-term performance. Resources that are valuable and rare can lead to the creation of competitive advantage, which can be sustained over longer time periods when the firm is able to protect against resource imitation, transfer, or substitution.</td>
<td>Penrose, E. T. (1959). The Theory of the Growth of the Firm. Wiley, New York.</td>
<td>Information as a resource supporting the achievement of organisational goals.</td>
<td>Lacking focus on security of information to maintain its utility as a resource.</td>
</tr>
<tr>
<td>27</td>
<td>Resource dependency theory</td>
<td>Resource</td>
<td>RDT proposes that actors lacking in essential resources will seek to establish relationships with (i.e., be dependent upon) others to obtain needed resources. Also, organisations attempt to alter their dependence relationships by minimising their own dependence or by increasing the dependence of other organizations on them.</td>
<td>Pfeffer, J., &amp; Salancik, G. 1978. The external control of organizations: A resource dependence perspective, New York, Harper &amp; Row.</td>
<td>Information as a resource supporting the achievement of organisational goals.</td>
<td>Lacks focus on security controls to protect the resources and on threats.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>28.</td>
<td>Selective organizational information privacy and security violations model (SOIPSVM) theory</td>
<td>Information, security</td>
<td>The selective organisational information privacy and security violations model (SOIPSVM), explains how organisational structures and processes, along with characteristics of regulatory rules, alter perceptions of risk when an organisation's performance does not match its aspiration levels and, thereby, affects the likelihood of rule violations.</td>
<td>Jeffrey D. Wall, Paul Benjamin Lowry, and Jordan Barlow (2016). “Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess,” Journal of the Association for Information Systems (JAIS), vol. 17(1), pp. 39-76</td>
<td>Organisational environment contextual conditions including regulatory compliance affecting approaches to securing information.</td>
<td>Lacks focus on threats and valuable information.</td>
</tr>
<tr>
<td>29.</td>
<td>Stakeholder theory</td>
<td>Strategy</td>
<td>Stakeholder theory argues that every legitimate person or group participating in the activities of a firm do so to obtain benefits and that the priority of the interests of all legitimate stakeholders is not self-evident.</td>
<td>Donaldson, T. &amp; Preston, L. 1995. The stakeholder theory of the modern corporation: Concepts, evidence and implications. Academy of Management Review 20, 65-91</td>
<td>Information flow between stakeholder groups including customers and supplier, regulators and staff.</td>
<td>Lacks focus on threats and security.</td>
</tr>
</tbody>
</table>
### APPENDIX B: THEORETICAL BACKGROUND LIST

<table>
<thead>
<tr>
<th>#</th>
<th>Theory</th>
<th>Search Term/s</th>
<th>Summary</th>
<th>Reference</th>
<th>Relevance to OrgISS</th>
<th>Limitations to OrgISS</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>Theory of slack resources</td>
<td>Strategy, resource</td>
<td>The theory of slack resources is a multilevel theory that suggests, understanding the value of IT at any level of interest requires understanding the way IT slack is created and then redeployed to IT and/or business processes beside the operationalized IT investment.</td>
<td>Rahrovani, Y., &amp; Pinsonneault, A. (2012). On the business value of information technology: A theory of slack resources. In Information Systems Theory (pp. 165-198). Springer New York.</td>
<td>Budgets for security controls managed in response to demand, which could potentially be derived from threats.</td>
<td>Lacks focus on valuable information.</td>
</tr>
<tr>
<td>33.</td>
<td>Transaction cost economics theory</td>
<td>Asset</td>
<td>In economics and related disciplines, a transaction cost is a cost incurred in making an economic exchange.</td>
<td>Kumar, Kuldeep, Van Dissel, Han G., Bielli, Paola, &quot;The Merchant of Prato--Revisited: Toward a Third Rationality of Information Systems&quot;, MIS Quarterly, 1998, Vol. 22, Issue 2.</td>
<td>Focus on reducing costs when transferring information to stakeholder groups such as customers and suppliers.</td>
<td>Lacks focus on threats and security controls.</td>
</tr>
<tr>
<td>#</td>
<td>Theory</td>
<td>Search Term/s</td>
<td>Summary</td>
<td>Reference</td>
<td>Relevance to OrgISS</td>
<td>Limitations to OrgISS</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>34</td>
<td>Work systems theory</td>
<td>Information, strategy</td>
<td>The basic idea of WST is that systems in organisations should be viewed as work systems by default. Technologies should be viewed as components of work systems rather than as systems on their own unless there is an intention to analyse a totally automated work system.</td>
<td>Alter, S. (1999) “A General, Yet Useful Theory of Information Systems,” Communications of the Association for Information Systems, 1(13).</td>
<td>Focus on processing information, which occurs through six types of activities, capturing, transmitting, storing, retrieving, manipulating, and displaying information.</td>
<td>Lack of focus on threats or security controls.</td>
</tr>
</tbody>
</table>
Appendix C: Ethics Approval

23 August 2016

Dr S.B. Maynard
Computing and Information Systems
The University of Melbourne

Dear Dr Maynard

I am pleased to advise that the Engineering Human Ethics Advisory Group has approved the following Minimal Risk Project.

Project title: Information Security Strategy in Organisations
Researchers: Dr A Ahmad, M Onibere, Dr S B Maynard, C Horne
Ethics ID: 1647424

The Project has been approved for the period: 23-Aug-2016 to 31-Dec-2016.

It is your responsibility to ensure that all people associated with the Project are made aware of what has actually been approved.

Research projects are normally approved to 31 December of the year of approval. Projects may be renewed yearly for up to a total of five years upon receipt of a satisfactory annual report. If a project is to continue beyond five years a new application will normally need to be submitted.

Please note that the following conditions apply to your approval. Failure to abide by these conditions may result in suspension or discontinuation of approval and/or disciplinary action.

(a) Limit of Approval: Approval is limited strictly to the research as submitted in your Project application.

(b) Amendments to Project: Any subsequent variations or modifications you might wish to make to the Project must be notified formally to the Human Ethics Advisory Group for further consideration and approval before the revised Project can commence. If the Human Ethics Advisory Group considers that the proposed amendments are significant, you may be required to submit a new application for approval of the revised Project.

(c) Incidents or adverse affects: Researchers must report immediately to the Advisory Group and the relevant Sub-Committee anything which might affect the ethical acceptance of the protocol including adverse effects on participants or unforeseen events that might affect continued ethical acceptability of the Project. Failure to do so may result in suspension or cancellation of approval.

(d) Monitoring: All projects are subject to monitoring at any time by the Human Research Ethics Committee.

(e) Annual Report: Please be aware that the Human Research Ethics Committee requires that researchers submit an annual report on each of their projects at the end of the year, or at the conclusion of a project if it continues for less than this time. Failure to submit an annual report will mean that ethics approval will lapse.

(f) Auditing: All projects may be subject to audit by members of the Sub-Committee.

Please quote the ethics registration number and the name of the Project in any future correspondence.

On behalf of the Ethics Committee I wish you well in your research.

Yours sincerely

[Signature]

Dr Rachelle Bosua – Acting Chair
Engineering Human Ethics Advisory Group

Melbourne School of Engineering
The University of Melbourne, Victoria 3010 Australia
T: +61 3 8344 6613   F: +61 3 8344 7707
Appendix D: Interview Protocol

Section 1. Background Information
a. Attributes of the interviewee
   i. What is your job title?
   ii. What job title do you report to?
   iii. What is your relationship to the Chief Information Officer?
   iv. How are you involved at a strategic level with information security?
   v. Qualifications and experience:
      1. What is your highest level of education?
      2. Do you hold any professional certifications on information security?
      3. How many years of experience with information security?
b. Attributes of the organisation
   i. Roughly how many employees in your organisation?
   ii. What industry does your organisation operate in?

Section 2. Information
a. To explore, does your organisation take the time to discover and identify business information used in daily operations? If yes:
   i. Does that information discovery include business information on social media platforms? E.g. business discussions on LinkedIn
   ii. Does that information discovery include business information on mobile devices? E.g. downloading business emails onto personal mobile phones
   iii. Does that information discovery include business information on cloud based storage? E.g. uploading business documents onto personal Dropbox accounts
b. Does your organisation classify information?
   i. If yes, what are the labels in your classification rating system?
c. Does your organisation have a business strategy document?
d. Does your organisation have an IT strategy document?
e. Does your organisation have an information security strategy document? Why?
   i. If yes, can I please get a (de-identified) copy for analysis?
f. Does your board of directors or equivalent make strategic decisions on information security? If yes, what guidance is available to help them?

Section 3. Valuable Information
a. How does your organisation decide whether information is high or low value?
b. [controls] How would your organisation protect information with high value any differently to other information?
c. [controls] Does possession of high value information affect decisions about what storage, networks or computer servers that information is stored on? How?
d. Does protection of high value information make organisations more secure?

Section 4. Reducing Value of Information
a. To lower the value of information, some organisations might delete old information, lower sensitivity of information, or choose not to hold it in the first place. What are some of the experiences you’ve had with organisations actively lowering the value of information?
b. Does lowering the value of information make organisations more secure?

Section 5. Getting Help
a. What are some of the benefits of outsourcing the storage of information?
b. How does risk appetite affect an organisation’s decision on whether to outsource?

c. [controls] Are there any additional security controls that organisations should use when outsourcing?

d. Could any of the following constrain your organisation from deciding to outsource:
   i. Regulatory compliance
   ii. Industry factors
   iii. Economic factors
   iv. Political factors
   v. Legal factors
   vi. External threat environment
   vii. Valuable information
   viii. Continuous information availability
   ix. Most importantly, Other: __________

e. Does outsourcing the storage of information make organisations more secure?

Section 6. Low Value Information

a. How does your organisation store information that has little value?

b. What are the benefits of this approach?

c. Do minimal efforts to protect low value information make your organisation more secure?

Section 7. Threats

a. Threats can be internal, external or physical. How does the threat environment affect the level or type of controls that an organisation uses to protect information?

b. How does the threat environment affect an organisation’s level of valuable information?

c. Can you think of an example where an organisation actively raised or lowered the value of its information based on the threat environment?

Section 8. Outcomes

a. To what degree (low, medium or high) do security breaches impact your organisation’s:
   i. Public reputation
   ii. Customer trust
   iii. Regulatory compliance
   iv. Share price
   v. Risk of litigation
   vi. Performance reporting
   vii. Protection of trade secrets or IP
   viii. Confidentiality, integrity and availability of information
   ix. Most importantly, Other: __________

Section 9. Philosophical - Information Security (if five minutes left)

a. What is the goal of information security?

b. How important is information to an organisation these days?

c. How can information become unusable over time?

d. How do threats affect an organisation’s information?

e. How do security controls affect an organisation’s information?

f. What is the goal of implementing security controls?
   i. If same answer as 9a goal of InfoSec, then why?

Section 10. Final

a. Have you ever had any resistance on security initiatives from any stakeholders? Why?

b. Who’s driving the decisions to increase the security of information? For example do decisions originate at staff level with a focus on regulatory compliance and
bubble up or at executive/board level with a focus on protecting competitive advantage and bubble down?

c. At a strategic level, how do you measure the security of organisational information?

d. Any other information you’d like to add?

e. What was your impression of this interview?

Thanks for your time!
Appendix E: Example Transcript from an Interview

Craig: What is your job title?

Interviewee: Global CISO and Vice President of Cyber Security, Technology, Risk, and Compliance.

Craig: What job title do you report to?

Interviewee: Chief Technology Officer.

Craig: What is your relationship to the Chief Information Officer?

Interviewee: There’s no Chief Information Officer. CTO oversees all technology and reports to the CEO.

Craig: How are you involved at a strategic level with information security?

Interviewee: I own this end-to-end, strategy to operations. In terms of outcomes, I’m accountable for the actual operations that happen across different functions within the technology function and the businesses, and I own the strategy and the execution plans as well.

Craig: Qualifications and experience: what is your highest level of education?

Interviewee: Master of Information Technology.

Craig: Do you hold any professional certifications on information security?

Interviewee: Yes, CISSP 2003. I had a CISSA that’s expired.

Craig: How many years of experience with information security?

Interviewee: Close to 22.
Craig: Roughly how many employees in your organisation?

Interviewee: 60,000.

Craig: What industry does your organisation operate in?

Interviewee: Resources.

Craig: To explore, does your organisation discover and identify business information used in daily operations?

Interviewee: Yes, by that, you mean data discovery.

Craig: Does that information discovery include business information on social media platforms? E.g. LinkedIn

Interviewee: Correct, that’s part of our cyber intelligence program that looks at external platforms where the company’s material is – essentially, the goal is to look for leaked information more than anything else.

Craig: Does that information discovery include business information on mobile devices? E.g. personal mobile phone

Interviewee: We do allow downloading of business email on personal devices, subject to the device being enrolled on our MDM platform.

Craig: Does that information discovery include business information on cloud-based storage? E.g. personal Dropbox

Interviewee: When it is done through corporate devices, yes, but we don’t actually go in and scan people’s personal cloud storages through other means. Anything using the corporate device, or corporate personal device used as BYOD, all goes through a CASB that we monitor.

Then there are other areas like public forums, yes, but not storage. As in chat forums, support forums, and others where people might upload information, but not private storages.

Craig: Does your organisation classify information according to its sensitivity?
Interviewee: Yes.

Craig: If so, what are the labels in your classification rating system?

Interviewee: Four levels: PUBLIC, INTERNAL USE, CONFIDENTIAL, HIGHLY CONFIDENTIAL.

Craig: Does your organisation have a business strategy document?

Interviewee: Yes.

Craig: Does your organisation have an IT strategy document?

Interviewee: There’s a technology strategy document which ties to the business strategy. It’s part of the business strategy.

Craig: Does your organisation have an information security strategy document? Why?

Interviewee: It’s part of the technology strategy. The strategy itself is at a high level, which basically drives everything else underneath that. It’s not a standalone document. The technology strategy document encompasses the need for security and vision for security comes separately out of it.

Craig: If yes, can I please get a (de-identified) copy for analysis?

Interviewee: That would be tough because it’s the business strategy document. I will try. It will be hard to sanitise it because of the structure of it. Table of contents shouldn’t be an issue.

Craig: Does your board of directors or equivalent make strategic decisions on information security? If yes, what guidance is available to help them?

Interviewee: Not specifically about information security. They set the business strategy, and then, the management executes that strategy.

Craig: Do you report to the board?

Interviewee: Yes, every quarter.
Craig: And the board’s job is to interrogate you about what you see is the risk?

Interviewee: They don’t really interrogate. It’s a different culture. They’re there to support us execute the strategy, so they want to know what our concerns are, and a lot of them are very concerned about cyber, as you’d expect with everything else going on. They have a lot of questions around what we are doing about a certain threat, or how we experience something, and what issues we have, any audit-related findings, and what our plans are to address those, that sort of thing.

It’s more around what do I want to tell them is more the tone, and then, they have specific questions around are we ready for these types of things, or we’re hearing this, or we hear about this big thing, like WannaCry as an example that caused a lot of – and we give quarterly updates, so there’s not a lot of gaps there.

Craig: How does your organisation decide whether information is high or low value?

Interviewee: It’s a bit of a challenge, maturity-wise. The actual decision is the business owner’s decision, the data owner’s decision. We have an enterprise risk management framework that calls out things like impact to reputation, impact to finance, that sort of stuff, different things on what the impact is, and then, people assess the data based on that.

Craig: How would your organisation protect information of high-value any differently to other information?

Interviewee: The types of controls being deployed varies by the nature. For example, if it is digital, my remit is predominantly only for digital data, not hard copies, physical data, so the levels of controls, whether we want to do encryption, whether it’s stored in a certain place, we have repositories that are allowed, specifically based on classification.

Craig: Does possession of high-value information affect any decisions you make about what storage or networks or servers that information sits on? How?

Interviewee: Yes. The controls around the storage and the infrastructure and the monitoring levels varies on the nature of the data stored over there.
Craig: Do you think that protection of high-value information makes your organisation more secure?

Interviewee: I guess it’s the other way around. The security protects the high-value information that we have, which then drives the business value. It’s the drive for protecting the value, as opposed to driving for security.

Craig: To lower the value of information, some organisations might delete old information, lower sensitivity of information, or choose not to hold it in the first place. What are some of the experiences you’ve had with organisations actively lowering the value of information?

Interviewee: All of the data that we have electronically, the data owner has responsibility for it. One of the responsibilities of being a data owner is to manage the life cycle of it. So, you classify those into business records versus other kind of data and associate that with the retention policy.

Anything that is classified as something will default into a certain retention policy, and the only way you deviate from the retention policy is if it’s required as part of litigation or something like that, legal or other. And there are certain types of data, depending on the nature of it, that might need to be kept for many, many years, up to 100 years in some cases.

Then you need to figure out how you store that data. It’s the data owner’s responsibility, how long does this need to be retained. Does it fall outside the normal data retention standards?

Craig: Do you think lowering the value of information can make organisations more secure?

Interviewee: In terms of secure, yes, but more importantly, the value of that information, if it is diminished and it is non-value add, then storing that drives cost in terms of IT and management costs for the storage and backups and everything else that happens with it, which is a lot of the primary drivers for that.

Secondly, if it is stored along with the rest of the information, then it would impact efficiencies of people who actually are looking for some information, and then they come up with 50-year-old information and no means of figuring out, unless they actually go through understanding what this is about.
The data retention and deletion is an operational challenge, even from a data owner perspective. Emails and central repositories like collaboration platforms, SharePoint, it works very well in those ones, but any other place where data is stored, it’s almost impossible to enforce the retention policy.

Craig: What are some of the motivations and some of the benefits to outsourcing the storage of information?

Interviewee: Depends on what, exactly. If it’s just a physical storage itself that’s being outsourced, I’m not really sure other than cost or scalability-wise. The only advantage I see is the hosted cloud storage, as an example. Then maybe the scalability, quickly scale up and down, may be the only benefit.

And then, obviously, probably not just the storage space, it just needs to be part of a broader technology strategy on what gets outsourced and what stays in-house. It’s a risk versus benefit discussion at that time, and strictly speaking, with all the kind of cyber threats and with all the legal implications lately with data breaches and the obligations that come along with it, while, in the past, outsourcing was a cost-driven activity, now that attraction might go away.

Maybe they have like GDPR as an example. Four percent of your company’s global revenue is what’s at stake [as a penalty] if you breach privacy information. So, when you have that kind of a high penalty situation, you want to make sure that you have direct control of the controls that protect that information.

When you have an outsourced environment, I’m not saying you can’t manage it properly, but it gets harder. So, I think what you send outside to an environment outside of your control depends upon what’s at risk.

Craig: It’s not something you would take a risk on because you need…?

Interviewee: We would take a risk for little or no value information, day-to-day stuff. But if it’s highly-sensitive information, merger/demerger, board level strategy documents, then it will have to go into a very special repository where we have management control or visibility.

Craig: A separated network.
**APPENDIX E: EXAMPLE TRANSCRIPT FROM AN INTERVIEW**

<table>
<thead>
<tr>
<th>Interviewee:</th>
<th>Mostly zoning of the network architecture and the overall technology landscapes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Craig:</td>
<td>How does risk appetite affect an organisation’s decision on whether to outsource?</td>
</tr>
<tr>
<td>Interviewee:</td>
<td>The risk appetite is where it all starts. The enterprise risk management will define all of the different types of risks, groups, grouping of risks, and then, each of these risk owners, they will own the specific risk. But the appetite comes from the top, from the board. What's the risk appetite? How much risk are you allowed to take for certain types of risk? That will allow management to execute deviations from there. That's the maturity of the organisation, or organisations, actually, which requires a very firm enterprise risk management framework, and it can’t be a standalone cyber security risk framework. It's got to be framed around an enterprise risk framework where different types of risks have different appetites, and then define how much risk appetite do we have for cyber risk.</td>
</tr>
<tr>
<td>Craig:</td>
<td>Does the board define risk only in financial terms when they write their risk appetite statement?</td>
</tr>
<tr>
<td>Interviewee:</td>
<td>It’s more from overall impact. So, we look at financial, productivity, as in operational impact, and reputation, and so brand and reputation together, health and safety is another one.</td>
</tr>
<tr>
<td>Craig:</td>
<td>Do you think there are any additional security controls that organisations should use when outsourcing?</td>
</tr>
<tr>
<td>Interviewee:</td>
<td>Significantly larger number of controls, specifically around – that’s outside of the technology remit. For example, the contracts and legal, and also the rights to audit. That’s the thing, and you may or may not audit, but you need to be able to make sure that those rights to audit are in the agreements between them, which gives us the assurance that if you want to go and check, you can check.</td>
</tr>
<tr>
<td>Craig:</td>
<td>Could any of the following constrain an organisation from deciding to outsource:</td>
</tr>
</tbody>
</table>

i. Regulatory compliance   Yes   No
Not stop. It depends on if it's privacy related stuff. For example, it depends on what's at stake when it's a regulatory compliance activity. If you want to qualify outsourcing versus [Software-as-a-Service] and others. So if it's outsourcing our infrastructure services, then it's not so much of an issue. But if it's outsourcing in terms of going into a [Software-as-a-Service] solution, then that would be a little bit of a concern because then you need to look at is this a multi-tenanted environment? How do we know when stuff happens because some of the requirements around notifying within a certain timeframe? How do we make sure these things happen? Who owns the risk if that happens? Recent issues around one of the recruitment portals here is a good example of that. Is that the customer of that portal that is liable versus the provider of the service? Obviously, it's the customer, so those kinds of things come, then you start losing the value of outsourcing.

ii. Industry factors  Yes  No

I can't think of a scenario where that would be – if it stops us from competing in a certain industry, yeah. I can't think of a scenario where that kind of situation...

iii. Economic factors  Yes  No

Absolutely. If it is going to be more expensive, obviously not.

iv. Political factors  Yes  No

If you’re operating in a certain jurisdiction, and the number one outsourcing provider there is not on good terms with a particular countries' political environment, it may not be a good thing to outsource. It won’t affect the outsourcing decision. It would affect the selection of the provider.

v. Legal factors  Yes  No

Absolutely. If there are jurisdictions where it’s not business-friendly, or where the laws of the land require or drives very nationalistic approach, for a global company like us, so unless you’re operating only in that country.

vi. External threat environment  Yes  No

It won’t stop, it would just increase our vigilance and cost, I guess. If it's avoidable with a choice, but the external threat environment I don't
believe will change, if someone’s really coming after our information, whether it’s outsourced or insource. It just makes it theoretically easier if it’s outsourced, but it doesn’t necessarily mean that we’re more secure for having it in-house.

vii. High-value information    Yes  No

Not necessarily outsource, it doesn’t influence the outsourcing decision, but where it goes, it would be, and how it was managed, would definitely be influenced. For example, board documents or cyber strategy documents could stay in an outsourced provider facility that we have full visibility and assurance that it’s being protected to our standards or higher. And in some cases, we might have to use an outsource provider because we probably are insecure internally. We might find an outsource provider who’s far more secure than we are. A good example would be merger/demerger discussions where you need to have a lot of third-party involvement. Most companies may not have a secure data room that is externally accessible and allows for collaboration. That’s not something you do every day, unless your nature of business is consulting, so you might end up outsourcing that data room service for that initiative to somebody who’s running a virtual data room as a service, which means they have the ability to onboard, offboard people who have the ability to manage documents and do all the things like watermarking and making sure who printed it and have all sorts of controls, which typically makes it hard to implement it in a large company environment. Internal collaboration is not an issue. It’s when it comes to merger/demerger discussions between two or three parties, then you need to provide a common platform that all three can trust, as opposed to one person’s premises.

viii. Continuous information availability    Yes  No

It depends on how you look at it. That’s based on the assumption that if you do it in outsourced, you’re not having that availability or – that’s a contractual problem. So if you define your SLAs and your requirements really clear up front, and find the right provider, I don’t see why that would be a problem. What will happen is, typically, if you have that high level of availability requirement, and the SLAs around it, you narrow down who you can outsource to, and then usually it’s one of the big players, which comes with a big price tag. Big companies may be okay with that, but then, big companies may have really good infrastructure. I suppose all of this, the value versus cost decision comes in.
ix. Other: If you had a very competitive environment, where your IP, your bread and butter, is all in electronic format, and if you lose that, then you’re going to run out of business. It’s a decision that you’ve got to take very carefully. The bottom line is what’s the impact if it’s lost or the integrity of the data gets changed, what’s the impact? Do you have mechanisms? If you don’t have the maturity to define those requirements up front, then it could be tough.

Craig: Do you think outsourcing storage of information can make your organisation more secure?

Interviewee: I don’t think it makes it more secure. It just gives you the perception that it’s somebody else’s problem, which could be wrong.

Craig: How does your organisation store information that’s got very little or low value?

Interviewee: Lower retention standards, and the controls around it are also very minimal. And obviously, things like don’t use prime storage for that sort of stuff. So, it goes in the standard file share.

Craig: What are the benefits of this approach?

Interviewee: Cheaper commodity storage and less intense operational challenges or availability requirements.

Craig: Do minimal efforts to protect low value information make your organisation more secure?

Interviewee: Using low-value storage doesn’t make it safer directly, but it actually helps in terms of knowing what to protect. The fact that you have low-value stuff sitting in a separate place, so that’s not what you want to worry about. It helps to do security easier or better. As opposed to focusing on everything, you narrow your focus on high-value stuff. From that perspective, yes, I guess.

Craig: Threats can be internal, external or physical. How does the threat environment affect the level or type of controls that an organisation uses to protect information?
Interviewee: It varies based on that. Depending upon, so this is where the threat model works. The changes in the threat landscape drives changes in controls.

Craig: What’s a threat model?

Interviewee: Threat model is let’s say you take a solution or technology environment, you do an analysis of what all can go wrong with it, all of the different types of threats to that environment, the threat actors, and what are the implications of those and what controls are needed.

So if you just take a file share as an example. You start by doing a threat model on it, and see, these are the threat actors and these are the types of things that can happen, and to mitigate each of them, these are the things you need to do, sort of thing.

It’s similar to a risk assessment, except that you have a lot more than just cost impact and likelihood. It helps drive very specific controls. It’s the difference between ISO 31000 framework and an assessment, and then, how do you continuously manage that. The other way to look at it is it’s the operationalisation of a risk assessment. Threat modelling is a domain in itself.

Craig: How do you think the threat environment might affect an organisation’s level of valuable information?

Interviewee: It affects in the sense that it affects where we store our information, and how we store it, and what type of controls we have on it, as if the threat environment, the external threat’s more on a certain type of environment then we, obviously, won’t be using that for sensitive data.

Craig: But it wouldn’t dictate that you would raise or lower the value of information that you hold? It more dictates the controls?

Interviewee: No, we don’t change the value based on the threat environment. We change the controls based on the threat environment.

Craig: Can you think of an example where an organisation, or your organisation, actively raised or lowered the value of information based on the threat environment?
Interviewee: No.

Craig: We’ve all heard of the impacts that a security breach can have on some organisations. On a scale of 1 to 5 where 1 is low importance and 5 is high importance, how important would security breach impacts be on:

i. Public reputation  L  M  H

It depends on what was breached. This is where the assessment of criticality of the nature of the information – as a part of your risk assessment, you look at impact to reputation, impact to brand, impact to financials, health and safety. So, every breach you need to assess the impact.

ii. Customer trust  L  M  H

Absolutely.

iii. Regulatory compliance  L  M  H

Yes.

iv. Share price  L  M  H

Yes.

v. Risk of litigation  L  M  H

Yes.

vi. Performance reporting  L  M  H

Yes.

vii. Protection of trade secrets or IP  L  M  H

Yeah.

viii. Confidentiality, integrity and availability of information  L  M  H
ix. Other: People. Operational technology control systems that manage physical things, so where people are working. Those things can be affected. It can cause physical harm to people. The equivalent of Stuxnet. It does harm to people. That harm to machinery causing the failure that impacts other things in the environment. Take data centres as an example. If your data centre is fully controlled by PLCs and other controllers that manage your environment at the data centre, and you have people in there, and a fire hazard happens and all the control systems that are there to control the doors and stuff have been taken over by somebody, you can't get out. That's a simple example that may be not even – but it's more impactful in the operational technologies where you have people in hazardous areas or platforms, working, and the pressure valves are controlled by electronics, and those things get hijacked, and that can happen. Or if you’re in critical infrastructure, so if your electricity grid gets taken off, then you lose power, and your town could have people who are on life support, in hospitals and other places, that can happen. So, a breach of critical infrastructure like a power grid can cause that kind of stuff.

Craig: Have you ever had any resistance on security initiatives from any stakeholders? Why?

Interviewee: Not so much resistance. It’s more from people not understanding the why, and what's in it for me? Are you going to make my life harder, operations-wise? Our business users are usually thinking, well, you’re affecting my usability of something.

Craig: Who’s driving the decisions to increase the security of information? For example, do decisions originate at staff level with a focus on regulatory compliance and bubble up or at executive/board level with a focus on protecting competitive advantage and bubble down?

Interviewee: Both.

Craig: At a strategic level, how do you measure the security of organisational information?

Interviewee: You measure that by the amount of data breaches and the impact. If you’ve had any business impact because of a breach, how much dollars did you lose because – or how much value did you lose because of a data breach. How much of our intellectual property, or how much IP we have, that sort of stuff.
The value of the IP. What's the value of all the IP that we have developed, and have we had any losses of any of those?

Craig: Any other information you'd like to add?

Interviewee: My favourite is the impact of culture on protecting data. You could have all of these controls that you can put in there. You can have all the frameworks, but at the end of the day, you're relying on the guy at the end of the keyboard to decide that this is the right thing to do for the certain type of data that he or she has been given access to, if he's an authorised user for that data, and what he or she does with that.

It's not that they're trying to be malicious. They're only trying to do their job, but this is how they know how to do it. Storing in Excel and places is a good example. I want to be able to work from home, so let me send it to my personal email address. I'll work from home and send it back. That's a decision that is usually because culturally there's no sensitivity to the threats, or it's going to my own personal account, so I feel it's secure, versus it should not leave the company’s controlled environment.

So, the culture and the appreciation and the awareness of security is a company-wide continuous improvement activity that should exist. You actively shape it. You reward people who are doing the right things and not punishing people. And if somebody did something malicious, then, obviously, exit people loud so that others know as a deterrent. But more importantly, reward good behaviour loudly so people know, oh, that's the right thing to do.

Because you have to go with the assumption that most people are trying to get their job done, as opposed to being malicious, but they may not have the right tools. They don't know how to do it, training, and possibly not given the right guidance on the sensitivity on the data, too, because the data they're handling, they don't understand the value of it.

Craig: What was your impression of this interview?

Interviewee: It was good. It's very data security focused, information security focused. If that was the intent, it's good.

[End of Audio 42:08]
Appendix F: Descriptions of Concepts and Relationships

Table F.1 summarises the findings from the analyses of the concepts discovered.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Information is the key asset around which the other stakeholders and platforms revolve.</td>
<td>MgtCo2 stated “we are pushing toward a data-centric approach to security”.</td>
</tr>
<tr>
<td>Value</td>
<td>Information has a value, which is one of its properties. In terms of dimensions, research participants generally thought it was low, high or irreplaceable.</td>
<td>ITCo4 “Traditionally, organisations … don't make any distinction [between high and low value data] and that's a part of the problem.”</td>
</tr>
<tr>
<td>Control</td>
<td>Control of information affects its location. If information is shared onto cloud-based platforms, the organisation may lose control of it because of the multitude of devices that are used to access the platform.</td>
<td>About Dropbox, ITCo1 explained, “It’s inherently insecure because it’ll take documents and stick them on all different devices. You've got no control over where they are, no control over what's going on and the like. So, we made a ruling that not using Dropbox and got a shared drive … for that specific purpose.”</td>
</tr>
<tr>
<td>Access to Functionality</td>
<td>The separation between information and its utility is important because the end benefit can sometimes be derived without actually owning the information.</td>
<td>ITCo1: “it might be great to have that credit card information, but you're better off finding another way to use that customer identity data, if you want to use the data, and not keeping their information ad-infinitem”.</td>
</tr>
<tr>
<td>Classification</td>
<td>Classification of information is performed by the information owner upon creation.</td>
<td>FinCo1: &quot;security [team] doesn't classify the data; the data-owners do.&quot;</td>
</tr>
<tr>
<td>Location</td>
<td>Information can be located internally, externally but within Australia, and externally anywhere in the world</td>
<td>ITCo2: “The difficulty … is how do you know that, even if it’s on-shore, that it’s not being backed up somewhere off-shore?”</td>
</tr>
<tr>
<td>Concept</td>
<td>Description</td>
<td>Evidence</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Ownership            | Information must have an owner, who remains accountable even if they decide to share the management of information with an outsourcing partner. | ResCo1: “All of the data that we have electronically, the data owner has responsibility for it.”  
FinCo1: “You can’t outsource accountability.” |
<p>| Organisation         | Organisations have various properties with dimensions, including goals and assets. Goals and assets combined affect strategic decisions. | FinCo1: “the simple plan for us is to keep our organisation safe, and our organisation is our customers and ourselves”. |
| Outsourcing Constraints | Numerous conditions can constrain organisations from outsourcing. If even one condition affects an organisation, then outsourcing may not be an option. | FinCo2 considered continuous information availability from outsource vendor to be important, stating, “It’s definitely a constraint. Our expectations are on availability from the provider. If they can’t provide the level of availability we need, then we can’t use them.” |
| Outsourcing Enablers  | Numerous conditions can enable organisations to engage in outsourcing. Their existence makes outsourcing a viable option for organisations. | Budget is an enabler and the lack of it can affect the decision on whether to outsource or not, as confirmed by MgtCo2 “It depends on how much money they have to spend on it”. |
| Information Approach  |                                                                              |                                                                         |
| Securing Valuable Information | If information is valuable, then it must be secured well. | FedGov2: “you have to look at all your data holdings and make very conscious business decisions about what is the most highly protected data that you have and then control access to that”. |
| Evading Trouble       | Removing value from information reduces impact if there is a security breach. | ITCo1: “we’ve taken the deliberate approach of devaluing the information that we have. What I mean is, by taking away the risk, taking away the importance, taking away the impact” |</p>
<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Help</td>
<td>Securing valuable information can be more effective when organisations take advantage of increased security controls and maturity of security processes by procuring services from specialist outsource partners.</td>
<td>FedGov1: “there’s economies of scale for large providers to provide much better services than we can ever provide. And in some of that I include information security as well”.</td>
</tr>
<tr>
<td>Accepting the Risk</td>
<td>Low-value information can be secured using minimal efforts only, which conserves security budget for securing more valuable information.</td>
<td>RetCo1: “Everybody’s got limited resources, and you want to make sure that you apply the appropriate level of security and resource allocation to securing data based on the value of the data. If the value of the data is very low, you don’t want to spend a lot of money in securing it.”</td>
</tr>
<tr>
<td>Strategic Impacts on Organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental Benefits</td>
<td>A security breach can affect a number of factors external to the organisation, such as the organisation’s public reputation or customer trust.</td>
<td>PharmaCo1: “We’re a highly ethical company. … We are very concerned about breach and what that would do to our brand, and especially the nature of the breach. So, whether it’s patient data or it’s donor data, or it’s loss of intellectual property, or denial of service, all of those things would have an impact.”</td>
</tr>
<tr>
<td>Organisational Benefits</td>
<td>Organisations might enjoy benefits which are internal and relate directly to the organisation itself, including avoiding bankruptcy or loss of life, and reducing expenses.</td>
<td>ResCo1: “If you had a very competitive environment, where your IP … is all in electronic format, and if you lose that, then you’re going to run out of business.”</td>
</tr>
<tr>
<td>Outsourcing Benefits</td>
<td>There are many benefits should an organisation engage in outsourcing, including the ability to work collaboratively, evergreen infrastructure, and increased security.</td>
<td>StatGov1: “I feel I’m going to be getting very significant business benefit as a result of moving into Office365 because it offers a range of services that we currently don’t have that should allow us to collaborate better … than we currently do.”</td>
</tr>
</tbody>
</table>
Table F.2 summarises the relationships that were discovered between the concepts.

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Description</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1a</td>
<td>The relationship where the presence of high value information causes an organisation to increase the volume and type of security controls.</td>
<td>FinCo3: “those labels on those documents … drive a differential application of security controls. So, things that aren’t very sensitive, we don’t put as much energy into securing them as we do those things that are very sensitive.”</td>
</tr>
<tr>
<td>P1b</td>
<td>The relationship where the presence of low value information causes an organisation to decrease the level of security controls.</td>
<td>ITCo3: “[if] the information is low value [then] don’t worry about protecting it. We have this concept in our company of minimum viable security.”</td>
</tr>
<tr>
<td>P2a</td>
<td>The relationship where the organisation maintains full control over high value information to increase its security.</td>
<td>RetCo1: “not in an outsource provider, but I will host it in a public cloud, yes”</td>
</tr>
<tr>
<td>P2b</td>
<td>The relationship where an organisation maintaining partial control over high value information increases its security.</td>
<td>FinCo1: “The customer doesn’t care that it wasn’t this organisation that lost their data. They trusted this organisation, not the third party.”</td>
</tr>
<tr>
<td>P3a</td>
<td>The relationship where the ability for information to form the basis of a core competency negatively affecting whether it can be stored externally.</td>
<td>ITCo1: “I’d imagine if someone had credit card information that would be something you’d want to be really tight on. And sure, it might be great to have that credit card information, but you’re better off finding another way to use that customer identity data, if you want to use the data, and not keeping their information ad-infinatum.”</td>
</tr>
<tr>
<td>P3b</td>
<td>The relationship where information does not form the basis of a core competency, which positively affects its ability to be stored externally.</td>
<td>ITCo1: “If something’s non-core, then you’ve got the ability to go out, but then if it’s non-core you probably don’t care as much anyway.”</td>
</tr>
<tr>
<td>Relationship</td>
<td>Description</td>
<td>Evidence</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>P4a</td>
<td>The relationship where an organisational concept positively affects how the organisation decides to approach its information, including storage, use and security.</td>
<td>A business goal for StatGov1 was to reduce customer cost, which they believed would increase customer satisfaction leading to increased revenue, which could then be used towards increasing security controls to better secure valuable information, commenting, “Our goal is to drive cost down for our customers rather than make money for ourselves, and if we generate a surplus, ... that surplus is turned into reduced prices, investing in new products, new services, beefing up our security, literally. Seriously, that's $6 million that's being used over the next three years for our very significant security uplift program.”</td>
</tr>
<tr>
<td>P4b</td>
<td>The relationship where an organisational concept negatively affects how the organisation decides to approach its information, including storage, use and security.</td>
<td>Information platform is an organisational concept that FedGov1 perceived could negatively affect their organisation’s security, stating, “we're very concerned about Dropbox”, ITCo1 stated “We don't have any business Dropbox deliberately … because it's insecure”, and FedGov2 stated “We don’t allow instances of … Dropbox”.</td>
</tr>
<tr>
<td>P5</td>
<td>The relationship where an outsourcing constraint negatively affects how the organisation decides to approach its information, including storage, use and security.</td>
<td>Outsourcing that required sharing of information with vendors negatively affected organisational security, and RetCo1 flatly refused to even consider partnering with an outsource vendor to manage their information, stating, “I would be very hesitant to hand my data to somebody who tells me they're going to store my data securely on my behalf. That's not a service I would consume in any way, shape, or form”.</td>
</tr>
</tbody>
</table>
## APPENDIX F: DEFINITIONS OF CONCEPTS

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Description</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>P6</td>
<td>The relationship where an outsourcing enabler positively affects how the organisation decides to approach its information, including storage, use and security.</td>
<td>Security controls are a concept that affects the security of information and PharmaCo1 perceived that over time, outsource vendors are maturing and getting better at applying security controls to protect information, stating &quot;outsourcers now are very security aware. … outsourcing partners have better security controls than we have because it's their core business.&quot;</td>
</tr>
<tr>
<td>P7a</td>
<td>The relationship between fortification techniques positively affecting the security of an organisation.</td>
<td>When asked whether protection of high value information makes an organisation more secure, ITCo3 answered, “Yes.”</td>
</tr>
<tr>
<td>P7b</td>
<td>The relationship between devaluation techniques positively affecting the security of an organisation.</td>
<td>ITCo3: &quot;in the same way that a bank that holds no money is a less attractive target to rob, yes&quot;.</td>
</tr>
<tr>
<td>P7c</td>
<td>The relationship between outsourcing techniques positively affecting the security of an organisation.</td>
<td>When asked whether outsourcing information storage can make an organisation more secure, ITCo3 answered “it can”.</td>
</tr>
<tr>
<td>P7d</td>
<td>The relationship between minimisation techniques positively affecting the security of an organisation.</td>
<td>When asked whether their organisation perceived that minimal efforts to protect low-value information made their organisation more secure, RetCo1 answered, “Yes, I do, because then you can actually put the resources where the valuable information is.”</td>
</tr>
</tbody>
</table>
## Appendix G: Data Structure

<table>
<thead>
<tr>
<th>First-Order Concepts</th>
<th>Second-Order Categories</th>
<th>Aggregate Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information ownership and utilisation are distinct not co-dependent</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Information ownership is contingent on its utility towards org goals</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Information is the key asset not the ICT systems it resides on</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Information as an asset affect governance and structures</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Full control avoids leaks from external parties and devices</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Partial control increases security but cannot decrease accountability</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>No control reduces cost and responsibilities</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Value can be low or high and affects classification and controls</td>
<td>Value</td>
<td>Information</td>
</tr>
<tr>
<td>High value can extend to being irreplaceable if it’s a trade secret</td>
<td>Value</td>
<td>Information</td>
</tr>
<tr>
<td>Information ownership and utilisation are distinct not co-dependent</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Information ownership is contingent on its utility towards org goals</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Information is the key asset not the ICT systems it resides on</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Information as an asset affect governance and structures</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Full control avoids leaks from external parties and devices</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Partial control increases security but cannot decrease accountability</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>No control reduces cost and responsibilities</td>
<td>Access to Functionality</td>
<td>Information</td>
</tr>
<tr>
<td>Value can be low or high and affects classification and controls</td>
<td>Value</td>
<td>Information</td>
</tr>
<tr>
<td>High value can extend to being irreplaceable if it’s a trade secret</td>
<td>Value</td>
<td>Information</td>
</tr>
<tr>
<td>If information is valuable, then it must be secured well</td>
<td>Securing Valuable Info</td>
<td>Information</td>
</tr>
<tr>
<td>Valuable information is usually stored internally for added control</td>
<td>Securing Valuable Info</td>
<td>Information</td>
</tr>
<tr>
<td>Removing the value of information reduces impact from a security breach</td>
<td>Evading Trouble</td>
<td>Information</td>
</tr>
<tr>
<td>Three ways to reduce value are to avoid, tokenise, and delete</td>
<td>Evading Trouble</td>
<td>Information</td>
</tr>
<tr>
<td>Outsource partners have robust, mature security controls</td>
<td>Outsourcing Constraints</td>
<td>Information</td>
</tr>
<tr>
<td>Engaging their services to protect valuable information can increase security</td>
<td>Outsourcing Constraints</td>
<td>Information</td>
</tr>
<tr>
<td>Low value information can be secured using minimal efforts only</td>
<td>Accepting Risk</td>
<td>Information</td>
</tr>
<tr>
<td>This can increase security by conserving budget for higher value info</td>
<td>Accepting Risk</td>
<td>Information</td>
</tr>
<tr>
<td>Goals affect the value and use of information as an asset</td>
<td>Organisation</td>
<td>Information</td>
</tr>
<tr>
<td>Available assets affect strategic decision-making</td>
<td>Organisation</td>
<td>Information</td>
</tr>
<tr>
<td>External environmental conditions affect strategic decisions</td>
<td>Outsourcing Enablers</td>
<td>Information</td>
</tr>
<tr>
<td>Existence of valuable information affects storage decisions</td>
<td>Outsourcing Enablers</td>
<td>Information</td>
</tr>
<tr>
<td>Outsourcer partner quality affects trust</td>
<td>Outsourcing Enablers</td>
<td>Information</td>
</tr>
<tr>
<td>Some conditions must be met to engage in outsourcing</td>
<td>Outsourcing Enablers</td>
<td>Information</td>
</tr>
<tr>
<td>Includes existence of budget and trust in partner’s security controls</td>
<td>Outsourcing Enablers</td>
<td>Information</td>
</tr>
<tr>
<td>Public reputation affects customer trust and share (stock) price</td>
<td>Environment Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Regulatory compliance can have severe impacts if not maintained</td>
<td>Environment Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Customer trust affected the risk of litigation</td>
<td>Environment Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Severe impacts from a breach include bankruptcy and loss of life</td>
<td>Organisation Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Protection of trade secrets also severe but takes longer to manifest</td>
<td>Organisation Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Expense frugality and increased productivity also benefits</td>
<td>Organisation Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Systems have higher availability and are more secure</td>
<td>Outsourcing Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Employees are more agile and collaborative</td>
<td>Outsourcing Benefits</td>
<td>Information</td>
</tr>
<tr>
<td>Reduced costs and workload on employees</td>
<td>Outsourcing Benefits</td>
<td>Information</td>
</tr>
</tbody>
</table>
Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Horne, Craig Andrew

Title:
Understanding information security strategy in organisations

Date:
2018

Persistent Link:
http://hdl.handle.net/11343/227196

File Description:
Final thesis file

Terms and Conditions:
Terms and Conditions: Copyright in works deposited in Minerva Access is retained by the copyright owner. The work may not be altered without permission from the copyright owner. Readers may only download, print and save electronic copies of whole works for their own personal non-commercial use. Any use that exceeds these limits requires permission from the copyright owner. Attribution is essential when quoting or paraphrasing from these works.