Towards Governance of Information Security Incident Response

Craig A Horne[1]
Computing and Information Systems, The University of Melbourne,
Parkville, Victoria, Australia

Sean B Maynard
Computing and Information Systems, The University of Melbourne,
Parkville, Victoria, Australia

Atif Ahmad
Computing and Information Systems, The University of Melbourne,
Parkville, Victoria, Australia

ABSTRACT

Organizations are increasingly digitizing their business models to complement or even replace physical contact with customers and suppliers. With this shift online comes an increase in information security attacks, which are occurring more frequently due to the increased attack surface, vulnerabilities in security controls, and a target-rich environment. Organizations prevent attacks however some attacks are still successful and result in security incidents that degrade operations. When an organization is successfully breached, the organization must respond to the incident as quickly as possible to ensure continued operations and business resilience. However, guidance is lacking for governance of the response function. In a thematic review, we find good governance plays a key role in smooth and efficient incident response and this paper extends knowledge about governance of information security incident response by identifying key governance concepts that improve incident response efforts within organizations.

Keywords: Governance, information security, cyber security, incident response, incident management.

[1] Dr Craig A Horne. hornec@unimelb.edu.au +61 3 8344 1573

INTRODUCTION

Globally, organisations are increasingly digitising their business models to complement or even replace physical contact with customers and suppliers (Bharadwaj et al. 2013a). With this shift online comes an increase in information security attacks, which are occurring more frequently due to the increased attack surface and target-rich environment (ACS 2016; Gupta and Sharman 2012). The problem is that a board of directors is accountable to shareholders for achieving organisational goals using internal capabilities, however extant incident response governance models do not link with the governing body to allow it to set direction for this.

This research investigates how an organisation should govern their response to information security incidents to ensure business resilience. The scope of the study includes identifying governance concepts within an organisation and their relationships. The research question is: *How should organisations govern information security incident response?*

The significance of this study is established by advancing knowledge about governance of information security incident response. The paper continues by reviewing the extant knowledge about governance of information security and focusses specifically on responding to a security incident. It then discusses a proposed structure for governance of information security incident response and concludes with key insights and suggestions for future research.

BACKGROUND

In conducting the literature review, employed the three-step search process suggested by Webster and Watson (2002). First, we manually searched all issues of the leading information systems journals (AIS Senior Scholars' Basket of Eight[2]) dating back to 2000, to ensure currency. Second, we performed a database search of the leading IS journals using keywords such as "governance of information security" or "information security governance" combined

[2] see https://aisnet.org/general/custom.asp?page=SeniorScholarBasket

with keywords such as "incident response" or "incident management". Third, we conducted similar searches in the *ABI/Inform, Business Source Complete (EBSCO)* and *JSTOR* databases, as leading information systems databases. Additionally, we searched for relevant standards published by the International Standards Organisation. This extensive search for governance of information security incident response papers discovered few that were relevant. This review therefore continues in three sections, first a review of governance of information security, then information security incident response, finishing briefly with the intersection between them.

Governance of Information Security

Information security governance forms part of overall corporate governance (McFadzean et al. 2006). Generally, corporate governance includes the governing body setting a strategic **vision and mission**[3], sharing responsibility via the corporate structure, ensuring reporting back up the organisation, **internal** and **external stakeholders** communication, shaping employee behaviour and culture, and aligning **team goals** with **organisational goals** such as **organisational resilience** (McFadzean et al. 2006). Maintaining integrity in reports back to the governing body and learning for the long-term from lessons are crucial (McFadzean et al. 2006).

The **governing body** of an organisation governs information security to align the objectives of information security with the vision and mission of the organisation, deliver value to the organisation, and to ensure that risk is appropriately managed (ISO/IEC 2013). Governance of information security has been defined as a "*system by which an organization's information security activities are directed and controlled*" (ISO/IEC 2018, pp. 4). This governance forms one part of the internal context of an organisation, along with the organisational structure, various employee roles and their accountabilities. Employees who are

[3] Concepts in **bold** appear in the conceptual model in Figure 1

information and system owners require ongoing education and training on the management of information security. Governance of information security ensures the confidentiality, integrity, and availability of information and often an **information security management system** is used for this. Objectives of information security governance include aligning an **information security strategy** with the **organisation's business strategy**, improved **risk management**, cost-effective resource management, accurate performance measurement, and deriving value from additional information security resources and capabilities (Brotby et al. 2006).

There are several frameworks available that guide the governance of information security in organisations. At the strategic level, the organisation's leadership team sets the information security strategy to ensure a return on investing in information resources (Da Veiga and Eloff 2007). An organisation's board of directors is required to direct and control the organisation and is accountable for success or otherwise (Posthumus and Von Solms 2004). To direct and control the organisation, directors are therefore also required to direct and control information security, because information is a crucial resource for any modern organisation. To direct information security, they must set a strategy for it with long-term goals, and approve **policies** to shape employee behaviour. To control information security, they must receive regular reports from **information security staff** on the current status of all information security initiatives. These reports help the directors monitor the effectiveness of the strategy and policies, and adjust resourcing for them via the **finance** function and a **budget** (Posthumus and Von Solms 2004).

Information Security Incident Response

Once the governing body of an organisation has approved an information security strategy, it directs **executive** management to implement an information security strategic plan that complies with the strategy (Horne et al. 2017). This information security strategic plan

includes a variety of different areas of information security, including security policies (ISO/IEC 2017b). Information security policies support the organisation's vision and mission, and harmonise with other **business policies**. One of these security policies is the information security incident management policy, which lists the processes, responsible managers, accountability and responsibility sharing, SETA programs, and reporting lines back to the leadership from the coal-face. **Internal stakeholders** are listed, including **legal** general counsel, public relations and media staff, the marketing liaison staff, managers in charge of other departments, security employees, system administrators and network engineers, other technology employees, service desk staff, executives, and possibly building facilities staff (ISO/IEC 2017b). This policy is monitored for effectiveness with responsible employee names and job titles (ISO/IEC 2017b).

The information security **incident response process** has six stages, including planning and preparing, detecting incidents and then reporting them both internally and externally, assessing the situation and making decisions about the best path forward, responding to the incident, recovering any damaged systems, and finally conducting a post-incident report and learning from any mistakes that may have been made (ISO/IEC 2017a; Tøndel et al. 2014). The incident response staff monitor security events, which are common occurrences of low-level security anomalies. When security events combine to indicate something more sinister is occurring, then they are escalated as a security incident, ensuring accurate **record keeping**.

Security Incident Response and Governance

Governance of an organisation is controlled by the governing body of an organisation, which in the private sector is the board of directors (Humphreys 2008). One basic aim of governance is to ensure that the activities of all employees comply with the prevailing law so that board directors are not exposed to personal liability and hence penalties. Governance concepts

also include ensuring an effective risk management process is utilised by employees, which is supported by a range of internal controls to ensure adherence (Humphreys 2008). Information security governance involves identifying all information resources within an organisation, implementing corresponding controls to secure all the information resources, and then monitoring the effectiveness of these controls over time to assess whether more resources or different controls are required to mitigate any risk. The risk management process complements governance by offering a process for identifying all information resources, assessing the inherent risk in exposing the information to a threat actor, guiding appropriate application of **controls** to secure **information** from **threats**, and then monitoring residual risk to the information resources over time (Humphreys 2008). Organisations maintain an awareness of **external environmental** and **internal conditions** that may affect the governance structures in place and respond appropriately through the risk management process. Information security **incident response staff** are typically technically-focussed and share knowledge in the lessons-learnt phase at the end, to improve other organisational functions (Ahmad et al. 2012).

PROPOSED GOVERNANCE OF INFORMATION SECURITY INCIDENT RESPONSE

In this section, we use open coding to take all the textual data in the preceding literature review section and break it up into discrete concepts. We then use axial coding to draw connections between these concepts and identify the core concepts, termed categories, via inductive and deductive thinking, emphasising casual relationships identified in the literature, which form a basic frame of generic relationships depicted in Figure 1. Finally, we use selective coding to identify the key category, which in this case is governance (Corbin and Strauss 2008). These concepts include the governing body of an organisation primarily making decisions about securing the information within the organisation based on the law, the threats that present

themselves, and other external environmental conditions. The incident response team take their cues from the risk management process and policies that have been approved by the board and complete their work by collaborating with the information security management team.

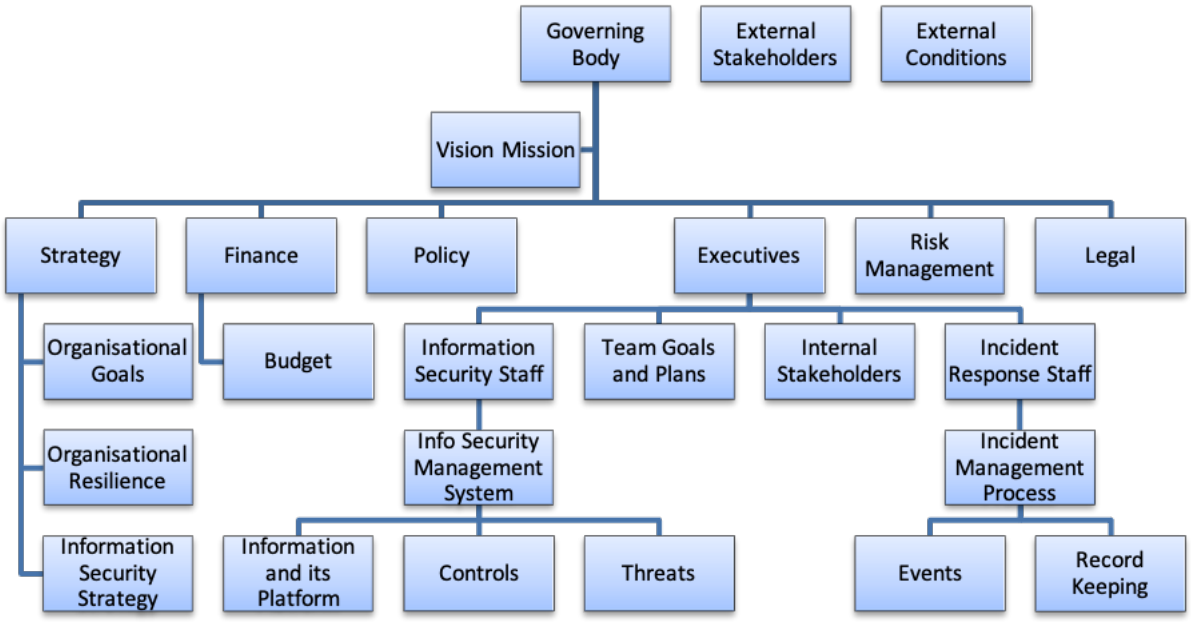

Figure 1. Proposed Conceptual Model of Security Incident Response and Governance

The organisation's strategy helps identify goals that must be achieved. The strategy is approved and set by the governing body with drafting assistance from the executive layer. Other tools that the governing body can use to shape employee behaviour and achieve these organisational goals are implementing a robust risk management program, setting policies, approving financial budget, monitoring expenditure, and employing a legal function. The governing body delegates responsibility for value-creating work to the executives, who then share responsibility with managers and information security staff underneath them. In return, staff report back to the governing body their progress towards goal achievement.

The organisational strategy provides enough information for the organisation to identify what information resources are required to achieve the organisational goals. This then informs

the setting of an information security strategy, along with consideration of the environmental conditions that affect the organisation. Information security staff can then identify team goals that align with and help achieve overall organisational goals. The intention is to generate value and return-on-investment from the information resources that have been identified and listed in an asset register. These information resources can be hosted on several platforms including technological infrastructure, paper when printed, and human brain memories. These information resources are secured by technology and business security controls to maintain their confidentiality, integrity, and availability. These controls are regularly monitored for effectiveness by security staff by conducting risk assessments against known threats.

Incidents are handled by the incident response staff via a formalised process. The process includes planning and preparing for the security incident ahead of time and implementing appropriate security controls to mitigate the risk from known threats, detecting and reporting any security incidents to relevant stakeholders via a preprepared communications plan, assessing the security incident for severity and deciding how to proceed, responding to the security incident to contain and defeat the attack, recovering any damaged systems and restoring them back to full operations, and finally conducting a post-incident review with the intention of learning from the incident to improve preventative controls and avoiding a reoccurrence.

CONCLUSION

The aim of this research is to investigate how an organisation should govern their response to information security incidents to ensure business resilience. The proposed model is an improvement on existing models because it provides the core concepts and relationships in a holistic governance model for information security incident response that connects with the governing body and is significant in that it establishes an impact in several areas. First, extant

academic literature does not address the topic of how governance of information security incident response links the top-most governing body down to the operational teams performing the incident response work, so this paper extends knowledge in this area. Second, there is a practical aspect to the problem of how to govern information security incident response and this paper identifies the functional teams, their organisational structure, board-level tools, record keeping requirements, and work products to be present when governing incident response.

As a suggested future research direction, the proposed model put forward in this paper has been developed based on a review of academic literature and international standards related to incident response, so a practitioner's perspective would be valuable to validate the model and improve generalisability of this model to organisations of various sizes and geographic locations. Also, researchers could conduct action research, where the governance model described in this paper could be collaboratively implemented within consenting organizations to collect empirical evidence. Researchers could apply critical reflection to understand underlying causes and help predict organizational change in resilience when responding to security incidents. Another direction is to investigate whether the scope of this proposed model relates to information residing on digital platforms only, or other platforms, such as ICT infrastructure, paper, and human memories. Finally, exploring the role of SMART KPIs in incident response governance would be a valuable addition to this model.

REFERENCES

ACS. 2016. "Cybersecurity: Threats, Challenges, Opportunities." Retrieved 28/3/2017, 2017, from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Ahmad, A., Hadgkiss, J., and Ruighaver, A.B. 2012. "Incident Response Teams–Challenges in Supporting the Organisational Security Function," *Computers & Security* (31:5), pp 643-652.

Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., and Venkatraman, N. 2013a. "Digital Business Strategy: Toward a Next Generation of Insights," *MIS Quarterly* (37:2), pp 471-482.

Brotby, W., Bayuk, J., and Coleman, C. 2006. *Information Security Governance: Guidance for Boards of Directors and Executive Management*. Illinois, IT Governance Institute.

Corbin, J.M., and Strauss, A. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (3rd ed.). Thousand Oaks, CA: Sage Publications Inc.

Da Veiga, A., and Eloff, J.H.P. 2007. "An Information Security Governance Framework," *Information Systems Management* (24:4), pp 361-372.

Gupta, M., and Sharman, R. 2012. "Determinants of Data Breaches: A Categorization-Based Empirical Investigation," *Journal of Applied Security Research* (7:3), pp 375-395.

Horne, C.A., Maynard, S.B., and Ahmad, A. 2017. "Organisational Information Security Strategy: Review, Discussion and Future Research," *Australasian Journal of Information Systems* (21), pp 1-17.

Humphreys, E. 2008. "Information Security Management Standards: Compliance, Governance and Risk Management," *information security technical report* (13:4), pp 247-255.

ISO/IEC. 2013. "27014:2013 Information Technology — Security Techniques — Governance of Information Security." Geneva, Switzerland: ISO/IEC.

ISO/IEC. 2017a. "27035.1 Information Technology—Security Techniques—Information Security Incident Management Part 1: Principles of Incident Management." Geneva, Switzerland: ISO/IEC, pp. 1-33.

ISO/IEC. 2017b. "27035.2 Information Technology—Security Techniques—Information Security Incident Management Part 2: Guidelines to Plan and Prepare for Incident Response." Geneva, Switzerland: ISO/IEC, pp. 1-69.

ISO/IEC. 2018. "27000:2018(E) Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary." Geneva, Switzerland: International Organization for Standardization and International Electrotechnical Commission.

McFadzean, E., Ezingeard, J.-N., and Birchall, D. 2006. "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions," *Journal of Information System Security* (2:3), pp 3-48.

Posthumus, S., and Von Solms, R. 2004. "A Framework for the Governance of Information Security," *Computers & Security* (23:8), pp 638-646.

Tøndel, I.A., Line, M.B., and Jaatun, M.G. 2014. "Information Security Incident Management: Current Practice as Reported in the Literature," *Computers & Security* (45), pp 42-57.

Webster, J., and Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp xiii-xxiii.