Author/s:
Anderson, A;Ahmad, A;Chang, S

Title:
Case-based learning for cybersecurity leaders: A systematic review and research agenda

Date:
2024-11-01

Citation:
Anderson, A., Ahmad, A. & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information and Management, 61 (7), pp.104015-104015. https://doi.org/10.1016/j.im.2024.104015.

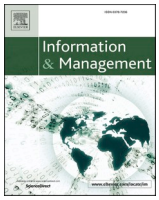
Persistent Link:
https://hdl.handle.net/11343/348155

Information & Management 61 (2024) 104015

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im



Case-based learning for cybersecurity leaders: A systematic review and research agenda☆

Ashley Anderson *, Atif Ahmad, Shanton Chang

University of Melbourne, Parkville, Vic 3052, Australia

ARTICLE INFO

Keywords:
Cybersecurity management
Information security management
Case-based learning
Higher education
Executive education
Chief information security officer (ciso)
competence
competency

ABSTRACT

Increasingly, large organisations are turning to cybersecurity leaders to protect their information resources against attack. However, because cybersecurity leadership roles are new, educational literature and practice targeting this role are nascent. In this systematic review, we assess the value of case-based learning (CBL) in educating cybersecurity leaders. We also aim to discover what gaps, if any, exist in this body of research. We find that cybersecurity leaders' attitudes and metacognitive abilities are important but overlooked elements of their competence, and that CBL has potential to develop these competencies. The article concludes with a competency matrix and agenda for further research.

1. Introduction

Modern organisations face an evolving challenge in protecting their information and IT infrastructure [1,2]. Threats facing businesses, governments, and not-for-profits can change rapidly, and an attack on information resources can stop an organisation in its tracks. In the infamous 2020 SolarWinds attack, for example, advanced persistent threat actors took a blended approach, using a novel technique to inject malicious software, mimicking legitimate communication protocols, and using anti-forensic techniques to cover their tracks [3,4]. Thousands of customers downloaded the affected code; compromised clients included Microsoft, the Cybersecurity and Infrastructure Security Agency (CISA), and even the Pentagon [4]. Estimates of the annual global cost of cybercrime reach into the trillions—one firm predicted US $8 trillion for 2023 alone—well beyond the annual global costs of natural disasters [5]. Industries with the highest exposure to incidents include hospitals and basic utilities [5], meaning that the costs of incidents are not just financial. When hospitals are unable to treat patients, or aged-care facilities are unable to turn on heat or air conditioning, the costs can include human lives [5,6].

With such challenges to face, cybersecurity has ceased to be a low-level operational problem—responding to such incidents effectively "requires command, control, and coordination" to enable teams to "develop situation awareness, adapt to the rapidly evolving situation, raise the necessary resources, and respond to threats" [7, p. 1]. Unless cybersecurity leaders can coordinate effectively across the whole organisation, they risk inadequate incident responses and even delayed incident detection [8]. In other words, organisations now exist in an environment filled with severe, unpredictable threats and need strategic leadership to survive them.

Increasingly, large organisations are engaging high-level cybersecurity leaders—such as Chief Information Security Officers (CISOs)—to lead the effort in protecting information resources against such threats [9,10]. Cybersecurity leaders' roles are unique; they are distinct from operational cybersecurity roles in their need for business strategy and communication skills [11] and are distinct from other leadership roles in their need for command and control against active attackers [7,12]. From this unique position, they play a vital enabling role in the broader business. Protecting the organisation's data, information, and knowledge enables the firm to pursue innovative new products, and protecting the organisation's technological infrastructure supports its overall operational continuity [1]. Given recent changes to the US Federal Trade Commission regulations, the cybersecurity leader brings these protection skills to the boardroom [10,13].

Initial professional education is unlikely to equip graduates with this unique skill set, as many cybersecurity knowledge frameworks are

☆ Note: A reduced version of this paper was accepted at the International Conference on Information Systems (ICIS), 2022. The ICIS paper analyses the role of the cybersecurity leader but does not explore the value of case-based learning.

* Corresponding author at: School of Computing and Information Systems, University of Melbourne.
E-mail addresses: anderson.a@unimelb.edu.au, abanderson@student.unimelb.edu.au (A. Anderson).

https://doi.org/10.1016/j.im.2024.104015
Received 14 November 2022; Received in revised form 28 July 2024; Accepted 28 July 2024
Available online 2 August 2024

operationally focused [14,15]. Hallett et al. [14] compared four frameworks against the UK Cybersecurity Body of Knowledge (CyBOK), including the National Initiative for Cybersecurity Education (NICE) and the Institute of Information Security Professionals (IISP). Although all five frameworks cover a wide range of topics from CyBOK, they are heavily focused on operational roles relating to network, software, and hardware security [see 14, p. 6]. Cybersecurity graduates educated using these frameworks will be well prepared for operational roles [15]; however, once they progress to leadership, cybersecurity professionals need skills beyond the technical [9,11].

As they progress to leadership positions, cybersecurity professionals are struggling to find high-quality leadership education targeted to their role [9]. This assertion may seem counterintuitive. Industry bodies do provide high-quality certifications for managers and advanced practitioners, such as the Certified Information Security Manager® (CISM®), COBIT and CGIET certifications, administered by ISACA, as well as the Certified Information Systems Security Professional (CISSP) management certification run by $(ISC)^2$. Universities are even providing Master of Cybersecurity degrees that aim to impart management skills (e.g., University of Queensland [16]). Nonetheless, the CISSP domains remain highly operational, centring on such areas as network security, identity and access management, and security operations [17]. Master of Cybersecurity curricula continue to be dominated by similar concerns [18,19]. The CISM® domains are more comprehensive [20].

Ongoing struggles in organisational practice suggest that some competencies are missing from our existing educational frameworks—something that differentiates strategic leadership from management [21–24]. After a series of workshops in 2022, Hielscher et al. found interviewed CISOs "to be somewhat detached from the organisation and its day-to-day business" [21, p. 11]. In 2013, Ashenden and Sasse found that CISOs could inadvertently hinder information security by expressing an autocratic stance in discourse [22]; in 2022, both Da Silva [23] and Da Silva and Jensen [24] noted that CISOs can inadvertently contribute to their own isolation by their use of specialist and fearful language. This disconnect itself is unsurprising; a recent global survey of CISOs found that they still largely have a technical education, technical professional experience, and have their time dominated by technical risks [25]. Recent research still shows CISOs striving to obtain legitimacy with the C-suite and board [10]. Given this disconnect, and the continually evolving nature of the field, there is scope for researchers to continue to work with industry to "to compare the ever-changing skills of the field as they relate or need updating based upon changes to technology, the landscape, and computing power" [9, p. 275].

The first step in addressing the challenges in cybersecurity leadership education is to refresh our understanding of the competencies needed [26]. Our choice of the word *competencies* rather than *skills* is deliberate; we seek to understand cybersecurity leadership from a situated professionalist viewpoint, situating competencies into their professional context, as well as from an integrated occupationalist viewpoint, integrating the necessary knowledge, skills, and attitudes (i.e., competencies) into one framework [27]. Like many knowledge frameworks, our framework of competencies for cybersecurity leaders necessarily will include a range of knowledge areas. Like previous research efforts, our framework will include a range of skills as well; however, we consider that performance is affected by conative/affective components as well as cognitive components [28], and thus attitudes also must be considered. In summary, this paper teases apart the knowledge and skill facets, incorporates relevant attitudes, and situates the competencies in the real-world challenges facing the modern CISO.

As discussed above, this paper looks beyond the current certifications to generate our competency framework. Whitten [29], Haqaf and Koyuncu [30], and Smit et al. [31] also have investigated aspects of leadership competencies in recent years. However, Smit et al. [31] restricted their analysis to soft skills, and Haqaf and Koyuncu [30] assessed skills only, not all dimensions of competencies. Furthermore, cybersecurity leaders' roles are constantly changing [1,30] and not very well understood [24], which suggests that all three analyses [29–31] are best considered as components of a broader body of literature. Our first objective in this paper, therefore, is to survey the existing literature and generate a framework of competencies required by cybersecurity leaders, yielding our first research questions:

RQ1. *What insights can be gained by applying a multidimensional competency lens to cybersecurity leadership?*

RQ2. *What is the current state of understanding of the competencies of cybersecurity leadership in extant literature?*

To provide strategic advice, cybersecurity leaders also require educational methods tailored for strategic roles [32]. In this paper, we explore one such education method—case-based learning (CBL)—and its suitability for educating cybersecurity leaders. Evidence suggests that learning with cases is valuable for executive learners [33,34]. For example, in reflecting on the experiences of Harvard Business School educators, Garvin [33] described how cases provide executive learners with a connection between their experiences and relevant theory. Rosenbaum and Shermis [34] found that scenarios enable information systems executives to test actions and consequences in cases that closely mimic their real lives.

Nascent evidence also suggests that CBL may be valuable for cybersecurity leaders specifically [35–38]. For example, Ahmad et al. [35,37] found that using a teaching case in information security management courses led to active debate, increased engagement, and an improved ability to apply a business perspective to information security. Indeed, IS researchers Cram and D'Arcy [38] explicitly called for researchers to write and make available more teaching cases to address "the increasing business focus of security education" [38, p. 33]. However, the body of literature exploring CBL in cybersecurity education is nascent, and for cybersecurity leaders, smaller still. This scarcity of research presents both a constraint and an opportunity; although there is not a significant body of literature exploring CBL for the relevant group of *learners*, there is an opportunity to review literature exploring CBL for the relevant group of *competencies*. Such a review can import insights from a variety of industries that conduct scholarship of teaching and learning. Consequently, after investigating the competencies needed by cybersecurity leaders, this paper evaluates the applicability of CBL to those capabilities. This aim yields our third research question:

RQ3. *To what extent is CBL applicable to the competencies of cybersecurity leadership?*

This paper contributes to the literature by presenting an agenda for empirical research. We identify gaps and biases in the extant literature and propose research questions and methodologies to explore both cybersecurity leadership and the potential of CBL. Furthermore, this paper contributes to practice by presenting an updated competency framework for the cybersecurity leader. This framework requires empirical validation, as set forth in the research agenda, but the proposed set of competencies represents the current understanding of cybersecurity leadership in the literature. Finally, the paper contributes to practice by proposing specific embodiments of CBL that educators can use in their teaching.

This article is structured as follows. First, we provide relevant background on the concept of competencies and on CBL approaches. Then we set out our methods for addressing both research questions. We follow the systematic review methodology set out by vom Brocke et al. [39] to collect data, followed by a content analysis approach for data analysis. In our results regarding the competencies required by a cybersecurity leader, we present a matrix of knowledge, skills, attitudes, and roles, followed by a description of each role. In our results on the value of CBL, we present a report of the competencies CBL is particularly suited to developing. We then synthesise our findings to describe the cybersecurity leadership role and propose the cybersecurity leadership competencies supported by CBL. We conclude by describing the gaps in

the existing literature and presenting an agenda for further research.

2. Background

2.1. The competency lens

The twin concepts of *competence* and *competency* have been hotly contested with respect to their meaning and their value to education. However, in a review of the literature, Blömeke et al. [28] noted several areas in which the field generally agrees. First, that the concept of competence is defined, in general, with respect to real-world situations; it is bound up with performance in actual tasks or scenarios. Second, that the term *competence* is an holistic term, referring to the overall ability to perform; whereas *competency* is an analytic term, referring to individual facets of competence. Salman et al. [40] brought additional nuance to their review, noting that in some cases, the terms *competence* and *competency* are used in similar and even overlapping ways. In this paper, to clearly differentiate the two concepts, we proceed with the agreements noted above and summarised in this passage by Mulder [41, p. 111]:

Professional competence is seen as the generic, integrated, and internalised capability to deliver sustainable effective (worthy) performance (including problem solving, realising innovation, and creating transformation) in a certain professional domain, job, role, organisational context, and task situation. Competence consists of various competencies. A competency is a part of generic competence; it is a coherent cluster of knowledge, skills, and attitudes that can be used in real performance contexts [41, p. 111].

In other words, this paper uses *competence* to refer to an individual's overall capacity to perform in a role. Because competence is internal, it must be inferred from observed performance or behaviours [28,40,42]. We use *competency* (plural: *competencies*) to refer to individual attributes [28,41,43].

Many subcategories of competencies have been proposed, including not only knowledge, skills and attitudes but also, variously, motives, self-image or self-concept, values, and even intuition [40,41,44-46]. The field generally has shown wide agreement in dividing competence into a cognitive component—consisting of traits like knowledge and skills—and a conative/affective component—consisting of traits such as attitudes [28,40]. Furthermore, within the cognitive component, a differentiation between knowledge and skill has been generally accepted [44,47,48], drawing on an older division between "knowing that" and "knowing how" proposed by Ryle [49].

A separate debate about the value of competence-based education has typically included criticisms of excessively partitioned checklists of tasks, as well as criticisms of the limitations of the construct of competence with respect to liberal education [27,42]. However, the value of competence as a construct has been more widely accepted in professional settings and in professional education [27]. It also is possible to move beyond a granular, task-based approach, grounded in functional behaviourism, by shifting the focus toward an integrated occupationalist and situated professionalist viewpoint [41]—that is, by integrating clusters of competencies and applying them to higher-level domains or "roles" [42,44].

Other theorists, while not denying a division between skills and propositional knowledge, do raise questions about what "knowing" looks like when put into practice. Schön, questioning a positivist view of professional expertise, proposes *knowing-in-action* as a distinct type of knowledge [50,51]. Eraut, discussing theory and propositional knowledge, proposes that knowledge "rarely gets taken off the shelf and applied without some kind of transformation" [43, p. 157]. Schön similarly describes the processes of *reflecting-in-action* and *reflecting-on-action* as processes by which knowledge is generated in analysing new professional challenges [50,51]. Therefore, while the integrated competency model of knowledge, skills, attitudes, and roles addresses many of the attributes needed to produce professional competence, educational literature points to another dimension, another kind of competency not captured by the integrated model.

Notably, processes akin to reflecting-in-action feature heavily in models for more advanced practitioners [43,47]. Writing on competencies for management, Eraut [43] describes *control knowledge*, a complex concept including reflection, self-evaluation, and organising one's knowledge. He describes this metacognitive form of "knowledge" as "the means by which one uses all the other forms of knowledge" [43, p. 81]. Similarly, when differentiating between professional competence and expertise, Evers and van der Heijden [47] add *metacognitive knowledge* and *conditional knowledge*. In this definition, if knowledge is "knowing that" and skill is "knowing how," then conditional knowledge is "knowing when and where or under what conditions" [47, p. 87]. Indeed, Evers and van der Heijden [47] claim that "expert" status requires a practitioner to have "analytical techniques used only in new situations" [47, p. 88], a description bearing similarity to reflecting-in-action [51]. In these passages, we glimpse an attribute for advanced practitioners that enables professionals to analyse complex situations, analyse their own knowledge and skills, and decide what action to take.

Reviewing the work of Schön and others, Cheetham and Chivers [52] integrate reflection into their conception of professional competence. They do not include reflection as a category alongside such attributes as knowledge, skills and attitudes but instead describe reflection and other "meta-competencies" as "permeating" the core components [52, p. 269]. This structure accords with Eraut's definition of the reflective "control knowledge" as the means by which professionals make use of other competencies [43].

For the purpose of this paper, we examine the competencies of cybersecurity leaders as a desirable end state so that we may design and direct cybersecurity leadership education appropriately. This examination also will enable us to evaluate educational methods, as effective methods then can be defined as those that help a cybersecurity leader develop the target competencies.

We propose to follow the broadly accepted division between knowledge and skills, and the further division between these cognitive facets and the conative/affective facet (i.e., attitudes). To situate these attributes in professional context, we further propose to use the integrated approach described by Gonczi et al. [44] and Hager [42], applying these internal traits to high-level tasks or roles. Thus, for our purposes, competence consists of:

- *Knowledge*: an understanding of concepts, principles, rules and procedures;
- *Skills*: abilities as applied in practice;
- *Attitudes*: desires and values; and
- *Roles:* higher-level areas of practice to which knowledge, skills, and attitudes are applied, also called *domains* or *functions* [44].

Because our long-term research aims are ultimately directed toward educational *practice*, we deliberately selected a streamlined competency model, one that practitioners can use to generate intended learning outcomes. For that reason, in this paper we do not further subdivide the conative/affective component into such aspects as motives, values, self-image, self-concept, or intuition [40,45,46]. We do not deny that these concepts are valuable; however, in this systematic review of the literature on the role of the CISO, we do not anticipate the extensive writing on the conative/affective component that would justify further analytic divisions. Instead, we use the umbrella term *attitudes*, as used by Gonczi et al. [44], Mulder [41], and Mulder and Winterton [27]. Similarly, we do not subdivide knowledge into further categories; rather, to make our framework accessible to practitioners, we broadly group all competencies related to recall or understanding as "knowledge" and all competencies applied in practice as "skills" [44,49].

We propose including the metacognitive/reflective attribute in our analysis for cybersecurity leaders, who indeed are advanced practitioners who regularly encounter new, complex professional challenges.

For ease of communication, we propose using the term *reflection* to refer to the reflective "meta-competency" described by Cheetham and Chivers [52], as well as the reflective elements described variously as meta-cognitive knowledge, conditional knowledge [47], control knowledge [43], and reflecting [43,52], whether real-time reflecting-in-action or deliberative reflecting-on-action [50,51]. Like Cheetham and Chivers [52], we do not propose to use reflection as a component alongside knowledge, skills, and attitudes. Instead, we consider reflection to be a "matrix competency" or "meta-competency"—the means by which one uses the other competencies [43]. As with the other dimensions, we do propose not to further subdivide this "meta-competency" into its multifaceted parts, but rather to acknowledge the role of reflection in enabling practitioners to deploy their other competencies.

This model allows us to investigate the capabilities needed by cybersecurity leaders, the roles played by cybersecurity leaders, and explore how these leaders can apply capabilities to professional situations in context. This integrated approach also has the advantage of laying bare the subtle requirements that often are skipped in lists of necessary skills. For example, in the 2010s, engineers from a competing firm combined a range of tactics to steal information about a mobile-phone testing robot [35]. Improved communication amongst physical security, information security, vendor management, and R&D personnel could have stopped the attack sooner, but the disconnects in communication almost certainly were not due to a lack of communication *skill*. Rather, the personnel involved needed knowledge of what information was salient to communicate and with which departments, and a commitment to maintaining organisational situational awareness [36]. We propose that cybersecurity leaders facing novel situations like these are likely to require conative/affective traits (i.e., attitudes) as well as the reflective ability necessary to select and deploy relevant skills.

2.2. CBL

In addition to industry certifications, most cybersecurity professionals pursue undergraduate or postgraduate education at universities [53]; however, most university education continues to adhere to traditional, lecture-based modes of instruction [54–56]. Although lecture-based learning continues to offer value [57], many analyses have found that effectiveness improves when integrating active, student-centred learning techniques [55,58–60].

CBL is one such student-centred learning approach, which uses hypothetical or real-life scenarios to give learners practice in applying concepts to professional situations. As discussed in the Introduction, research on cybersecurity leaders continues to show a disconnect between these leaders and the rest of the business [10,21,22,24], and early research about CBL proposes that it is valuable for bridging precisely this kind of gap [35–38].

What is meant by the term "case-based learning" depends to some extent on the occasion; embodiments of CBL vary widely. Differing definitions of CBL abound; Jonassen's [61] typology describes embodiments ranging from learners reading cases as examples to learners constructing new cases themselves. Nonetheless, the literature does point to a few characteristics of effective CBL. High-quality CBL often involves a well-facilitated discussion of the case [62] and, for higher-order learning outcomes, solving a problem based on the scenario rather than simply discussing the events [61]. This experience can be enhanced by thoughtful use of multimedia [63]. To maximise effectiveness, educators also can consider the learning sequence carefully; for example, an educator might choose to present a case before presenting the relevant theory, so that the theory is situated in a narrative context [63]. These techniques can vary but all retain the core characteristic: a learning experience centred around a narrative.

CBL has the potential to develop relevant competencies in multiple ways. First, working with cases allows learners to situate theory and practice with respect to a narrative [64], interleave practice on a range of skills [65], and vicariously experience a wide range of scenarios [66], all of which help learners quickly choose a course of action and carry it out. Second, comparing multiple cases can help "low-structure learners" and "example learners" behave more like "high-structure learners" and "rule learners," improvements in learning capabilities that aid conceptual comprehension [65]. Third, learners can use cases to practise the skill of case-based reasoning [61,67], in which they reason about how to approach new incidents based on prior experiences. Case-based reasoning is associated with faster reasoning in unfamiliar scenarios [66,67]. In summary, the CBL literature suggests that cybersecurity leaders can make use of cases to vicariously experience a wide range of organisational scenarios, situate their learning of theory with respect to those scenarios, and then quickly solve new problems, referring to cases as prior experience.

As mentioned above, the research relating CBL to cybersecurity leadership education is nascent. Ahmad et al. [35–37] have found cases to be effective in engaging information security management students in commentary and debate and in helping them appreciate the potential for conflicts and dilemmas in their roles. Yuan et al. [68,69] also found cases to be useful in teaching a range of security management topics. To find more research into the value of CBL for cybersecurity, we need to broaden our lens to encompass the information security field as a whole.

A range of educators teaching technological techniques to prevent and respond to attacks have found cases to be helpful in improving learner engagement and results [70–72]. He et al. [72] proposed CBL as a valuable approach for novice instructors, noting that analysing cases helps novice instructors learn how to "interpret security issues, gain contextual knowledge, personal skills and situated experiences" [72, p. 2]. Other researchers have experimented with introducing CBL for elementary information security topics [73], network engineering skills [74,75], and ethics in information security [76]. Describing the benefits of CBL, these authors frequently cite motivation and interest [35,36,68,69,71,72] and connection of disparate concepts and practices [35,36,71,73].

In this paper, after exploring the competencies required by cybersecurity leaders, we investigate the value of the CBL approach for developing those competencies.

3. Research methodology

We chose a systematic review methodology to address our research questions. As described by Webster and Watson [77], a systematic review "closes areas where a plethora of research exists, and uncovers areas where research is needed" [77, p. xiii]. That is, exploring the current literature systematically allows researchers to ascertain whether existing literature has sufficiently addressed a research question or if there are gaps in the current research body, which aligns with our research aims.

3.1. Literature search process

We conducted two searches: one search for RQ 1 and RQ 2, regarding the competencies of cybersecurity leaders, and the other search for RQ 3, regarding the utility of CBL. For both searches, we followed the systematic review process set out by vom Brocke et al. [39], as documented in Table 1.

For both the competency and CBL searches, we selected databases by identifying a selection of top-tier scholarly journals in the field and then checking the database publication lists against those journals. For our competency search, we selected ProQuest Central; for our CBL search, we selected Education Source (EBSCO).

In both cases, the lead author refined the search results (step 2 in Table 1) as follows. The search results were exported to a spreadsheet containing the author, date, title, DOI or URL, and abstract of each publication. The initial results were scanned to remove duplicates and contributions in languages other than English. The lead author then reviewed the titles and abstracts of papers for inclusion, recording either

Table 1
The search process.

	Competencies of cybersecurity leaders	Utility of CBL
1. Database search	Search date: 7 May 2023 - Database: ProQuest Central (ProQuest) - Search string: noft("Chief information security officer" OR CISO) OR (noft ("cybersecurity" OR "cyber security" OR "information security") NEAR noft (director OR manager)) - Peer-reviewed only Result: 204 search results	Search date: 14 May 2023 - Database: Education Source (EBSCO) - Search string: ("case-based learning" OR "case based learning") AND (utility OR value OR impact* OR effectiveness OR efficacy OR comparison) - Peer-reviewed only Result: 172 search results
2. Refine: remove irrelevant results	Criteria: - Primarily relates to the competencies required by cybersecurity leaders - Is in English Result: 14 relevant articles (out of 204)	Criteria: - Primarily relates to the utility or efficacy of case-based learning in tertiary or professional education. - Is in English Result: 14 relevant articles (out of 172)
3. Backward chaining of results from item 2	Criteria: - Primarily relates to the competencies required by cybersecurity leaders - Is in English Result: 5 additional articles	Criteria: - Primarily relates to the utility or efficacy of case-based learning in tertiary or professional education. - Is in English Result: 10 additional articles
4. Forward chaining of results from item 2	Criteria: - Primarily relates to the competencies required by cybersecurity leaders - Is in English Search tool: Google ScholarResult: 7 additional articles	Criteria: - Primarily relates to the utility or efficacy of case-based learning in tertiary or professional education. - Is in English Search tool: Google ScholarResult: 4 additional articles
5. Supplementary search for industry reports on the role of cybersecurity leaders	Search date: 21 May 2023Search engine: GoogleSearch terms: cybersecurity leader organisation CISO director of cybersecurityCriteria: - Primarily relates to the competencies required by cybersecurity leaders - Is in English Source: Government and reputable industry publicationsResult: 5 additional articles	N/A
6. Sum of rows 2–5	31 articles	28 articles
Final sample:	**59 articles**	

"yes" for inclusion or a reason for exclusion. Where relevance could not be determined based on the title and abstract, the lead author reviewed the full text. Following our initial searches, we performed backward-chaining and forward-chaining [39,77] to find sufficient sources for a robust analysis.

We selected the database for our competency search using a selection of premier journals from the AIS Senior Scholars' List of Premier Journals [78] and including a selection of journals recommended by the Security Special Interest Group (SIG SEC). Both ProQuest Central and EBSCO made all journals available; however, EBSCO does not publish full texts from the *International Journal of Information Security* and *Journal of the Association for Information Systems* until after 12 months.

We selected ProQuest Central for its superior coverage, and ran our search using ProQuest's "noft" function—that is, searching the title, author, abstract and keywords of an article, but not its full text (i.e., "no full text" or "noft"). In line with the recommendations of vom Brocke et al. [39, p. 215], we carefully selected our keywords to exclude contributions that are not relevant. We searched either for instances of "cybersecurity," "cyber security," or "information security" near mentions of "director" or "manager" or, alternatively, for mentions of "Chief Information Security Officer" or "CISO". We restricted our search to peer-reviewed sources only.

We excluded 8 contributions in languages other than English and 180 contributions for failing to meet our inclusion criterion (the paper must primarily concern the role of the cybersecurity leader). We excluded one other article due to age: Wylder [79] described a role for information security managers that is almost unrecognisable due to changes in technology between 1992 and 2023. We selected sources that explicitly described knowledge, skills, or attitudes required by cybersecurity leaders, or which described the roles they perform. This inclusion criterion, paired with the search terms, means that we did not survey the body of literature concerning cybersecurity management and governance that did not explicitly discuss the role of the leader.

Given our focus and search criteria, the number of relevant academic papers was low. Moreover, the topic of cybersecurity leadership is also frequently discussed in industry sources. Therefore, for the topic of competencies needed by cybersecurity leaders, we also conducted a Google search to select grey literature from government agencies and top-tier consultancies [80]. When using the Google search engine, the lead author logged out of Google to minimise the personalisation of search results. The lead author refined these search results, initially by title and then by a full read, looking for sources that explicitly describe knowledge, skills, or attitudes required by cybersecurity leaders or that describe the roles they perform.

We selected the database for our CBL search using a selection of A*-, A-, or B-ranked education journals from Scimago [81] and excluding titles focusing on childhood development, education of teachers, research methods for education, or educational policy. Education Database contained only 6 of 10 journals identified, whereas EBSCO contained 9 of 10.

We selected EBSCO for its superior coverage, and ran our search on the full text of entries, as EBSCO does not have a "noft" function. To exclude contributions that are not relevant, we sought only mentions of "case-based learning" or "case based learning" that also mention its efficacy, effectiveness, impact, utility, or value. We also restricted this search to peer-reviewed sources only.

We excluded 2 contributions in languages other than English, 5 duplicates, and 118 papers that failed to meet our inclusion criteria: the paper must not be for childhood (K-12) education, and it must primarily discuss the utility of CBL against named competencies. That is, we excluded papers that measured the effect of CBL on students' results but did not specify the skills or intended learning outcomes being measured. We also excluded papers that specified clearly nontransferable learning outcomes, such as diagnosis based on medical imaging. Finally, we excluded papers that only reported students' perceived learning, given the common discrepancies between students' perception of learning and their actual learning [55,82]. In other words, in the parlance of the Kirkpatrick taxonomy of evaluation, we excluded papers that identified the "reaction" level without specifying the "learning" level [83].

3.2. Data analysis method

We used a modified content analysis approach [84] to analyse our search results. We began with a more grounded approach, extracting

relevant sentences and then assigning codes to functions and attributes of the cybersecurity leader mentioned in our articles. Because our search explicitly sought knowledge, skills, attitudes, and roles, our next step followed traditional content analysis, classifying the emergent competency codes as knowledge (K), skill (S), or attitude (A). We then grouped knowledge, skill, and attitude codes to into higher-level themes or "axial" codes for their relevant roles (R). For example, we clustered the codes *Plan incident response strategy* (S), *Lead response and recovery* (S), and *Lead incident investigations* (S) into the theme *Leading incident response* (R). A sample page from our codebook appears as Appendix C.

4. Results

Our search for the competencies of cybersecurity leadership revealed a small but growing body of literature. The small body of literature is representative of organisational practice in cybersecurity more broadly. For example, despite the widespread acknowledgement in industry and government of the critical need for cyberthreat intelligence to better combat cyberthreat actors, a recent review of practice research in cyberthreat intelligence only revealed a handful of papers on organisational practice [85]. We found little research addressing the role of the cybersecurity leader explicitly. Cybersecurity and information security research tends to focus on management as a practice rather than on the role of the manager; that is, much research focuses on the actions that organisations typically take rather than on the individuals who carry out those actions. We speculate that the longstanding technological perception of the role has held back research in this area.

Our search for the utility of CBL resulted in a more substantial sample; however, our criteria for the search limited the sample. Many of our results did not measure the efficacy of CBL, preferring descriptions of learner perceptions to measurements of learning, or else did not disclose the competencies or learning objectives against which the method was measured.

Our two searches also revealed very little intersection of the two bodies of literature, with very little research examining the utility of CBL for cybersecurity leadership, information security management, or even information systems more generally. For that reason, in this section we present the results of the two searches separately before proposing relationships in Section 5.

4.1. Results: Competencies required by cybersecurity leaders

The 31 articles analysed included 24 from peer-reviewed journals and conferences. Our results also included publications regarding the role of cybersecurity leaders from the Australian Cybersecurity Centre and New Zealand Cyber Security Centre; the Carnegie Mellon Software Engineering Institute; New York Society of CPAs; Deloitte, Ernst & Young; and Forbes. In the small, emerging body of research on the cybersecurity leader, most articles described a role focused not only on technological risk, but also on influence, strategy, and organisational behaviour.

Cybersecurity leaders may be positioned at either middle management or executive management, but our sample typically looked at leadership in the context of organisations large enough to have a board—organisations in which the cybersecurity leader acts at a strategic or tactical level rather than an operational level. We did notice some variation amongst the results; for example, Hooper & McKissack [86], in choosing to examine the role of the CISO via job advertisements, concentrated their search on smaller organisations. As a result, the competency needs identified did vary somewhat between the strategic and tactical levels. However, we did not survey competency needs at a purely operational level. In other words, because our research question focused on the leader rather than on the early-career professional, all of the knowledge, skills, attitudes and roles that we identified are intended to refer to the context of management or executive leadership.

Table 2 summarises the higher-level themes—the roles—generated from the knowledge, skill, and attitude codes. The full list of sources supporting each knowledge, skill, attitude, and role is provided in Appendix A.

Table 2
Key themes (cybersecurity leadership) and selected references.

Theme (Role)	Selected references
Co-create cybersecurity with business leaders	Aguas et al. [11]; Da Silva & Jensen [24]
Lead the cybersecurity team toward enhanced integration	Ashenden & Sasse [22]; Burg et al. [1]
Direct cybersecurity strategy	Baskerville et al. [96]; Maynard et al. [87]
Direct cybersecurity governance and policy	Aguas et al. [11]; Monzelo & Nunes [91]
Oversee the SETA program	Ashenden & Sasse [22]; Hielscher et al. [21]
Oversee cybersecurity risk management	Alexander & Cummings [12]; Baskerville et al. [96]
Lead incident response	Shayo & Lin [89]; Whitten [29]

4.1.1. Role: Co-create cybersecurity with business leaders

In this role, cybersecurity leaders must act more like interpreters than security professionals. Maynard et al. [87] observed that cybersecurity leaders' communication role is sometimes limited to overseeing the cybersecurity awareness program, but that cybersecurity leaders must also advocate to business leaders to be effective: "[The CISO] must be able to clearly communicate the strategy in clear and understandable terms to convince and secure the buy-in of all relevant stakeholders" [87, p. 71]. The literature highlights the need for cybersecurity leaders to provide business leaders with well-contextualised reports, the need to advise them about relevant risks, and the need to advocate for the cybersecurity function—sometimes all at once. As Fitzgerald [88] remarked, "the savvy CISO…shows how they are reducing ongoing costs, reducing the wait time necessary for business user access to systems, or reducing the lost productivity which happens as a result of a virus" [88, p. 261].

The need to be able to communicate with leaders was a strong recurring theme, but sources also pointed to the importance of partnering with leaders who work for vendors, clients and even regulators. Cybersecurity leaders need the skills to foster relationships and create a culture within the cybersecurity team of building relationships and sharing information. Notably, however, only Aguas et al. [11] and Shayo and Lin [89] placed equal importance on the willingness to put effort into collaboration. Aguas and colleagues put it plainly: "CISOs and their teams that do not make an effort to understand and partner with the business leaders often become roadblocks to the business achieving its objectives" [11, p. 76]. Considering the cybersecurity risks brought about by disconnects in communication [8], we assert that being viewed as a "roadblock" by other leaders is itself a risk factor, and thus that a commitment to collaborating with other leaders is integral to the cybersecurity leader's role.

Throughout our findings, we noticed a tension at the heart of this position: Business leaders engage cybersecurity leaders with the aim of controlling risk [86,90–92]. Simultaneously, business leaders frequently accept risk to achieve business objectives and feel frustrated by risk-conscious cybersecurity leaders who advise limitations on their activities [11,12]. Indeed, more recent analyses suggest that CISOs and executive/board leadership are acting together to create a kind of "soothsayer" role for the CISO, one in which the CISO interprets and forecasts risk and even may be expected to advise on whether the risk is acceptable [24]. Effective cybersecurity leaders navigate this tension—and gain the trust of business leaders—by learning about business objectives, helping leaders decipher information about the threat landscape, and advocating for resources in line with leaders' risk tolerance [11,87,93–95]. Skills in communication are essential for this endeavour, but we argue that the knowledge of what information to convey and the

commitment to collaboration are equally essential for the cybersecurity leader to succeed.

4.1.2. Role: Lead the cybersecurity team toward enhanced integration

In their role as co-creator of security, our findings suggest that cybersecurity leaders must act as interpreters of technical information for strategic leaders. In their role as team leaders, our findings suggest that cybersecurity leaders must act as interpreters of strategy for technical personnel. As described by Burg et al. [1], "the CISO's role is to explain security concepts in terms that can be understood within the C-suite (e.g., through the use of analogy) and to educate the security team about the business drivers that direct the focus of security investment." The authors considered the example of the Global Chief Security Officer at TikTok, who engages with strategic decision-makers weekly and prepares the team for changes needed to integrate security by design and privacy by design. We propose that this role is a necessary complement to co-creating security with business leaders. Failing to align tactical and operational-level cybersecurity teams with strategic aims can lead to gaps in threat intelligence and incident reporting [8], while aligning the team with strategic objectives can enhance situational awareness [87].

Here again the literature focuses heavily on skills. Ashenden and Sasse [22] are an outlier in observing that "an autocratic stance inhibits effective information security" and in encouraging cybersecurity leaders to "[emphasise] delegation and empowerment of employees with an acceptance that, as a result, mistakes and errors may occur" [22, p. 404]. On a related note, Shayo and Lin believe that cybersecurity leaders should "have the ability to create a culture of shared responsibility and accountability should a breach occur" [89, p. 9]. Although our results did not frequently focus on such attitudinal requirements, there is evidence that cybersecurity leaders are more effective if they avoid demonising failure.

4.1.3. Role: Direct cybersecurity strategy

Our findings show that without an explicit focus on knowledge, skills, and attitudes, educators and industry professionals gravitate toward describing skills. Therefore, it is notable that in the "cybersecurity strategy" theme, so many articles touched on a knowledge component; there was broad agreement that cybersecurity leaders need to understand the overall strategy of their organisation. Effective cybersecurity leaders "recognise that security should not be in isolation to the business. They understand the prevailing threat landscape faced by the organization, they also understand the long-term objectives and goals of the organization" [87, p. 73]. Indeed, they "must be able to ascertain what is going on in the business to adequately support the mission" [88, p. 262]. The literature showed broad agreement that cybersecurity leaders need to understand the organisation's strategy, develop and implement a cybersecurity strategy in alignment with the organisation's strategy, and then allocate resources effectively in service of that strategy.

By contrast, only one paper pointed that cybersecurity leaders' understanding of the organisation's strategy depends on their willingness to make an effort to understand it [11]. Furthermore, only one article mentioned that cybersecurity leaders need to "employ creativity and imaginative thinking to devise effective and relevant strategies" [87, p. 72]. However, the lack of ubiquity here might not speak to a lack of importance, but rather may speak to a general trend wherein researchers, employers, and educators focus on measurable skill requirements and presume that if the skill requirement is reached, then the corresponding knowledge and attitude requirements are also met.

According to Baskerville et al. [96], directing the organisation's cybersecurity strategy also involves selecting the right balance between the "prevention paradigm" and "response paradigm." The authors describe the prevention paradigm as one in which leaders look for predictable, measurable risks and assume a static relationship between security controls and risk reduction—a paradigm associated with the time before an incident occurs. In contrast, they describe the response paradigm as one in which leaders assume that risks are unpredictable and safeguards must be innovative to be effective—a paradigm often associated with response after an incident. Cybersecurity leaders, they contend, must "strategically balance security operations across both paradigms depending on the organizational context" [96, p. 139]. Baskerville et al. also speculate that the prevention paradigm is "dominant in contemporary commercial organizations" [96, p. 149]. Our findings indicate that the prevention paradigm may dominate the research view of the cybersecurity leader as well. Although many articles in our sample pointed to the need for cybersecurity leaders to be competent strategists, only Baskerville et al. [96] and one other paper [87] describe strategies that encompass a response "mode."

As for the need for cybersecurity leaders to use creativity and imaginative thinking, it is possible that this skill is important despite its infrequent appearance in the literature. Indeed, Baskerville and colleagues argue, deploying the response paradigm is becoming more important:

"While a dependence on the prevention paradigm works with repetitive and low-sophistication attacks, progressively more sophisticated attacks demand the increasing use of the response paradigm. Managers who understand the incident-centred model and whose environment reflects increasing sophistication in attacks will recognize the need to place additional emphasis on activities in the organization's response paradigm" [96, p. 150].

In other words, much of the extant literature on the role of the leader does not address the response paradigm. However, Baskerville et al. [96] and Maynard et al. [87] contend that cybersecurity leaders need to be increasingly aware of the response paradigm—and be able to select the right balance between the paradigms—to direct cybersecurity strategy effectively in the face of increasingly sophisticated threats.

4.1.4. Role: Direct cybersecurity policy and governance

Unsurprisingly, our review found that cybersecurity leaders need to be able to implement a suite of policies, plans, and procedures. In the service of strategy, leaders must be able to oversee these policies and procedures with effective governance. This link between strategy and governance is noted in Deloitte's report "The New CISO," in which they assert that CISOs need to "understand which business operations and information assets are the enterprise crown jewels" and "institute strategic governance that prioritizes information security investments" [11].

Governance is a prime example of an essential role of cybersecurity leaders that can be overlooked by organisations and educators. When combatting a cyber-attacker, governance is a crucial tactic; indeed, breaking down silos minimises organisational exposure [36]. And yet, many organisations still place cybersecurity leaders under Chief Information Officers (CIOs), ignoring their importance outside the realm of IT [97]. As Lanz points out, "even if the CISO can control all technology-related risks, hackers can take advantage of the human factor…and place the organization at unnecessary risk" [97, p. 57]. Cybersecurity leaders must be able to influence the whole organisation to be effective [97], and according to the literature, this influence must extend beyond the security education, training, and awareness (SETA) program into governance and policy [11,30,91,97–99]. Arguing for breaking down the silo even further, Loonam et al. [100] identify reviewing "the flow of business processes *across the organization*" as "critical" for strategic leaders [100, p. 3761, emphasis added]. They emphasise that strategic leaders should not outsource this task, as the review "significantly supports a more strategic view of how cyber-security systems can effectively protect the organization" [100, p. 3761].

4.1.5. Role: Oversee the seta program

The need to oversee the SETA program came up comparatively infrequently; furthermore, many of the mentions about security

education, training, or awareness had more to do with marketing than education. According to an industry report by Deloitte, cybersecurity leaders need to "draw from the work of consumer marketers in developing communications" [11, p. 86]. One participant cited in Hielscher et al. [21] even spoke of publishing stories in their organisation's internal newspaper. In interviews with CISOs analysed by Ashenden and Sasse, existing cybersecurity leaders spoke about delivery channels, market segmentation, and creative messaging, adding: "it isn't really necessarily a set of security skills that are needed—it's a set of marketing skills" [22, p. 403]. Clearly, cybersecurity leaders in the industry see the need for a complex set of communication skills.

Building on the communication-skills component of SETA, both Loonam et al. [100] and Hielscher et al. [21] proposed that trust and communication need to flow both ways to be effective. In these more recent papers, we see a mandate for strategic leaders to supplement top-down communication and training with "a bottom-up appreciation for the potential risks and threats facing the organisation" [100, p. 3765], a "culture of openness toward errors and mistakes" [100, p. 3761], and a willingness to "break those silos, start working with other departments, listen to them, [and] accept contradicting ideas" [21].

4.1.6. Role: Oversee cybersecurity risk management

The cybersecurity leader's role as a risk manager was by far the most frequently described in the literature. Information security risk and technology skills featured in 3 of the top 4 skills ranked by CISOs in a 2018 Delphi study, including a broad umbrella "skill" of understanding such standards as ISO 27,001 and such frameworks as NIST and COBIT [30]. In 2021, 49 % of the CISOs surveyed by Ernst & Young confirmed that compliance is "the most stressful part of their job," and 57 % predicted that regulation will become more fragmented in the next few years [1]. Risk management competencies came up repeatedly [e.g., [101-104]] and with more nuance than the leadership skills, resulting in a large array of well-sourced competency codes. We consider that this weighting reflects a general perception of cybersecurity leaders in which managing technological risk and compliance are thought to be the entirety of the role rather than components of it.

Here again, some of the most interesting competencies came up in the knowledge and attitudinal requirements. In a 2016 interview, one cybersecurity specialist contended that a "a CISO who is narrowly focused on technology cannot see the broader spectrum of cyber risk. Threat actors constantly change their cyberattack methodologies, so having a CISO who has the ability to look beyond technology and at the corporation and its people, customers, and suppliers holistically has become imperative" [12]. That is, cybersecurity leaders must understand risk holistically, even while others may conceptualise cyber risk narrowly as a technological problem.

If the first step is for cybersecurity leaders to understand risk as a whole-of-business concept, the next step is for cybersecurity leaders to be willing to accept calculated risk in service of the business. The Deloitte report makes the connection neatly, saying that cybersecurity leaders need to "understand risk in terms of its potential to positively affect competitive advantage, business growth, and revenue expansion," and adding that "the ability to accept more risk can increase business opportunities, while ruling it out may lead to their loss" [11, pp. 79, 81]. This attitude would seem to run counter to the role of a security professional, but multiple sources describe it as an alignment with the organisation's overall risk appetite [11,97,98].

Additionally, cybersecurity leaders need to maintain organisational situational awareness. In one of the results from our supplementary search, CTO Deepak Gupta describes cyberspace as "a chessboard with pieces constantly moving. The critical and crucial moves are being continuously made, making it necessary to put proper emphasis on defensive cyber posturing" [94, para 3]. For Gupta, organisations must cultivate a defensive posture for a constantly changing landscape—one with an active opponent [94]. An information security manager cited by Baskerville et al. [96] uses an alternative metaphor that highlights how leaders need to conceptualise an organisation's situational awareness in both prevention and response modes:

"Information Security shouldn't be thought as the security of a closed and barricaded castle, but as the security of an airport, crossed by millions of people, where the exact control of who enters and leaves is not possible, but however security of processes and smooth operations must be guaranteed, so that the whole machine has to work regardless of who enters and leaves. Nevertheless processes that recognize and block the anomalies must be activated. Response must be quick" [96, p. 149].

These cybersecurity leaders are expressing that they cannot manage risk effectively through risk management, even with situational awareness, solely in prevention mode. While recognising that they cannot exercise "exact control of who enters and leaves," these leaders need to help the organisation recognise "anomalies" or the opponent's "crucial moves." This finding suggests additional complexity to the competencies "oversee risk management" and "maintain organisational situational awareness." We question whether educators can define these competencies with a simple series of knowledge, skills, and attitudes, because the competencies may have different dimensions in prevention mode and response mode. We revisit this question in Section 5.

4.1.7. Role: Lead incident response

The roles described in Sections 4.1.1–4.1.6 pertain mainly to "business as usual." One could argue that during business as usual, a cybersecurity leader behaves much like any other business leader, albeit a leader with more awareness of a constantly shifting threat landscape. In contrast, incident response requires the cybersecurity leader to address breaches and hacks, which could range from minor business continuity incidents to major disasters.

The incident response role requires cybersecurity leaders to not only plan incident response strategies, but also test and rehearse them [12,89,105]. In crisis situations, cybersecurity leaders need to show a "flexible problem-solving approach" and remain calm enough to "facilitate the appropriate response" [29, p. 16]. Additionally, Whitten asserts that the "problem-solving attribute should also entail investigative skills that aid in tracking a security issue trail" [29, p. 16]. In this role, cybersecurity leaders need to be able to problem solve and make decisions in real time, as well as to analyse scenarios afterward to prevent recurrence. Time-sensitive problem-solving and decision-making skills are challenging to teach and sometimes deprioritised in cybersecurity education.

We might predict that Baskerville et al. [96] would place this competency firmly in response mode. In our descriptions of the strategy and risk management roles, we have described the prevention mode as characterised by traditional risk management and the response mode as characterised by incident response. However, Baskerville et al. offer a connection between incident investigations and prevention mode, noting that organisations can use double-loop learning, improved defences, and lawsuits to translate incident response into incident prevention [96]. It is notable that even incident response competencies have dimensions related to both prevention and response modes.

4.2. Results: Utility of CBL

In our search, we uncovered a mature body of literature exploring CBL in a range of professional fields. A great deal of research has explored CBL, often in medical and education fields. This research frequently examines particular designs or tools, such as the effect of a multimedia CBL system, and it often measures the success of CBL through learner perceptions or increases in motivation. Relatively few articles measure the effectiveness of CBL against specified learning outcomes. Moreover, few papers dealt with information systems, information security, or cybersecurity, reflecting the general scarcity of research into learning approaches in this field.

Once we had refined our data set to those papers which measured CBL against specified learning outcomes that are transferrable to

cybersecurity leadership, our analysis revealed the competencies listed in Appendix B. Using this set of relevant competencies, we have identified the high-level themes listed in Table 3.

We expand on each theme below.

4.2.1. Analysing failure scenarios

The central feature of CBL is the case itself. Regardless of the embodiment of CBL tested, learners are discussing or analysing a scenario; therefore, we might not be surprised to find results showing that CBL helps learners to better analyse scenarios [106–112]. This use of CBL may be unsurprising, but it is applicable beyond the classroom. Because cybersecurity leaders need to investigate incidents to prevent recurrence, they will apply these skills directly.

Indeed, it seems that analysing failure cases may have particular value. When comparing failure-based cases with cases describing success, Tawfik and Jonassen found that "students who accessed failure cases were able to better understand and construct arguments using alternative perspectives" [113, p. 397]. In a different study using a failure-based case, one participant speculated: "I don't know why our brain works that way, but it is so much easier to remember the bad stuff than it is to remember the good, so maybe I wouldn't have taken so much away from the case if everything had gone perfectly" [110, p. 2134]. These studies demonstrate that cases including failure are more effective at promoting knowledge retention and perspective-taking.

The value of analysing failure scenarios is not limited to memory and perspective-taking, however. Researchers also argue that analysing failures improves learners' ability to prepare for future incidents as well as their motivation to prepare. For example, Scalese et al. [111] studied CBL with pharmacy students and cases involving medication errors. Discussing their findings, they remarked that "through this experience, students have started to overcome the social stigma associated with making errors. In moving past blame, students focus on process analysis and changes to circumvent the errors that humans will inevitably make. Removing the shame of errors can facilitate error reporting and subsequent efforts toward quality improvement" [111, p. 462].

In other words, changing learners' attitude toward errors improved their ability to analyse scenarios and prevent future incidents. Scalese et al. [111] also noticed that learners' beliefs about error prevention changed; after CBL, learners were more likely to report that interprofessional collaboration would prevent future errors. Rong et al. [110], in summing up their study of veterinarian students and failure cases, claimed that "learning from failure cases may encourage students to strive for improvements" [110, p. 2140], indicating that CBL involving failure may improve not only the skill, but also the motivation to continuously improve.

Our review deliberately included multiple embodiments of CBL, regardless of whether a case *discussion* was involved. Nonetheless, our findings show that the act of discussing a case seems to help learners in a particular way. For example, Maslen and Hayes [107] explored the use of CBL with engineers and project managers discussing an aircraft collision case and observed that participants gained significant insight into the organisational causes of disasters. A process engineer in the study expressed a view that as an expert, he might fail to identify aircraft collision risks, especially if the forces and pressures were within officially allowable limits. On listening to a mechanical engineer with a different perspective, however, he updated his view on experts and risk identification: "I see if you don't have the experts, that's very real [the possibility that the risk would be overlooked]. I agree" [107, p. 315]. Participants began to conceptualise the collision through an abstract, organisational analysis lens, even citing the Swiss cheese model of accident causation [114]. In a separate study of nursing students, Yoo and Park [115] concluded that "analysis of cases involving miscommunication enhances problem-solving ability due to the transition from individually formulated solutions to systematic problem-solving that occurs during group discussions" [115, p. 170]. In both cases, the act of discussing failure cases seems to help learners prevent future incidents.

Taken together, these results show that CBL has the potential to help professionals analyse incidents and retain information about the conditions that led to failure. It also can help professionals look at a failure as an object of analysis rather than an incident requiring blame, improving their ability to prevent recurrence. Discussing cases may even help professionals prevent miscommunication and the kinds of incidents that follow from miscommunication.

Table 3
Key themes and selected references for CBL.

Theme (Capability supported by CBL)	Selected references
Analysing failure scenarios	Rong et al. [110]; Maslen & Hayes [107]
Solving complex, ill-structured problems	Gao et al. [121]; Tawfik & Jonassen [113]
Taking multiple perspectives	Drake [106]; Maslen & Hayes [107]
Making decisions under time pressure	North & Brookes [109]
Communicating, particularly adapting communication for different audiences	Dow et al. [130]; Noblitt et al. [132]

4.2.2. Solving complex, ill-structured problems and taking multiple perspectives

One of the strongest findings in our review was the power of CBL in helping learners learn to solve complex, ill-structured problems [113, 115–123]. Gao et al. [121] tested a combination of case-based and project-based techniques in an information system security subject and found that learners "learned and mastered many effective tools for systematic thinking and problem solving" [p. 8]. Given the design of their study, it would be difficult to estimate the extent to which their results were due to CBL or to project-based learning; however, other studies have investigated more "classic" CBL approaches. Choi and Lee [122] investigated the value of a CBL environment in learners' ill-structured problem-solving capacity. Across two studies with university students, they found that CBL aided students in developing multiple "sub-skills" for both identifying problems and generating solutions, including the ability to transfer problem-solving skills to new scenarios. Similarly, Tawfik and Jonassen [113] observed the value of learners accessing case libraries to solve problems and construct effective arguments.

CBL's power in problem solving may be related to its capacity to help learners inhabit multiple perspectives—that is, when learners are analysing a problem in the form of a narrative, they have the opportunity to examine the problem from multiple angles, which may help them form more robust solutions [106,122–125]. In both of Choi and Lee's [122] studies, learners' tendency to consider multiple perspectives during problem solving improved to a significant degree. Drake [106] poses a connection between perspective-taking and good-quality problem solving, noting that "considering these multiple stakeholder perspectives leads to a more complete analysis of the problem and a better overall recommendation" [106, p. 60]. Drake continues: "case studies provide opportunities for students to identify and consider these stakeholder interests" [106, p. 60].

Another, more recent study made this connection between perspective-taking and problem-solving specifically for organisational leadership, with participants gaining the understanding that any problem "could be understood in a wide variety of ways" [125, p. 201]. In this study, participants with experience in teaching studied cases with complex problems facing school principals, combining their own perspectives with the perspective of a school principal and those of practitioners in other schools. As a result, participants gained an understanding of their organisation as a complex system, recognised that other organisations may have more effective responses than their own, and realised that there are many ways to deal with one complex problem [125]. Although that study addressed CBL with teachers moving into educational leadership roles, we note a significant potential for crossover to other organisational leadership roles.

4.2.3. Making decisions under time pressure

Although studies like those of Gao et al. [121] and Shaked et al. [125] examined problem-solving across a longer duration, many others looked at professional problem solving and decision making in fields where decisions need to be made quickly "in the heat of the moment," such as medicine, nursing, and outdoor education. Kantar and Sailian [126] found that CBL improved nursing students' reflection in decision making, while Cherubini [127] found that after learning with CBL, pre-service teachers' "level of awareness was heightened in terms of the importance of factoring all considerations, other perspectives, and reflective practice into their decision-making" [127, p. 232]. According to these sources, improving perspective-taking and self-reflection ability has the potential to improve dynamic decision-making skills.

Cevik and Andre [128] found value for CBL in helping pre-service teachers make decisions about classroom management, and North and Brookes [109] found that CBL has potential for "leader decision-making" in outdoor education. They describe this style of decision making as a time-critical activity: "leader decision-making is particularly important in [outdoor education], because the leader may be the only person in a position to recognise, assess, and act on a safety-critical situation" [109, p. 195]. This collection of studies points to the potential value of CBL not only in complex problem solving generally, but also in time-critical problem solving and decision making.

4.2.4. Communicating

Another theme that surfaced repeatedly in the literature was the potential of CBL to improve communication skills. Communication skills were linked to persuasion [129], leadership [130,131], and problem-solving abilities [115], showing the many ways in which communication can aid professionals who need to collaborate and lead.

Most notably, Noblitt et al. [132] reported that CBL in helping learners to customise communications for various audiences. Learners in the control group had received a lecture and were then asked to present on one of a list of preselected peer-reviewed papers. The case-study group received a nearly identical lecture but were asked to present their analysis of data for a fictional case. Both groups were asked to present as though to a lay audience. Noblitt et al. noted that "although both groups of students were taught a series of techniques to integrate information into a coherent accessible message, only those students in the case method were able to successfully implement these techniques" [132, p. 31]. Although the researchers found that multiple dimensions of communication had improved, the most notable improvements seemed to be in the learners' ability to effectively integrate information and their ability to adapt their communication to the appropriate context. While many papers in our sample touched on the value of CBL for communication, Noblitt et al. [132] show that CBL has potential for professionals who need to adaptively communicate with different audiences.

4.2.5. A note on learner engagement

The literature exploring student and faculty experiences of CBL is nuanced and beyond the scope of this review. However, it is worth noting that 13 of the papers in our analysis reported a positive relationship between CBL and learner engagement. (The remaining papers did not discuss learner engagement.) Although learners' engagement is not a *direct* predictor of learning performance, it can affect multiple mediating factors, including attention, comprehension, effort, and persistence [133]. Furthermore, according to self-efficacy theory, learning engagement aids self-efficacy, which in turn can improve academic performance [134]. An exploration of learner perceptions of CBL warrants a separate review.

5. Synthesising the literature on competencies and CBL

5.1. The role of the cybersecurity leader: A balancing act

Our first research questions were:

RQ1. *What insights can be gained by applying a multidimensional competency lens to cybersecurity leadership?*

RQ2. *What is the current state of understanding of the competencies of cybersecurity leadership in extant literature?*

We listed the competencies found in the literature in Section 4, and to summarise, the role of the cybersecurity leader appears to be a balancing act. First, cybersecurity leaders must balance risk controls with innovation. Organisations engage these leaders to protect information resources, but a firm stance against all risks can inhibit innovation [11,96]. If the cybersecurity leader is unwilling to learn about the organisation's overall strategy, devote time and effort to collaboration, and accept some risks strategically, they may damage their relationship with the broader business, lose standing in the boardroom, and be cut out of decision-making processes [11].

Second, cybersecurity leaders must balance information protection with information sharing. At the operational level, cybersecurity needs to build barriers, but at the strategic level, cybersecurity needs to build bridges—with business leaders, the cybersecurity team, and other departments throughout the organisation [21,100]. Externally, they need to build information sharing networks with vendors, clients, regulators, and even competitors [86,94,97]. The fundamental requirement continues to be protecting information resources against threat actors and other risks, and herein lies the balancing act: Create too rigid a structure and the organisation may take risks without consulting you; create too relaxed a structure and you may leave the organisation exposed.

Finally, cybersecurity leaders must balance their efforts and resources between prevention mode and response mode [96]. Cybersecurity leaders in many industries are forced to spend a great deal of time on regulatory compliance [1], but they need to balance their resources between those obligations and scanning for unexpected threats that require innovative or improvised safeguards. Depending on the organisation's industry, location, clientele, or outsourcing strategy, overlooking the response mode entirely could have catastrophic consequences.

It is this balancing act that returns us to the concept of reflection-in-action posed by Schön [50]. If we use the definitions from Gonczi et al. [44], we can classify, for example, the strategy competencies: understanding the principles of strategy as a knowledge attribute, being able to develop a strategy as a skill, and approaching a situation with creativity and imaginative thinking as an attitude (see Table 4). However, we propose that the ability to find the "right" balance between the prevention paradigm and the response paradigm for an organisation in any given context does not lend itself to measurement as a typical skill. Selecting the balance between preventive tactics and response tactics requires a metaphorical conversation between the cybersecurity leader and the scenario. Schön refers to this "conversation" as *reflection in action* [50]; Eraut describes this same process as rapid or deliberative metacognition, depending on speed [43]. Eraut uses the term *control knowledge* for a generalised form of this process [43], which includes self-evaluation and strategic thinking. Indeed, due to its metacognitive nature, we propose to treat reflection as a "meta-competency" rather than as a competence category like knowledge [52].

Based on our findings, we argue that a cybersecurity leader needs to use control knowledge and metacognition to bring together their other competencies. In other words, the role needs a self-aware leader who can ask, "What paradigms suit this situation? What tactics did I use last time, and how well did they work? What information do I need to find out what threat actors might be doing, and how can I get it?" Cybersecurity leaders' competency needs are a blend of business leadership and

Table 4
Competencies of cybersecurity leadership with proposed "implied" competencies (select citations in square brackets).

Role	Knowledge	Skill	Attitude
Co-create cybersecurity with business leaders	• Understand ethical and legal dimensions [86] • *Implied:* Understand stakeholder engagement	• Facilitate ethical problem-solving [29] • Collaborate with external stakeholders [100] • Communicate with business leaders [24]	• Commitment to integrity [31] • Willingness to devote effort to collaboration [11] • *Implied:* Commitment to sharing information
Lead the cybersecurity team toward enhanced integration	• *Implied:* Understand people leadership	• Communicate with cybersecurity team [86] • Motivate cybersecurity team [95] • Develop talent pipeline [1]	• Accepting of errors [22] • *Implied:* Willingness to devote effort to communicating, motivating and mentoring
Direct cybersecurity strategy	• Understand the organisation's strategy [87] • *Implied:* Understand principles of business strategy • *Implied:* Understand budgeting • *Implied:* Understand resource management	• Develop and implement strategy [96] • Align cybersecurity strategy with organisational strategy [1] • Allocate resources effectively [89]	• Willingness to learn about the organisation's strategy [11] • Use creativity and imaginative thinking [87]
Direct cybersecurity governance and policy	• *Implied:* Understand the role of policies, plans and procedures • *Implied:* Understand which international standards and guidelines are relevant to cybersecurity policy development and planning • *Implied:* Understand the principles of governance	• Develop and implement cybersecurity policies [30] • Oversee plans and procedures [86] • Develop and implement a governance mechanism [30] • Drive continuous improvement [103]	• *Implied:* Willingness to devote effort to policies, plans, procedures and governance • *Implied:* Desire to continuously improve
Oversee the SETA program	• *Implied:* Understand training principles • *Implied:* Understand communication strategies	• Champion culture of awareness [22] • Oversee security training and development program [21]	• *Implied:* Commitment to creating a culture of awareness • *Implied:* Willingness to devote effort to implementing training program
Oversee cybersecurity risk management	• Understand technological controls [30] • Understand risk holistically [12] • Understand current threat landscape [104] • Understand cybersecurity standards and frameworks [30] • *Implied:* Understand relevant regulations • *Implied:* Understand adversarial thinking	• Identify and prioritise assets [11] • Identify and evaluate risks and threats [100] • Oversee technology security controls [104] • Facilitate physical security [9] • Manage compliance [97] • Monitor and evaluate controls [11] • Maintain organisational situational awareness [94] • Adapt to circumstances [87]	• Willingness to accept calculated risk [12] • *Implied:* Willingness to devote effort to managing organisational cybersecurity risk • *Implied:* Desire to continuously maintain situational awareness • *Implied:* Willingness to adapt
Lead incident response	• *Implied:* Understand strategy and adversarial thinking • *Implied:* Understand investigation and reporting	• Plan incident response strategy [89] • Lead response and recovery [98] • Lead incident investigations [97]	• *Implied:* Willingness to devote effort to planning incident response strategy • *Implied:* Capacity to respond during an emergency • *Implied:* Willingness to devote effort to investigations

combat leadership, continually advancing an organisation's goals while countering active adversaries. Furthermore, contrary to our expectations, we found that the cybersecurity leaders could use the prevention or response paradigm to approach any of their roles, meaning that they are constantly using metacognition to suit circumstances.

We contend that this metacognitive balancing act—including the balance between risk control and innovation, the tension between protecting and sharing different kinds of information, and particularly the balance between prevention and response paradigms—differentiates the cybersecurity leader from other, more established leadership roles, even older leadership roles in IT. Furthermore, we argue that to train a cybersecurity leader effectively, educators must help develop not only the competencies, but also the metacognition necessary to see past dominant paradigms and select the tactics necessary for each unique situation. Therefore, educating these leaders is a unique process.

5.2. How CBL supports cybersecurity leaders

To prepare cybersecurity leaders, educators need more than a list of necessary competencies—we need evidence-based approaches to teach these competencies. Our final research question was:

RQ3. *"To what extent is CBL applicable to the competencies of cyber leadership?"*

As expected, the two bodies of literature (cybersecurity leadership and CBL literature) did not name identical competencies, but we assert that many of CBL's strengths are transferrable to cybersecurity leadership. Early indications from the literature suggest that educators can use CBL to help learners build the skills shown at the left in Fig. 1, and that cybersecurity leaders need to perform the roles shown at the right. Based on our results, we have identified potential relationships in Fig. 1.

5.2.1. The value of adapting communications for partnership, leadership, and cybersecurity awareness

CBL enhances the ability to adapt communications for different audiences. Cybersecurity leaders with this skill can tailor communication for business leaders, external stakeholders, and the cybersecurity team. As discussed in Section 4.1, the ability to communicate relevant technical information to strategic leaders and communicate strategy information to technical personnel is necessary for cybersecurity leaders, who need to partner with the first stakeholder group and lead the other. By engaging regularly in the process of communication—whether in practice or in CBL scenarios—cybersecurity leaders also will gain

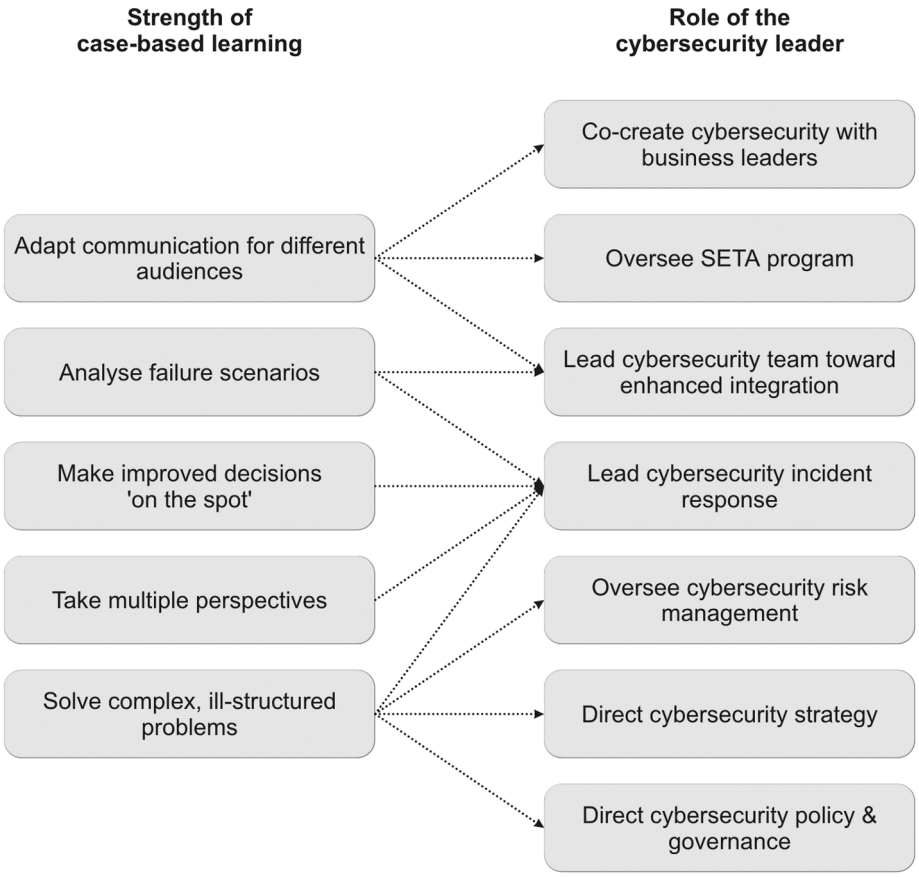


Fig. 1. Potential relationships between the skills built by CBL and the roles of cybersecurity leadership.
CBL's strengths include helping learners adapt communication, analyse failure scenarios, make time sensitive decisions and solve complex problems. These strengths may aid cyber leaders in partnering with business leaders, integrating teams, enhancing incident response, risk management, strategy, policy and governance.

knowledge about what information is relevant to different audiences, or knowledge about what communication style will motivate the cybersecurity team. Furthermore, as identified in Section 4.1.5, championing a culture of cybersecurity awareness requires a complex set of communication skills, requiring cyber leaders to adapt their communication to a more receptive style than they may be accustomed to. Finally, as Lyons and Bandura [64] noted, CBL supports self-regulated learning behaviours, which are closely linked to both self-efficacy and motivation. Therefore, in addition to its ability to improve adaptive communication skills, CBL's effect on self-regulated learning has the potential to enhance the motivation of cybersecurity leaders to communicating with a range of stakeholders. In sum, CBL has the ability to positively influence multiple competencies across the cybersecurity leader's roles of partnering with business leaders, overseeing the SETA program, and leading the cybersecurity team.

5.2.2. The value of analysing failure scenarios in leadership and incident response

Similarly, CBL's strengths in supporting the ability to analyse failure scenarios aids cybersecurity leaders in their role as a team leader. In this role, learning to remove the element of shame in failure analysis enables the cybersecurity leader to be accepting of human error [111] and to focus on creating a culture of shared responsibility for future improvement [22,89]. Well-developed skills in failure analysis also will aid cybersecurity leaders in investigating cybersecurity incidents, a key skill identified in the incident response role [94,97].

This strength of CBL in changing learners' attitudes toward failure showcases a noteworthy potential role for CBL in cyber leadership. Much of the research on CBL's effectiveness focused on skill development, but we speculate that CBL's true power lies in its potential to change attitudes. In the case of attitudes toward failure, cases destigmatise adverse incidents for learners by exposing them to narratives of previous incidents that happen to others and give learners practice in analysing adverse incidents without taxing emotions such as anxiety. Our findings strongly suggest that cyber leaders can improve their performance (paradoxically) by accepting the inevitability of errors and mistakes to empower employees, building a culture of openness and shared responsibility [21,22,89,100]. If CBL has the power to bring about the necessary attitudinal change, it has the potential to be a powerful asset for cybersecurity educators.

5.2.3. The value of perspective-taking, problem solving, and improved decision making to incident response

The ability to make improved decisions in tight timeframes and to solve complex, ill-structured problems will help cybersecurity leaders lead more effective responses to cybersecurity incidents, which are complex problems that occur under considerable time pressure. Moreover, a leader who can take multiple perspectives—including, for example, the perspective of attackers—is better equipped to respond to incidents strategically, and to communicate with regulators and the public thoughtfully. In this way, cybersecurity leaders who learn with CBL can gain a significant advantage in incident response.

5.2.4. Other uses of complex problem solving for cybersecurity leaders

Enriching the cybersecurity leader's problem-solving capacity also will aid them in developing the skills of designing a strategy, developing cybersecurity policies, and developing governance mechanisms, as well as a range of risk management activities, such as managing compliance

and evaluating threats. We also propose that by enhancing perspective-taking, CBL provides cybersecurity leaders with the metacognitive elements of problem-solving. When leaders trained to take other perspectives ask questions like "what mix of paradigms suits this situation?", they can "test" their responses against other perspectives, such as the perspectives of attackers, of regulators, of other leaders inside their organisation, and even of competitors, whose practices may be better suited to the situation at hand. As with the power of CBL in changing attitudes, we consider this capacity for improving metacognition to be an under-considered but powerful asset for cybersecurity educators.

6. Research agenda

We have identified opportunities for CBL to address the parts of a cybersecurity leader's role that are critical for their success but notoriously difficult to address with traditional teaching approaches. However, in its current state, the literature does not examine this relationship. Although a great deal of research has investigated the value of CBL, this research frequently did not identify the outcomes they intend learners to achieve, making identifying the relevant knowledge, skills, and attitudes impossible. Education researchers have focused only infrequently on cybersecurity practice, let alone on cybersecurity practice for post-professional audiences. Further research is needed to explore the value of CBL for cybersecurity leadership competencies, particularly for post-professional learners. To progress our understanding further, we propose the following research agenda.

6.1. Research directions for the role of the cybersecurity leader

Researchers interested in the role of the cybersecurity leader could supplement the results of our systematic review with exploratory literature reviews as well as empirical research. Delphi studies could prove particularly instructive in helping prioritise the extensive list of competencies identified in the literature, discovering which competencies are crucial, which are desirable but not essential, and which (if any) may be carried out chiefly by others in a large team.

Although the role itself is still relatively new and will continue to change, we anticipate that this program of research will develop a relatively stable picture of an "incident-centred" cybersecurity leader—that is, a cybersecurity leader capable of traversing both the relatively stable environment of commercial operations and the volatile environment of cyber warfare.

6.1.1. Research direction: Finding the missing competencies

We propose that the first research direction is to build a more complete picture of the requisite competencies. We believe that the list of competencies generated by the literature is sound but not yet complete, as generating a complete list of competencies has not been the focus of prior research. For example, interviews with industry experts could add detail to our understanding, while building expert consensus through a Delphi study could help predict emerging requirements. The role of the cybersecurity leader changes more quickly compared with other roles, and a consensus of industry experts can be a valuable way to add detail to our existing understanding while forecasting changes in the field.

Our collective understanding of the cybersecurity leader's competency needs will be enriched by reference to relevant cybersecurity management literature, including literature regarding governance, strategy, and the development of information security policies. These bodies of literature were excluded by our systematic search criteria; however, a literature review using a more exploratory approach would complement this review and provide valuable context for empirical studies such as the Delphi study mentioned above.

We anticipate two sets of findings. First, we expect that future research will reveal necessary competencies related to privacy and legal knowledge. Although privacy and law received passing mentions in our sample, they were not listed as explicitly required competencies. We expect that privacy, legal, and regulatory requirements are touched on only lightly because the role is new and because the need for these competencies is newer still. As the role matures, we anticipate that further research will reveal knowledge requirements for privacy and relevant law, as well as the skills and commitment (i.e., attitudes) needed to work within these bounds.

Second, we anticipate that such research will reveal additional knowledge and attitude requirements. We observed the literature tended to focus heavily on skill requirements rather than on knowledge or attitude requirements, although in some cases, a requirement for a skill logically implied a requirement for accompanying knowledge or attitudes. For example, the literature identified a need for cybersecurity leaders to be able to communicate with business leaders (a skill) and be willing to devote time and effort to collaboration (an attitude). Although not explicitly stated, understanding principles of communicating with different audiences (knowledge) is an essential accompaniment to the skill and the attitude. In Table 4, we list knowledge, skills, or attitudes not stated in the literature but rather implied. We anticipate that further research into the competencies needed by cybersecurity leaders will reveal that these "implied" competencies are necessary.

The tendency of literature to identify skills rather than attitudes or knowledge is not surprising. When employers design position descriptions and university educators design curricula, the desire for quantifiable outcomes encourages a focus on skills, which are often observable and measurable. Knowledge and attitudes are virtually impossible to measure directly; however, as illuminated by Gonczi et al. [44], by neglecting requisite knowledge and attitudes, employers and educators could be overlooking competencies crucial for success. Indeed, the professional bodies of many competency-focused professions—such as nursing, social work and K-12 education—explicitly differentiate knowledge, skills, and attitudes in their registration requirements.

We expect that metacognition will continue to play an important role as a "matrix competency," the means by which cybersecurity leaders deploy their other competencies.

In summary, our expected version of Table 4 will include privacy and legal requirements, as well as a much richer list of knowledge and attitudes. The updated list could form the basis for future professional development or executive education for this role. Although it will be difficult for educators to measure knowledge and attitudes, we expect some of them to emerge as very high-priority competencies.

6.1.2. Research direction: Prioritising competency requirements

A second research direction would be to find out which competencies have the most significant impact on the performance of a cybersecurity leader. Educational curricula are often shaped by experts' tacit awareness of which competencies to prioritise, but if educators do not examine those assumptions explicitly, they may take those priorities out of context. In this case, existing curricula for cybersecurity are most often aimed at pre-professional audiences (both undergraduate and post-graduate). We expect that research will show different priorities for cybersecurity graduates and cybersecurity leaders. In practice, this difference would mean that cybersecurity graduates who progress to leadership risk having crucial gaps in their expertise unless they obtain further targeted education or training. Conversely, in a packed curriculum, prioritising competencies would allow educators to prune out competencies that can be fulfilled by other members of an organisation.

Industry experts also would provide valuable insight for identifying the crucial competencies, although the act of ranking lends itself to a more quantitative (or at least mixed-methods) approach. A Delphi study would be instructive, particularly with maximal variation sampling. We do note that Haqaf and Koyuncu [30] conducted such a Delphi study; however, they recommended that Delphi studies be re-run every few years as the role changes, and the study did not focus on the metacognitive or attitudinal requirements revealed in the present review.

We believe that such research will reveal a need to emphasise

competencies related to information gathering and information sharing, particularly when augmented with adversarial thinking. Competencies related to information gathering include the skill and commitment to maintaining organisational situational awareness and the commitment to maintaining up-to-date knowledge about risks and threats, the technological landscape, and the organisation's strategy as well as its risk tolerance. Competencies related to information sharing include skill in and a commitment to communicating with business leaders, as well as with the cybersecurity team. Our findings suggest that information gathering and information sharing can extend to regulators, suppliers, and even competitors, with the ultimate aim of blocking cyber-threat actors [86,89,97,98,135]. Crucially, however, in the information-rich environment of 21st-century organisations, we contend that cybersecurity leaders must augment these competencies with adversarial thinking. To discern what information to gather, what information to analyse, what information to share, and what actions to take, cybersecurity leaders need to conceive of threat actors as adversaries. By conceiving of threat actors as adversaries—much like chess players or military leaders do—cybersecurity leaders can plan and prioritise their activities based on the strategy and tactics they expect their opponents to use.

6.1.3. Research direction: Investigating the framing of the cybersecurity leader's role

A third direction for further research would be to investigate the extent to which the current dominant framing of the cybersecurity leader matches the actual requirements. For researchers pursuing this line of enquiry, it is possible that multiple frames are limiting the way in which we conceptualise the role of the cybersecurity leader. A frame or paradigm is valuable for providing cohesion to our concept of the role, but to gather a comprehensive set of competencies, we need to assess the frame itself for what it excludes. It would be worthwhile to identify which paradigms frame the role of a cybersecurity leader and assess their suitability.

To research the difference between the perceived and actual needs of the role, it would be valuable to combine perception data with observational data. For example, a researcher with access to an incident management database could use data from logs and emails to explore the relationships between a leader's decisions and the events in a given incident. Follow-up interviews could explore how the leader perceived their role before, during, and after the incident and compare with the observational data. The lens of metacognition would be valuable for interviews with leaders. How do they decide which situations or actions require prevention mode thinking? On what basis do they decide to deploy response mode?

Our findings indicate that one paradigm—prevention mode—appears to dominate in both industry and research conceptualisations of the role. We also identified that another paradigm—response mode—contributes dimensions to many of the cybersecurity leader competencies. Based on our findings, we speculate that educators and some industry bodies will perceive the role more frequently through the prevention lens, but that experienced cybersecurity leaders will express more awareness of both paradigms. We also suspect that research into the framing of the role will find that in practice, most competencies have dimensions in both the prevention and response modes. A few competencies, such as developing a strategy, may exist outside those two modes but still require a leader to select tactics from both modes. Finally, we anticipate that although both modes are essential, in the future cybersecurity leaders may need to focus more heavily on the "response mode" dimensions of their competencies owing to the increase in sophisticated attacks.

6.1.4. Research direction: Exploring meta-competencies

In this paper, we have deliberately constrained our competency lens to knowledge, skills, attitudes and roles, conceptualising reflection as a surrounding matrix – as the means by which one employs other competencies. This restriction in the frame allows us to propose a set of competencies that will, with empirical validation, be practical to use for educators and cybersecurity leadership recruiters alike. However, for more theoretical research aims, a wealth of meta-competencies waits to be explored.

As discussed in Section 2, in situating our dimensions of competence, we have drawn on Cheetham and Chivers [52]. In their model, reflection is termed a "super meta" competency, surrounding both functional competencies like knowledge and "meta competencies" such as problem solving [52, p. 275]. A fourth research direction would be to investigate meta-competencies (e.g., problem solving, strategic thinking, and visioning) as they are applied to cybersecurity leadership specifically.

As with "finding the missing competencies" above, this exploration would suit qualitative methods such as in-depth interviews with existing practitioners. The more interesting question for this research direction would be the choice of analysis method; for example, a reflexive thematic analysis conducted by an experienced researcher and practitioner has the potential to paint a rich portrait of the profession.

We expect that this exploration would find a range of general meta-competencies that apply to cybersecurity leadership as a profession, along with meta-competencies that could be applied to specific roles cyber leaders perform. For example, strategic thinking will likely emerge as a meta-competency necessary for the professional, but strategic thinking also will have particular embodiments in leading incident response (selecting tactics, etc.). Exploring strategic thinking as a meta-competency may be particularly fruitful for cybersecurity leadership, because components such as system thinking, visionary thinking, creativity, and synthetic thinking [136,137] may have different facets in prevention mode and response mode. We do not expect meta-competencies to fit neatly in the competency framework proposed in Table 4; however, a thematic analysis of these meta-competencies has the potential to shape educational curricula at the program level by identifying and prioritising necessary graduate attributes. Our research questions regarding the competencies of cybersecurity leadership are summarised in Table 5.

6.2. Research directions for CBL

Targeted empirical research is needed to explore the value of CBL for cybersecurity leaders. We expect that CBL has value for competencies beyond what we have identified in this review. Although numerous studies have investigated the value of CBL, many did not identify the intended learning outcomes, making it impossible to identify the relevant knowledge, skills, and attitudes. Education researchers also focus only infrequently on cybersecurity practice, let alone on cybersecurity practice for post-professional audiences. Further research is needed to validate the value of CBL for cybersecurity leadership competencies, particularly for post-professional audiences.

We recommend a suite of teaching studies to explore the utility of CBL in educating cyber-resilient leaders. Following such a program of research, we hope to find an educational design that builds cyber-resilient leaders, leaders who can simultaneously collaborate with the

Table 5
Research questions (RQs) for cybersecurity leadership (CL).

CL RQ1	What knowledge, skills and attitudes do cybersecurity leaders need to fulfil their roles?
CL RQ2	What methods can educators use to help cybersecurity leaders gain cyber leadership competencies?
CL RQ3	Which competencies are the most critical for a cybersecurity leader?
CL RQ4	What paradigms best frame the cybersecurity leader's role?
CL RQ5	What are the characteristics of cyber leadership competencies in response mode?
CL RQ6	What meta-competencies do cyber leaders deploy in their role?

business in its day-to-day operations and lead a team capable of detecting and responding to the many cyber threats to come.

6.2.1. Research direction: Exploring the use of CBL in new, ill-defined roles

We propose that one research direction for CBL is to explore its value in a range of new and ill-defined professions. Educators have long faced the challenge of preparing professional learners for evolving professions, especially in technology-based roles; however, it is likely that during this century, professional roles in general will begin to evolve more rapidly, and that professions will emerge that do not yet exist. Educators now need learning approaches that prepare learners for newly emerged, ill-defined, and rapidly changing roles—and not just in cybersecurity. This style of education has a fundamental difference from others: when preparing professionals for a new, poorly defined role, educators will not have decades of research, theory, and practice data to weave into a set of principles. Rather, they will need teaching and learning approaches that quickly capture what is happening in the industry.

CBL offers a particular strength in this regard, as cases can be amalgamated from real-life scenarios and made available to learners relatively quickly. Therefore, it would be worthwhile to investigate the utility of CBL in preparing professionals for roles like that of the cybersecurity leader—recently emerged and rapidly changing.

Studies in this area could narrow the question and examine the utility of a case-based reasoning approach: providing post-professional learners with a problem to solve and a library of recent cases as a study tool [61,67]. Researchers could investigate whether case-based reasoning enables cybersecurity leaders to improve their problem-solving, particularly with reference to new threats. Researchers also could design follow-up questions to determine whether post-professional learners begin to extrapolate their own principles using case-based reasoning.

It also takes time for researchers and practitioners to build up a nuanced picture of a new role; diverse perspectives from various industries and contexts take time to gather. We also anticipate that CBL could provide unique value here, allowing learners to study cases from a broad range of contexts and therefore experience the variety close to first-hand.

6.2.2. Research direction: Investigating CBL's strengths under time pressure

A second direction for researchers would be to investigate CBL's suitability for decision making in situations when speed is crucial, such as cybersecurity incidents, medicine, emergencies, piloting planes, or even coaching a sport. There are hints in the literature that CBL can help professionals improve their decision making under time pressure. The studies in our sample did not set out explicitly to evaluate the utility of CBL in time-critical decision making; however, in reviewing the impact of CBL on reflection and decision making in time-critical contexts—such as such as nursing [126] and outdoor education [109]—we consider that the connection warrants empirical study. Indeed, it would be valuable to investigate the utility of CBL in aiding reflection-in-action [50] as a component of real-time decision making.

Multiple research designs could investigate this connection. For example, a randomised-controlled trial could assign post-professional learners to one of two groups, with one group receiving lecture-based instruction on the principles of cybersecurity incident response and the other group participating in CBL sessions. Following the intervention, both groups could participate in incident drills for the same pre-designed scenario. More straightforward preintervention and postintervention tests are also possible, as long as they are designed to simulate decision making in a crisis.

We expect that such studies will find learners make better decisions in short timeframes when they have experienced CBL. As long as learners are required to test themselves in some way (e.g., through problem solving), learning with cases provides the kind of spaced, interleaved practice that helps professionals make effective decisions quickly in high-pressure situations [65]. Other problem-based approaches, such as drills and simulations, also provide this kind of practice; however, CBL allows learners to achieve comparable outcomes in less time [138]. Results from such studies have the potential to be valuable not only for cybersecurity, but also for a range of professions that require real-time decision-making.

6.2.3. Research direction: Exploring the use of CBL in response mode

Our findings reveal the potential for cybersecurity leadership competencies to have dimensions in prevention mode and response mode. We anticipate that CBL will be particularly suited to the dimensions of the cybersecurity leader's role in response mode. In response mode, leaders assume that attackers deliberately aim to "take defenders by surprise" and "focus on the area in which defenders are poorly prepared" [96, p. 142]. For leaders to manage risk under this paradigm, they need to practise taking the perspective of attackers, a skill that our findings suggest CBL is well suited to building.

Further, in response mode, cybersecurity leaders assume that threats are unpredictable and risks are transient, and thus they need to build the organisation's capacity to gather and share relevant intelligence. In a modern, information-rich environment, competencies related to intelligence gathering and intelligence sharing require the ability to sort "signal" from "noise"—that is, to discern relevant intelligence from irrelevant information. CBL is uniquely well placed to simulate this challenge; case writers can build bespoke scenarios, dense with seductive detail, to enable learners to practise identifying the relevant information. Learners can undertake interleaved practice when learning with cases, weaving practice at identifying relevant information in with practice in time-sensitive decision making and practice with other skills, closely simulating industry experience. When combined with CBL's affordance for learners to take an adversary's perspective, these traits make for a powerful learning experience.

We propose a third research direction devoted to studying CBL's potential in response mode. Researchers interested in CBL and response mode could explore these hypotheses through teaching studies. A traditional experimental design with a CBL group and a lecture-based control group could be illuminating; however, it might be more revealing to use design science: undertake repeated trials with single groups undergoing CBL and refine the embodiment of CBL in each round. Thus, earlier trials become a control-style comparison for later trials, and the research design lends itself to finding the most effective educational design.

6.2.4. Research direction: Finding the best educational design

The answer to our final question—is CBL suited to educate cybersecurity leaders?—will depend to some extent on the quality and relevance of the cases, the teaching techniques, the setting, and the timeframe. Thus, it bears investigating that question together with another: what CBL design is the most effective at educating cybersecurity leaders?

This research direction also lends itself to a design-science paradigm, a series of teaching studies with iterative refinements to the educational design. Triangulation of different data sources may be valuable in this case as well; pre-tests and post-tests could be supplemented with observation of the classroom (or analysis of online discussion board discourse), as well as either interviews or a focus group to explore learners' experiences. In an ideal scenario, post-tests could be supplemented with follow-up tests a week or a month following the teaching study to see what has been retained.

As discussed in the Introduction, previous research does point to certain CBL designs as being highly effective. Presenting the case prior to presenting the relevant theory, then asking learners to collaboratively solve a problem based on the case has potential [61–63]. Thoughtful use of multimedia also can enhance the experience [63]. Researchers interested in the most effective educational designs of CBL could start with a design along these lines.

The features of the case are likely to be as important as the features of

the teaching sequence. Our findings from this review suggest potential for cases that involve failure. It could seem challenging to write a case involving failure and then ask learners to problem solve, but prior failures could form part of the background information of a case-based scenario – part of the problem that the learners need to solve. It could also be fruitful to ask learners to review several cases involving failure prior to presenting a new case for problem-solving practice. In this way, the learners simultaneously use CBL to practise case-based reasoning as well as double-loop learning. Researchers may wish to start their first trial with cases involving failure.

Significantly, such research can point to generalisable findings about effective embodiments of CBL for a range of fields. Our research questions regarding the utility of CBL are summarised in Table 6.

7. Discussion

The primary contribution of this article is its proposals for further work, embodied in the research agenda. This section describes the article's limitations and contributions.

7.1. Contributions to literature

This article contributes to the literature by framing a major current problem in cybersecurity practice: the gaps in understanding the cybersecurity leader's role and how to educate them. This article also contributes two research agendas to the literature: one to explore the true nature of the cybersecurity leader's role, and a second to investigate the power of CBL in fostering cybersecurity leaders' competence. These two agendas contribute to knowledge by providing researchers with future directions [139].

Cybersecurity leadership (or "cyber leadership") is an emerging area that is critical to cyber defence in the modern era, and yet not much is known about the competence of cyber leaders in this role, and even less is known about how to educate future leaders. Previous literature has examined the technical skills of cybersecurity management [e.g., 30], but this article has comprehensively synthesised what is currently known about the role of cyber leaders and identified likely gaps in our collective understanding. By applying a competence lens [44] to the existing literature on cyber leaders, we have identified a collective fixation on skills to the exclusion of other facets of competence, which has left gaps in our shared understanding of knowledge and attitude competencies. We also have identified a bias toward risk management, which necessarily reduces the focus available to examine capabilities in strategy or incident response. In that way, this literature review has synthesised previous literature, provided new insights, and identified gaps and biases in the existing corpus [139].

Our proposed research agenda into the role of the cyber leader enables researchers to explore more facets of cyber leadership. We propose a comprehensive investigation into the cyber leader's many roles, including a close examination of capabilities in incident response, strategy, and integration with the organisation through partnership with business leaders, SETA, and leadership of the cybersecurity team—that is, the competencies beyond management of technological risks. Our agenda enables researchers to enquire into the attitudes, knowledge, and meta-competencies that complement the necessary skills and to explore how the competencies might differ in response mode. Thus, this work enables researchers to improve organisational practice in ways not previously possible. Because of this unique combination of prevention-mode and response-mode competencies, this paper proposes that educating cybersecurity leaders is a unique task.

Table 6
Research questions (RQs) for the utility of CBL.

CBL RQ1	To what extent is CBL suited to developing a cybersecurity leader?
CBL RQ2	To what extent is CBL valuable for making decisions and solving problems under time pressure?
CBL RQ3	Is CBL particularly valuable for 'information-warfare' mode?
CBL RQ4	Is CBL particularly useful for new, ill-defined roles?
CBL RQ5	How can case based learning be used to improve cybersecurity leadership?
CBL RQ6	What are the particular strengths of analysing failure-based cases?

7.2. Contributions to practice

This article identifies the limitations of traditional methods of cybersecurity leadership education and proposes CBL as a candidate for improving the competence of cyber leaders. To keep up with modern cyber threats, cyber leaders will need to become masterful at adaptation, growing and adapting themselves while also adapting strategies in the organisations they lead. We find that CBL holds the potential to help cyber leaders develop the ill-structured and time-pressured problem solving, decision making, and communication that will be necessary to thwart threat actors and respond to attacks. Educators can use these findings to expand their educational techniques, experimenting with incorporating cases—particularly failure-based cases with a variety of perspectives —into their teaching.

This article also contributes a preliminary competency framework, which practitioners can use for recruitment and educators can use for curriculum design. While the competencies in Table 4 await empirical validation, as set out in our research agenda, they are representative of the state of knowledge in the published literature and thus still provide value to recruiters and educators. In addition, both recruiters and educators can use awareness of the biases in the literature—the bias toward prevention mode as well as the bias toward skills—to correct for possible blind spots in position descriptions and curricula, respectively.

7.3. Limitations and outlook for future research

This systematic review is limited by the number of databases searched. Moreover, we did not review literature in languages other than English. We do not claim that this search identified every relevant article; however, we do contend that the results provided a sufficient representative sample for analysis. Further research exploring the value of CBL for cybersecurity leadership in education would benefit from a more exploratory approach to reviewing the literature, as well as from empirical exploration.

This review is also limited in scope. Because the focus of this paper is so close to the body of scholarship on cybersecurity/ information security management more broadly, it would be possible to read this paper as a contribution to the broad field of organisational practice in information security. However, our research question and search criteria focused on research conducted with the cybersecurity leader in mind. There is much research on cybersecurity management in general that contributes to context but does not mention the cybersecurity leader, and these sources have not been consulted. Therefore, it is necessary to limit inferences from this paper to the role of the cybersecurity leader itself.

Third, this review is limited by the number of coders. The primary author coded all papers, discussing and validating the codes with the additional authors. Because the final codes were reached by discussion, it is not possible to calculate inter-rater reliability on the content analysis component.

Finally, as with all literature reviews, this review provides an analysis of the understanding in the literature alone. In other words, it is likely that empirical investigation would yield a greater understanding of the competencies required by cybersecurity leaders and a more targeted understanding of the utility of CBL for cybersecurity leadership education. We submit that the proposed research programs described in Section 6 can overcome this limitation by adding empirical data.

8. Conclusion

In this article, we have reviewed the research on cybersecurity leaders and proposed a preliminary matrix of competencies required. We observed that affective/conative competencies ("attitudes") have a strong impact on overall competence and are missing from existing frameworks. We then reviewed research on CBL, finding that although while existing research hints at the value CBL for cybersecurity leadership education, neither information systems research nor education research has examined this relationship explicitly. We have described the cybersecurity leader's role as a balancing act, balancing risk mitigation with risk-taking, information protection with information sharing, and prevention mode with response mode. This balancing act requires not only a range of knowledge, skills, and attitudes, but also a strong metacognitive ability. Based on our analysis of the literature, we propose that CBL has significant potential to develop this metacognitive ability as well as the conative/affective competencies. Our research agenda calls for further exploration of the cybersecurity leader's role, and further examination of CBL's potential. This burgeoning area of research can contribute significantly to educating cybersecurity leaders and keeping modern organisations safe.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CRediT authorship contribution statement

Ashley Anderson: Writing – review & editing, Writing – original draft, Visualization, Validation, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Atif Ahmad:** Writing – review & editing, Validation, Supervision, Methodology, Conceptualization. **Shanton Chang:** Writing – review & editing, Validation, Supervision, Conceptualization.

Declaration of competing interest

The authors declare that they have no conflicts of interest.

Acknowledgements

We are grateful for the constructive comments of the editor and reviewers on the earlier versions of this paper.

Appendix A. The competencies of a cybersecurity leader

Roles	Competencies: Knowledge (K), Skills (S) and Attitudes (A)
Partner with business leaders	• **Understand ethical and legal dimensions (K)** [86,88] • **Communicate with business leaders (S)** [1,9,11,12,21,22,24,29,30,86–95,97,100,102–105] • **Collaborate with external stakeholders (S)** [1,9,29,86,89,90,94,96,97,100,101,103,105] • **Facilitate ethical problem-solving (S)** [29] • **Willingness to devote effort to collaboration (A)** [1,11,21,89,100] • **Integrity (A)** [24,31]
Lead the cybersecurity team	• **Communicate with cybersecurity team (S)** [1,86–89,91,95,103] • **Motivate team (S)** [95,99,105] • **Develop talent pipeline (S)** [1,11,90,95,105] • **Accepting of errors (A)** [22,93,95]
Direct cybersecurity strategy	• **Understand the organisation's strategy (S)** [9,11,12,86–92,103,104] • **Develop and implement strategy (S)** [1,30,87,91,92,96,101,103] • **Align cybersecurity strategy with organisation's strategy (S)** [1,9,11,30,87,91,100,101,103–105] • **Allocate resources effectively (S)** [9,11,86–90,92,94,105] • **Willingness to learn about the organisation's strategy (A)** [11] • **Use creativity and imaginative thinking (A)** [87]
Lead cybersecurity policy and governance	• **Develop and implement cybersecurity policies (S)** [9,11,29,30,90–92,94,97–99,104,105,135] • **Oversee plans and procedures (S)** [9,86,87,91–93,97,98,100,104] • **Develop and implement a governance mechanism (S)** [11,30,86,90–93,97,98,100,103] • **Drive continuous improvement (S)** [11,87,91,103]
Oversee the SETA program	• **Champion culture of awareness (S)** [9,11,21,22,87,89–91,93,94,100,103,104,135] • **Oversee security training and development program (S)** [9,21,29,86,90,91,99,100,105,135]
Oversee cybersecurity risk management	• **Understand technological controls (K)** [29,30,91–93,102,103,135] • **Understand risk holistically (K)** [11,12,30,90,91,103] • **Understand current threat landscape (K)** [1,11,29,87,90,94,104,135] • **Understand cybersecurity standards and frameworks (K)** [30,86] • **Identify and prioritise assets (S)** [11,89,91,100,103,104] • **Identify and evaluate risks and threats (S)** [9,11,86,89,92,93,100,135] • **Oversee technology security controls (S)** [9,11,86,89,93,94,97,98,100,101,103,104,135] • **Facilitate physical security (S)** [9,88] • **Manage compliance with legislation,regulations and standards (S)** [1,11,22,86,90,91,94,97,98,101,103,104,135] • **Monitor and evaluate controls (S)** [1,9,11,30,86,90–92,97,103,105,135] • **Maintain organisational situational awareness (S)** [11,86,87,89,90,94,96,98,100] • **Adapt to circumstances (S)** [1,12,86,87,89,94] • **Willingness to accept calculated risk (A)** [11,12,91,92,97,98,103]
Lead incident response	• **Plan incident response strategy (S)** [9,12,29,89,96,97] • **Lead response and recovery (S)** [9,12,29,86,90,96,98,105,135] • **Lead incident investigations (S)** [29,94,96–98,101,135]

Appendix B. The utility of CBL

Table B.1 Competencies supported by CBL in our sample

Competency supported by CBL	Sources
Analyse failure scenarios	[107,109–112,115]
Reflect	[107,124,126,127,130]
Solve complex, ill-structured problems	[82,106,107,110,112,113,115–122,125,129]
Take multiple perspectives	[106,107,111,122–125,127]
Make decisions in tight timeframes	[109,126,128]
Communicate	[82,106,115,129,130,132,138]
Adapt communication	[115,130,132]
Identify risks for future scenarios	[107,109]
Understand complex systems	[112,125,129]
Understand the human nature of errors	[110,111]
Identify and evaluate the outcomes of business strategies	[108]
Lead teams	[131]
Put plans into practice	[129]

Appendix C. Example from codebook

Key:
(K) – Knowledge
(S) – Skills
(A) – Attitudes
(R) – Roles

Table C.1 Example from codebook

Example extract	Code	Theme
"*Fully understand the business mission, vision, values, and strategic plan.*" ([9], p. 275)	Understand the organisation's strategy (K)	Direct cybersecurity strategy (R)
"*Defines and implements information and cyber security strategies.*" ([92], p. 6)	Develop and implement cybersecurity strategy (S)	
"*Ensuring cyber-strategy is aligned to business strategy; otherwise, there is the possibility of viewing the initiative as an IT project. As one participant (P1) noted 'keeping cyber-strategy aligned to the organization, its critical to start off with business first and build cyber into organizational strategy. Otherwise you could end up taking an overly technical view of the whole thing and suddenly holes appear in your security analysis because important things are not protected and aligned to the business.'* ([100], p. 3760)	Align cybersecurity strategy to the organisational strategy (S)	
"*This paper therefore argues that CISOs must be able to implement an actionable plan (translated from a clear vision and direction) within the organizational context using efficient and effective allocation of resources.*" ([87], p. 13)	Allocate resources effectively (S)	
"*CISOs and their teams that do not make an effort to understand and partner with the business leaders often become roadblocks to the business achieving its objectives.*" ([11], p. 76)	Willingness to learn about the organisation's strategy (A)	
"*This paper therefore posits that CISOs must be able to draw on creative, imaginative, abstract, lateral thinking approaches towards developing novel security strategies to address evolving threat landscape in the face of uncertainty.*" ([87], p. 12)	Use creativity and imaginative thinking (A)	

References

[1] D. Burg, A. Hussein, R. Watson, Cybersecurity: How do You Rise Above the Waves of a Perfect storm? Ernst & Young, 2021.
[2] D. Ehrlicher, Council post: The evolution of cybersecurity In 2021, Forbes (2020). https://www.forbes.com/sites/forbestechcouncil/2021/03/05/the-evolution-of-cybersecurity-in-2021/.
[3] Cybersecurity & Infrastructure Security Agency (CISA). (2021, April 15). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.
[4] D. Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story of The Solarwinds Hack, April 16, NPR, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
[5] S. Morgan, 2022 Official Cybercrime Report, Cybersecurity Ventures | eSentire, 2022. https://www.esentire.com/resources/library/2022-official-cybercrime-report.
[6] C. Dameff, J. Tully, T.C. Chan, E.M. Castillo, S. Savage, P. Maysent, T. M. Hemmen, B.J. Clay, C.A. Longhurst, Ransomware attack associated with disruptions at adjacent emergency departments in the US, JAMa Netw. Open. 6 (5) (2023), https://doi.org/10.1001/jamanetworkopen.2023.12270.
[7] A. Ahmad, S. Maynard, R. Baskerville, Editorial: Cybersecurity incident response in organizations, Comput. Secur. 112 (2022), https://doi.org/10.1016/j.cose.2021.102530.
[8] A. Ahmad, K.C. Desouza, S.B. Maynard, H. Naseer, R.L. Baskerville, How integration of cyber security management and incident response enables organizational learning, J. Assoc. Inf. Sci. Tech. 71 (8) (2020) 939–953, https://doi.org/10.1002/asi.24311.
[9] W.M. Kappers, N. Harrell, From degree to chief information security officer (CISO): A framework for consideration, J. Appl. Econ. Bus. Stud. 22 (11) (2020) 260–288.
[10] M. Lowry, Z. Sahin, A. Vance, Taking a Seat at the Table: The Quest for CISO Legitimacy, in: ICIS 2022 Proceedings, 2022. https://aisel.aisnet.org/icis2022/security/security/14.
[11] T. Aguas, K. Kark, M. François, The New CISO: Leading the Strategic Security Organization, Deloitte Insights, 2016. https://www2.deloitte.com/content/www/us/en/insights/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html.
[12] A. Alexander, J. Cummings, The rise of the chief information security officer, People & Strategy 39 (1) (2016) 10–14.
[13] US FTC, Standards For Safeguarding Customer Information, December 9, Federal Register, 2021, https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information.
[14] J. Hallett, R. Larson, A. Rashid, Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks, in: Proceedings of the 27th USENIX Security Symposium 9, 2018. https://www.usenix.org/conference/ase18/presentation/hallett.

[15] K.J. Knapp, C. Maurer, M. Plachkinova, Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance, J. Inf. Syst. Educ. 28 (2) (2017) 101. https://jise.org/Volume28/n2/JISEv28n2p101.html.

[16] University of Queensland, *Leadership—Master of Cyber Security—Study—The University of Queensland* [Website], The University of Queensland, 2023. Study, https://study.uq.edu.au/study-options/programs/master-cyber-security-5257/leadership-ldshpx5257.

[17] (ISC)^2. (2023). CISSP - Certified Information Systems Security Professional. https://www.isc2.org/Certifications/CISSP.

[18] K. Cabaj, D. Domingos, Z. Kotulski, A. Respício, Cybersecurity education: Evolution of the discipline and analysis of master programs, Comput. Secur. 75 (2018) 24–35, https://doi.org/10.1016/j.cose.2018.01.015.

[19] S.C. Yang, A curriculum model for cybersecurity master's program: A survey of AACSB-accredited business schools in the United States, J. Educ. Bus. 94 (8) (2019) 520–530, https://doi.org/10.1080/08832323.2019.1590296.

[20] ISACA, CISM Certification | Certified Information Security Manager, ISACA, 2023. https://www.isaca.org/credentialing/cism.

[21] J. Hielscher, U. Menges, S. Parkin, A. Kluge, M.A. Sasse, Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": the CISO View of Human-Centred Security, in: Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher.

[22] D. Ashenden, A. Sasse, CISOs and organisational culture: Their own worst enemy? Comput. Secur. 39 (2013) 396–405, https://doi.org/10.1016/j.cose.2013.09.004.

[23] J. Da Silva, Cyber security and the leviathan, Comput. Secur. 116 (2022) 102674, https://doi.org/10.1016/j.cose.2022.102674.

[24] J. Da Silva, R Jensen, Cyber security is a dark art: The CISO as soothsayer, Proc. ACM. Hum. Comput. Interact. 6 (CSCW2) (2022) 1–31, https://doi.org/10.1145/3555090.

[25] M. Aiello, S. Thompson, M. Randria, C. Reventlow, G. Shaul, A. Vaughan, 2022 Global Chief Information Security Officer (CISO) Survey, Heidrick & Struggles, 2022. https://www.heidrick.com/en/insights/compensation-trends/2022-global-chief-information-security-officer-ciso-survey.

[26] R. Norton, DACUM Handbook, 2nd ed., Ohio State University, 1997. https://files.eric.ed.gov/fulltext/ED401483.pdf.

[27] M. Mulder, J. Winterton, Chapter 1: introduction, in: M. Mulder (Ed.), Competence-based Vocational and Professional Education: Bridging the Worlds of Work and Education, Springer International Publishing, 2017, pp. 1–43, https://doi.org/10.1007/978-3-319-41713-4_1.

[28] S. Blömeke, J.-E. Gustafsson, R.J. Shavelson, Beyond dichotomies, Z. Psychol. 223 (1) (2015) 3–13, https://doi.org/10.1027/2151-2604/a000194.

[29] D. Whitten, The chief information security officer: An analysis of the skills required for success, J. Comput. Inf. Syst. 48 (3) (2008) 15–19. https://www.tandfonline.com/doi/abs/10.1080/08874417.2008.11646017.

[30] H. Haqaf, M. Koyuncu, Understanding key skills for information security managers: SSIS, Int. J. Inf. Manag. 43 (2018) 165, https://doi.org/10.1016/j.ijinfomgt.2018.07.013.

[31] R. Smit, J.M.J. Hagedoorn, Y. van, P. Versteeg, P. Ravesteijn, The Soft Skills Business Demands of the Chief Information Security Officer, in: Journal of International Technology and Information Management, Suppl. Special Edition – Conference Proceedings of IIMA 2021 30, 2021, pp. 41–61. https://www.proquest.com/docview/2619484533.

[32] R. Trilling, Creating a New Academic Discipline: cybersecurity Management Education, in: Proceedings of the 19th Annual SIG Conference on Information Technology Education, 2018, pp. 78–83, https://doi.org/10.1145/3241815.3241860.

[33] D. Garvin, Teaching executives and teaching mbas: Reflections on the case method, Acad. Manag. Learn. Educ. 6 (3) (2007) 364–374, https://doi.org/10.5465/amle.2007.26361626.

[34] H. Rosenbaum, M. Shermis, Making a Case for Scenario-Based Learning in IS and Executive Education, in: AMCIS 2010 Proceedings, 2010. https://aisel.aisnet.org/amcis2010/530.

[35] A. Ahmad, S.B. Maynard, S. Motahhir, M. Alshaikh, Teaching Information Security Management Using an Incident of Intellectual Property Leakage, in: ACIS 2020 Proceedings, 2020, pp. 1–11. https://aisel.aisnet.org/acis2020/36.

[36] A. Ahmad, S. Maynard, S. Motahhir, Teaching Information Security Management in Postgraduate Tertiary Education: the Case of Horizon Automotive Industries, in: ACIS 2020 Proceedings, 2020. https://aisel.aisnet.org/acis2020/54.

[37] A. Ahmad, S.B. Maynard, S. Motahhir, A. Anderson, Case-based learning in the management practice of information security: an innovative pedagogical instrument, Pers. Ubiquitous Comput. (2021), https://doi.org/10.1007/s00779-021-01561-0.

[38] W. Cram, J D'Arcy, Teaching information security in business schools: Current practices and a proposed direction for the future, Commun. Assoc. Inf. Syst. 39 (1) (2016), https://doi.org/10.17705/1CAIS.03903.

[39] J. vom Brocke, A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, A. Cleven, Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research, Commun. Assoc. Inf. Syst. 37 (1) (2015), https://doi.org/10.17705/1CAIS.03709.

[40] M. Salman, S.A. Ganie, I. Saleem, The concept of competence: A thematic review and discussion, Eur. J. Train. Dev. 44 (6/7) (2020) 717–742, https://doi.org/10.1108/EJTD-10-2019-0171.

[41] M. Mulder, Conceptions of Professional Competence, in: S. Billett, C. Harteis, H. Gruber (Eds.), International Handbook of Research in Professional and Practice-based Learning, Springer Netherlands, 2014, pp. 107–137, https://doi.org/10.1007/978-94-017-8902-8_5.

[42] P. Hager, Chapter 10: the Integrated View on Competence, in: M. Mulder (Ed.), Competence-based Vocational and Professional Education: Bridging the Worlds of Work and Education, Springer International Publishing, 2017, pp. 203–228, https://doi.org/10.1007/978-3-319-41713-4_10.

[43] M. Eraut, Developing Professional Knowledge and Competence, Taylor & Francis Group, 1994.

[44] A. Gonczi, P. Hager, L. Oliver, Establishing Competency-Based Standards in the Professions, Department of Employment, Education and Training, 1990. https://www.voced.edu.au/content/ngv%3A29478.

[45] C. Harteis, Chapter 45: intuition as Crucial Component of Professional Competence: its Relevance for Competence-based Vocational and Professional Education and Training, in: M. Mulder (Ed.), Competence-based Vocational and Professional Education: Bridging the Worlds of Work and Education, Springer International Publishing, 2017, pp. 971–984, https://doi.org/10.1007/978-3-319-41713-4_45.

[46] A. Rausch, K. Kögler, J. Seifried, Validation of embedded experience sampling (EES) for measuring non-cognitive facets of problem-solving competence in scenario-based assessments, Front. Psychol. 10 (2019) 1200, https://doi.org/10.3389/fpsyg.2019.01200.

[47] A.T. Evers, B.I.J.M van der Heijden, Chapter 4: competence and Professional Expertise, in: M. Mulder (Ed.), Competence-based Vocational and Professional Education: Bridging the Worlds of Work and Education, Springer International Publishing, 2017, pp. 83–101, https://doi.org/10.1007/978-3-319-41713-4_4.

[48] E.H. Schein, Professional education: Some new Directions, McGraw-Hill, 1972. https://openlibrary.org/books/OL20946445M/Professional_education.

[49] G. Ryle, The Concept of Mind, 60th anniversary, Taylor & Francis Group, 2009.

[50] D.A. Schön, The Reflective Practitioner: How Professionals Think in Action, Routledge, 1983, https://doi.org/10.4324/9781315237473.

[51] D.A. Schön, Educating the Reflective Practitioner, Jossey-Bass, 1987.

[52] G. Cheetham, G. Chivers, The reflective (and competent) practitioner: A model of professional competence which seeks to harmonise the reflective practitioner and competence-based approaches, J. Eur. Ind. Train 22 (7) (1998) 267–276, https://doi.org/10.1108/03090599810230678.

[53] (ISC)^2. (2022). (ISC)^2 Cybersecurity Workforce Study. https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study.pdf.

[54] E. Crisol-Moya, M.A. Romero-López, M.J. Caurcel-Cara, Active methodologies in higher education: perception and opinion as evaluated by professors and their students in the teaching-learning process, Front. Psychol. 11 (2020), https://doi.org/10.3389/fpsyg.2020.01703.

[55] L. Deslauriers, L.S. McCarty, K. Miller, K. Callaghan, G. Kestin, Measuring actual learning versus feeling of learning in response to being actively engaged in the classroom, Proc. Natl. Acad. Sci. 116 (39) (2019) 19251–19257, https://doi.org/10.1073/pnas.1821936116.

[56] M. Stains, J. Harshman, M.K. Barker, S.V. Chasteen, R. Cole, S.E. DeChenne-Peters, M.K. Eagan, J.M. Esson, J.K. Knight, F.A. Laski, M. Levis-Fitzgerald, C. J. Lee, S.M. Lo, L.M. McDonnell, T.A. McKay, N. Michelotti, A. Musgrove, M. S. Palmer, K.M. Plank, A.M. Young, Anatomy of STEM teaching in North American universities, Science (1979) 59 (6383) (2018) 1468–1470, https://doi.org/10.1126/science.aap8892.

[57] S. French, G. Kennedy, Reassessing the value of university lectures, Teach. High. Educ. 22 (6) (2017) 639–654, https://doi.org/10.1080/13562517.2016.1273213.

[58] M.S. Carriger, What is the best way to develop new managers? Problem-based learning vs. lecture-based instruction, Int. J. Manag. Educ. 14 (2) (2016) 92–101, https://doi.org/10.1016/j.ijme.2016.02.003.

[59] D. Gijbels, F. Dochy, P. Van den Bossche, M. Segers, Effects of problem-based learning: A meta-analysis from the angle of assessment, Rev. Educ. Res. 75 (1) (2005) 27–61, https://doi.org/10.3102/00346543075001027.

[60] M. Wijnen, S.M.M. Loyens, G. Smeets, M. Kroeze, H. van der Molen, Comparing problem-based learning students to students in a lecture-based curriculum: Learning strategies and the relation with self-study time, Eur. J. Psychol. Educ. 32 (3) (2017) 431–447, https://doi.org/10.1007/s10212-016-0296-7.

[61] D.H. Jonassen, Typology of case-based learning: The content, form, and function of cases, Educ. Technol. 46 (4) (2006) 11–15. https://www.jstor.org/stable/44429309.

[62] P.A. Ertmer, A.A. Koehler, Online case-based discussions: Examining coverage of the afforded problem space, Educ. Technol. Res. Dev. 62 (5) (2014) 617–636, https://doi.org/10.1007/s11423-014-9350-9.

[63] D.M. Hull, P.B. Lowry, J.E. Gaskin, K. Mirkovski, A storyteller's guide to problem-based learning for information systems management education, Inf. Syst. J. 29 (5) (2019) 1040–1057, https://doi.org/10.1111/isj.12234.

[64] P. Lyons, R.P. Bandura, Stimulating employee learning: The confluence of case-based and self-regulated learning, Ind. Commer. Train. 52 (3) (2020) 171–183, https://doi.org/10.1108/ICT-12-2019-0109.

[65] P.C. Brown, H. Roediger, M. McDaniel, Make It Stick: The Science of Successful Learning, Harvard University Press, 2014, https://doi.org/10.4159/9780674419377.

[66] J.L. Kolodner, M. Guzdial, Theory and Practice of Case-Based Learning Aids, in: D. Jonassen, S. Land (Eds.), Theoretical Foundations of Learning Environments, 2nd, Routledge, 2012, p. 27, https://doi.org/10.4324/9780203813799.

[67] J.L. Kolodner, An introduction to case-based reasoning, Artif. Intell. Rev. 6 (1) (1992) 3–34, https://doi.org/10.1007/BF00155578.

[68] X. Yuan, K. Jiang, S. Murthy, J. Jones, H. Yu, Teaching security management with case studies: Experiences and evaluation, J. Educ. Inform. Cybern. 2 (2) (2010) 25–30. https://www.iiis.org/CDs2010/CD2010SCI/EISTA_2010/PapersPdf/EA605YI.pdf.
[69] X. Yuan, S. Murthy, J. Xu, H. Yu, Case studies for teaching physical security and security policy, in: 2010 Information Security Curriculum Development Conference, 2010, pp. 21–26, https://doi.org/10.1145/1940941.1940947.
[70] A. Ahmed, K. Lundqvist, C. Watterson, N. Baghaei, Teaching Cyber-Security for Distance Learners: a Reflective Study, in: 2020 IEEE Frontiers in Education Conference (FIE), 2020, pp. 1–7, https://doi.org/10.1109/FIE44824.2020.9274062.
[71] Y. Cai, Using case studies to teach cybersecurity courses, J. Cybersecur. Edu. Res. Pract. 2018 (2) (2018). https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/3.
[72] W. He, X. Yuan, L. Yang, Supporting case-based learning in information security with web-based technology, J. Inf. Syst. Educ. 24 (1) (2013) 31–40. http://jise.org/Volume24/n1/JISEv24n1p31.html.
[73] D. Ktoridou, I. Dionysiou, Case-based learning: an instructional model to incorporate information security topics in multidisciplinary courses at the University of Nicosia, in: IEEE Global Engineering Education Conference (EDUCON), 2011, pp. 466–469, https://doi.org/10.1109/EDUCON.2011.5773177.
[74] L. Cifuentes, W. Marti, O. Alvarez, R. Mercer, J. Scaparra, Systematic Design of a Case-based Learning Environment, 2009, pp. 4176–4183. https://www.learntechlib.org/primary/p/32083/.
[75] L. Cifuentes, R. Mercer, O. Alverez, R. Bettati, An architecture for case-based learning, TechTrends. 54 (6) (2010) 44–50, https://doi.org/10.1007/s11528-010-0453-9.
[76] J. Blanken-Webb, I. Palmer, S.-E. Deshaies, N.C. Burbules, R.H. Campbell, M. Bashir, A Case Study-based Cybersecurity Ethics Curriculum, in: 2018 USENIX Workshop on Advances in Security Education (ASE), 2018. https://www.usenix.org/conference/ase18/presentation/blanken-webb.
[77] J. Webster, R.T. Watson, Analyzing the past to prepare for the future: Writing a literature review, MISQ 26 (2) (2002) xiii–xxiii. https://www.jstor.org/stable/4132319.
[78] Association for Information Systems (AIS), Senior Scholars' List of Premier Journals, AIS, 2023. https://aisnet.org/page/SeniorScholarListofPremierJournals.
[79] J.O.D. Wylder, The life cycle of security managers: New responsibilities for a distributed environment, Inf. Syst. Manag. 9 (1) (1992) 62. https://www.proquest.com/docview/214127771.
[80] C. Hagstrom, S. Kendall, H. Cunningham, Googling For grey: Using Google and Duckduckgo to Find Grey Literature, The 23rd Cochrane Colloquium, Vienna, AT, 2015. http://2015.colloquium.cochrane.org/abstracts/googling-grey-using-google-and-duckduckgo-find-grey-literature.
[81] Scopus. (2023). Scimago Journal & Country Rank. https://www.scimagojr.com/.
[82] A. Yadav, V. Alexander, S. Mehta, Case-based instruction in undergraduate engineering: Does student confidence predict learning? Int. J. Eng. Educ. 35 (1) (2019) 25–34.
[83] D. Kirkpatrick, J. Kirkpatrick, Evaluating Training Programs: The four Levels, 3rd ed., Berrett-Koehler Publishers, 2006.
[84] H.-F. Hsieh, S.E. Shannon, Three approaches to qualitative content analysis, Qual. Health. Res. 15 (9) (2005) 1277–1288, https://doi.org/10.1177/1049732305276687.
[85] S. Ainslie, D. Thompson, S. Maynard, A. Ahmad, Cyber-threat intelligence for security decision-making: A review and research agenda for practice, Comput. Secur. 132 (2023) (2023) 103352, https://doi.org/10.1016/j.cose.2023.103352.
[86] V. Hooper, J. McKissack, The emerging role of the CISO, Bus. Horiz. 59 (6) (2016) 585–591, https://doi.org/10.1016/j.bushor.2016.07.004.
[87] S. Maynard, M. Onibere, A. Ahmad, Defining the strategic role of the chief information security officer, Pac. Asia J. Assoc. Inf. Syst. 10 (3) (2018), https://doi.org/10.17705/1pais.10303.
[88] T. Fitzgerald, Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other, J. Inf. Syst. Secur. 16 (5) (2007) 257–263, https://doi.org/10.1080/10658980701746577.
[89] C. Shayo, F. Lin, An exploration of the evolving reporting organizational structure for the chief information security officer (CISO) function, J. Comput. Sci. Inf. Tech. 7 (1) (2019) 1–20, https://doi.org/10.15640/jcsit.v7n1a1.
[90] Australian Cybersecurity Centre. (2020). Guidelines for cyber security roles | Cyber.gov.au. https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cyber-security-roles.
[91] P. Monzelo, S. Nunes, The role of the chief information security officer (CISO) in organizations, in: CAPSI 2019 Proceedings, 2019. https://aisel.aisnet.org/capsi2019/36.
[92] New Zealand National Cyber Security Centre, Governance Step Two: Establishing Roles & Responsibilities, 2019. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf.
[93] D. Ashenden, Information security management: A human challenge? Inf. Secur. Tech. Rep. 13 (4) (2008) 195–201, https://doi.org/10.1016/j.istr.2008.10.006.
[94] D. Gupta, Council post: The role of a ciso in building a modern cybersecurity culture, Forbes (2021). https://www.forbes.com/sites/forbestechcouncil/2021/08/17/the-role-of-a-ciso-in-building-a-modern-cybersecurity-culture/.
[95] G. Tejay, M. Winkfield, How CISOs can become effective leaders? A path-goal approach, in: SIG LEAD 2015 Proceedings, 2015. https://aisel.aisnet.org/siglead2015/1.
[96] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: managing a strategic balance between prevention and response, Inf. Manag. 51 (1) (2014) 138–151, https://doi.org/10.1016/j.im.2013.11.004.
[97] J. Lanz, The chief information security officer: The new CFO of information security, CPA Journal 87 (6) (2017) 52–57. https://www.proquest.com/docview/2213054557.
[98] J.H. Allen, G. Crabb, P.D. Curtis, B. Fitzpatrick, N. Mehravari, D. Tobar, Structuring the Chief Information Security Officer Organization, Software Engineering Institute, 2015, https://doi.org/10.1184/R1/6584423.v1.
[99] M. Choi, Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing, Sustainability. 8 (7) (2016) 638, https://doi.org/10.3390/su8070638.
[100] J. Loonam, J. Zwiegelaar, V. Kumar, C. Booth, Cyber-resiliency for digital enterprises: A strategic leadership perspective, IEEE Trans. Eng. Manag. 69 (6) (2022) 3757–3770, https://doi.org/10.1109/TEM.2020.2996175.
[101] E. Karanja, The role of the chief information security officer in the management of IT security, Inf. Comput. Secur. 25 (3) (2017) 300–329, https://doi.org/10.1108/ICS-02-2016-0013.
[102] E. Karanja, M.A. Rosso, The chief information security officer: An exploratory study, J. Inf. Technol. Manag. 26 (2) (2017) 23–47, https://doi.org/10.58729/1941-6679.1299.
[103] P. Monzelo, S. Nunes, Information security awareness and its impact on the CISO's responsibilities – A study of the portuguese environment, J. Inf. Secur. 17 (2) (2021) 81–102. https://www.jissec.org/Contents/V17/N2/V17N2-Monzelo.html.
[104] H.S. Sveen, F. Østrem, J. Radianti, B.E. Munkvold, The CISO role: A mediator between cybersecurity and top management, Norsk IKT-Konferanse for Forskning Og Utdanning 2 (2022) 2. https://ojs.bibsys.no/index.php/NIK/article/view/1013.
[105] M. Dawson, D. Burrell, E. Rahim, S. Brewster, Examining the role of the chief information security officer, J. Inf. Syst. Technol. Plan 3 (2010) 1–5. https://scholarworks.lib.csusb.edu/jitim/vol26/iss2/2.
[106] M.J. Drake, Teaching OR/MS with cases: A review and new suggestions, INFORMS Trans. Educ. 19 (2) (2019) 57–66, https://doi.org/10.1287/ited.2018.0204.
[107] S. Maslen, J. Hayes, Case based learning among practicing engineers: Design, facilitation and lessons learned, Cogn. Technol. Work 22 (2) (2020) 307–319, https://doi.org/10.1007/s10111-019-00569-0.
[108] M.Z. Nkhoma, T.K. Lam, N. Sriratanaviriyakul, J. Richardson, B. Kam, K.H. Lau, Unpacking the revised bloom's taxonomy: Developing case-based learning activities, Educ. Train. 59 (3) (2017) 250–264, https://doi.org/10.1108/ET-03-2016-0061.
[109] C. North, A. Brookes, Case-based teaching of fatal incidents in outdoor education teacher preparation courses, J. Adventure Educ. Outdoor Learn. 17 (3) (2017) 191–202, https://doi.org/10.1080/14729679.2017.1308873.
[110] H. Rong, I. Choi, C. Schmiedt, K. Clarke, Using failure cases to promote veterinary students' problem-solving abilities: a qualitative study, Educ. Technol. Res. Dev. 68 (5) (2020) 2121–2146, https://doi.org/10.1007/s11423-020-09751-y.
[111] M.J. Scalese, J. Kristeller, E. Hoot, F. Kong, A case-based approach for teaching medication safety to pharmacy students, Curr. Pharm. Teach. Learn 7 (4) (2015) 458–464, https://doi.org/10.1016/j.cptl.2015.04.011.
[112] A. Yadav, M. Vinh, G.M. Shaver, P. Meckl, S. Firebaugh, Case-based instruction: improving students' conceptual understanding through cases in a mechanical engineering course, J. Res. Sci. Teach 51 (5) (2014) 659–677, https://doi.org/10.1002/tea.21149.
[113] A. Tawfik, D. Jonassen, The effects of successful versus failure-based cases on argumentation while solving decision-making problems, Educ. Technol. Res. Dev. 61 (3) (2013) 385–406, https://doi.org/10.1007/s11423-013-9294-5.
[114] J. Reason, Managing the Risks of Organizational Accidents, 1st ed., Routledge, London, UK, 1997 https://doi.org/10.4324/9781315543543.
[115] M.-S. Yoo, H.-R. Park, Effects of case-based learning on communication skills, problem-solving ability, and learning motivation in nursing students, Nurs. Health Sci. 17 (2) (2015) 166–172, https://doi.org/10.1111/nhs.12151.
[116] A.A. Tawfik, W. Hung, P.J. Giabbanelli, Comparing how different inquiry-based approaches impact learning outcomes, Interdiscip. J. Probl.-based Learn. 14 (1) (2020) 1, https://doi.org/10.14434/ijpbl.v14i1.28624.
[117] M. Bi, Z. Zhao, J. Yang, Y. Wang, Comparison of case-based learning and traditional method in teaching postgraduate students of medical oncology, Med. Teach. 41 (10) (2019) 1124–1128, https://doi.org/10.1080/0142159X.2019.1617414.
[118] S. Gade, S. Chari, Case-based learning in endocrine physiology: an approach toward self-directed learning and the development of soft skills in medical students, Adv. Physiol. Educ. 37 (4) (2013) 356–360, https://doi.org/10.1152/advan.00076.2012.
[119] J. Hernandez-Serrano, D.H. Jonassen, The effects of case libraries on problem solving, J Comput. Assist. Learn 19 (1) (2003) 103–114, https://doi.org/10.1046/j.0266-4909.2002.00010.x.
[120] D. Jennings, Strategic management and the case method, J. Manag. Dev. 15 (9) (1996) 4–12, https://doi.org/10.1108/02621719610146211.
[121] G. Gao, K. Xiao, Y. Jia, H. Wang, Improving students' problem-solving ability through the 'information system security' project guided by the theory of inventive problem solving (TIPS), Innov. Educ. Teach. Int. (2021) 701–710, https://doi.org/10.1080/14703297.2021.1935292.
[122] I. Choi, K. Lee, Designing and implementing a case-based learning environment for enhancing ill-structured problem solving: classroom management problems

for prospective teachers, Educ. Technol. Res. Dev. 57 (1) (2009) 99–129, https://doi.org/10.1007/s11423-008-9089-2.
[123] S. Atwa, V.J. Gauci-Mansour, R. Thomson, I. Hegazi, Team-based and case-based learning: a hybrid pedagogy model enhancing students' academic performance and experiences at first-year tertiary level, Aust. Educ. Res. 46 (1) (2019) 93–112, https://doi.org/10.1007/s13384-018-0282-y.
[124] H.L. Harrington, K. Quinn-Leering, L. Hodson, Written case analyses and critical reflection, Teach. Teach. Educ. 12 (1) (1996) 25–37, https://doi.org/10.1016/0742-051X(96)89078-0.
[125] H. Shaked, The contribution of case-based learning to adopting a multidimensional view in educational leadership students, Int. J. Educ. Manag. 36 (2) (2022) 194–205, https://doi.org/10.1108/IJEM-08-2021-0347.
[126] L.D. Kantar, S. Sailian, The effect of instruction on learning: Case based versus lecture based, Teach. Learn. Nurs. 13 (4) (2018) 207–211, https://doi.org/10.1016/j.teln.2018.05.002.
[127] L. Cherubini, Exploring prospective teachers' critical thinking: Case-based pedagogy and the standards of professional practice, Teach. Teach. Educ. 25 (2) (2009) 228–234, https://doi.org/10.1016/j.tate.2008.10.007.
[128] Y. Cevik, T. Andre, Studying the impact of three different instructional methods on preservice teachers' decision-making, Res. Pap. Educ. 29 (1) (2014) 44–68, https://doi.org/10.1080/02671522.2012.742923.
[129] J. Jackson, Case-based teaching in a bilingual context: Perceptions of business faculty in Hong Kong, English Specif. Purp. 23 (3) (2004) 213–232, https://doi.org/10.1016/j.esp.2003.05.001.
[130] M.J. Dow, C.A. Boettcher, J.F. Diego, M.E. Karch, A. Todd-Diaz, K.M. Woods, Case-based learning as pedagogy for teaching information ethics based on the dervin sense-making methodology, J. Educ. Libr. Inf. Sci. 56 (2) (2015) 141–157. https://www.jstor.org/stable/90015179.
[131] S.B. Kapti, D.I. Beyaztas, A. Kapti, N. Senemoglu, Case based curriculum in administration and leadership course, Eur. J. Sci. Res. 11 (11) (2015) 82–93. https://eujournal.org/index.php/esj/article/view/5440.
[132] L. Noblitt, D.E. Vance, M.L.D. Smith, A Comparison of case study and traditional teaching methods for improvement of oral communication and critical-thinking skills, J. Coll. Sci. Teach. 39 (5) (2010) 26–32. https://www.jstor.org/stable/42993815.
[133] S. Hidi, K.A. Renninger, The four-phase model of interest development, Educ. Psychol. 41 (2) (2006) 111–127, https://doi.org/10.1207/s15326985ep4102_4.
[134] A Bandura, Self-efficacy: The exercise of Control, W.H. Freeman, 1997. https://openlibrary.org/books/OL1011521M/Self-efficacy.
[135] K. Ki-Yoon, K. Surendran, Information security management curriculum design: A joint industry and academic effort, J. Inf. Syst. Educ. 13 (3) (2002) 227–236. https://www.proquest.com/docview/200136446.
[136] M.T. Geier, Strategic thinking: Theoretical development and assessment, J. Strategy Manag. 17 (1) (2023) 1–21, https://doi.org/10.1108/JSMA-10-2021-0212.
[137] L. Young, Developing strategic thinking, Australian Army J. 13 (2) (2016) 5–22.
[138] M. Katsikitis, P.J. Hay, R.J. Barrett, T. Wade, Problem- versus case-based approaches in teaching medical students about eating disorders: A controlled comparison, Educ. Psychol. 22 (3) (2002) 277–283, https://doi.org/10.1080/01443410220138511.
[139] F. Rowe, What literature review is not: Diversity, boundaries and recommendations, Eur. J. Inf. Syst. 23 (3) (2014) 241–255, https://doi.org/10.1057/ejis.2014.7.

Ashley Anderson is a PhD candidate in the School of Computing and Information Systems at the University of Melbourne, where she also works as a senior educational designer. Her areas of interest include information security management, professional education, access and equity in education and academic self-efficacy.

Atif Ahmad is a Professor at the University of Melbourne's School of Computing and Information Systems where he also serves as Deputy Director of the Academic Centre of Cyber Security Excellence. Atif leads an interdisciplinary research team that studies how organizations protect their information resources through the managerial practices of prevention and response. He has authored over 100 scholarly articles in cybersecurity and received over AUD$4 M in grant income. Atif is a visiting fellow at the International Islamic University of Malaysia. He is a member of the editorial boards of Computers & Security and the Journal of Information Warfare. Atif has previously worked as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. Atif is a Certified Protection Professional with the American Society for Industrial Security. For more information, please visit https://www.atifahmad.me/.

Shanton Chang is a Professor of Information Behaviour and Social Aspects of Information Systems at the School of Computing and Information Systems, The University of Melbourne. He conducts interdisciplinary and mixed-methods research that often engages with end users of systems. He has co-authored over 100 interdisciplinary articles that explore end users' information behaviours, and the adoption and use of information systems. He is also Associate Dean (International) at the Faculty of Engineering and Information Technology.