Competencies of Cybersecurity Leaders: A Review and Research Agenda

Ashley Baines Anderson
University of Melbourne, abanderson@student.unimelb.edu.au

Atif Ahmad
University of Melbourne, atif@unimelb.edu.au

Shanton Chang
The University of Melbourne, shanton.chang@unimelb.edu.au

Competencies of cybersecurity leaders: A review and research agenda

Completed Research Paper

Ashley Anderson
University of Melbourne
Parkville, Vic 3052
abanderson@student.unimelb.edu.au

Atif Ahmad
University of Melbourne
Parkville, Vic 3052
atif@unimelb.edu.au

Shanton Chang
University of Melbourne
Parkville, Vic 3052
shanton.chang@unimelb.edu.au

Abstract

Increasingly, large organisations are turning to cybersecurity leaders such as chief information security officers (CISOs) to protect their information resources against attack. The role of the cybersecurity leader is distinct from other cybersecurity professionals in its need for strategy and collaboration, and distinct from other business leaders in its need to maintain situational awareness against active adversaries. Because the role is so new, however, organisations and educators continue to conceptualise it as a senior technological role rather than a strategic, business-oriented role. This representation leaves open a gap between what is viewed as 'business' and what is viewed as 'IT' – a gap that can leave organisations vulnerable to attack. In this systematic review, we examine the literature on cybersecurity leaders to develop a picture of the competencies required. Following analysis, we propose a preliminary matrix of competencies required for cybersecurity leaders. We conclude with an agenda for further research.

Keywords: information security management, cybersecurity, Chief Information Security Officer (CISO), professional education, leadership education, executive education, tertiary education, higher education, competence, competencies

Introduction

Modern organisations face an evolving challenge in protecting their information and IT infrastructure (Ahmad et al., 2014). Threats facing businesses, governments and not-for-profits can change rapidly, and an attack on these information resources can stop an organisation in its tracks. For example, in 2021, ransomware attackers locked down IT services giant Kaseya, then offered a global decryption key for US $70 million (Winder, 2021). Attackers combined technological and 'human' tactics: using a malware protection program to deliver the ransomware code, and timing their attack strategically on a holiday weekend in the US, when fewer staff would be on hand to detect and respond to the attack (Loman et al., 2021). Attacks like these show that cybersecurity is no longer a low-level operational problem. Organisations now exist in an environment with severe, unpredictable threats, and need strategic advice on how to survive them.

Increasingly, large organisations are turning to cybersecurity leaders – such as Chief Information Security Officers (CISOs), directors of cybersecurity, and information security managers – to lead the effort of protecting information resources against such threats. Cybersecurity leaders play a vital enabling role for the broader business: protecting an organisation's data, information and knowledge enables researchers and developers to pursue innovative new products; protecting an organisation's technological infrastructure supports its overall operational continuity. The cybersecurity leader brings these protection skills to the board room.

Despite the importance of the cybersecurity leader, professionals who wish to progress into these roles struggle to find high-quality leadership education targeted to their role. Most cybersecurity knowledge frameworks are technologically focused. Generated in outcome-based education models, these curricula frequently use an operational cybersecurity role as their planned 'outcome'. For example, in a recent review, Hallett et al. compared the UK Cybersecurity Body of Knowledge (CyBOK) with four other frameworks, including the National Initiative for Cybersecurity Education (NICE) and the Institute of Information Security Professionals (IISP). While all five frameworks are clearly robust, they are heavily focused on issues like network, software and hardware security (see Hallett et al., 2018). Cybersecurity graduates educated using these frameworks will be well prepared for their roles; however, once they progress to leadership, a lack of education in policy and strategy would leave them with a skill gap. Even leadership-focused training, such as ISACA's Certified Information Security Manager (CISM) certification and the Certified Information Systems Security Professional (CISSP) certification run by (ISC)^2, focus mainly on technical rather than perceived 'soft' skills.

The gap between cybersecurity knowledge frameworks and cybersecurity leadership has arisen because cybersecurity leaders' roles are newer than operational cybersecurity roles, newer than established roles such as the Chief Information Officer (CIO), and not very well understood (Fitzgerald, 2007). Cybersecurity used to be an operational-level problem, and so curricula have focused on producing graduates who can find operational solutions. Now that cybersecurity has grown into a strategic problem with some technological solutions (Ahmad et al., 2014), we need a framework for the leader, one which differentiates the strategic role from the operational. Such a role description will provide educators with a more accurate 'outcome' on which to base a cybersecurity leadership curriculum, thereby helping educators prepare professionals who wish to fulfil these roles.

To describe this role, we will draw upon the competency model described by Gonczi et al. (1990), and upon the concept of the reflective practitioner proposed by Schön (1983) and further developed by Eraut (1994). Gonczi, Hager and Oliver, in their 1990 report for the Australian Department of Employment, Education and Training, shift the idea of professional competence to what they call an "integrated approach" (p. 30). Earlier conceptions of professional competence had either consisted of a list of roles and tasks that must be performed to a pre-set standard (Gonczi et al., 1990), or of a list of attributes – usually knowledge, skills and attitudes – that a professional must possess (Schein, 1973). The finding of Gonczi et al. (1990) was that an integrated approach to these four components overcomes many of the shortcomings of granular focus on knowledge, abilities or tasks. Thus, competence consists of:

- *Knowledge*: an understanding of concepts, principles, rules and procedures
- *Skills*: abilities as applied in practice
- *Attitudes*: desires and values
- *Roles:* areas of practice to which knowledge, skills and attitudes are applied, also called *domains* or *functions* (Gonczi et al., 1990).

This integrated approach also has the advantage of laying bare the attitudinal requirements that are often skipped in task-based lists of competencies. For example, in the 2010s, engineers from a competing firm combined a range of tactics to steal information about a mobile-phone testing robot (Ahmad et al., 2020). Improved communication among physical security, information security, vendor management and R&D personnel could have stopped the attack sooner, but the disconnects in communication were almost certainly not due to a lack of communication *skill*. Rather, the personnel involved required knowledge of what information was salient to communicate and with which departments, and a commitment to maintaining organisational situational awareness.

These definitions of *knowledge* and *skills* above draw upon an older divide between 'knowing that' and 'knowing how' (Ryle, 1949). Later theorists, while not denying a division between skills and propositional knowledge, do raise questions about what 'knowing' looks like when it is put into practice. Schön, questioning a positivist view of professional expertise, proposes knowing-in-action as a distinct type of knowledge (Schön, 1983). Eraut, discussing theory and propositional knowledge, proposes that knowledge "rarely gets taken off the shelf and applied without some kind of transformation" (Eraut, 1994, p. 157). Schön also postulates: "It seems right to say that the knowing is *in* our action" (Schön, 1983, p. 49). 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 existing models. For a complex, strategic role like that of the cybersecurity leader, we aim to consider all facets of professional competence, which requires us to phrase our question broadly. In the sections that follow, we address the following question:

What competencies do cybersecurity leaders need to carry out their roles?

This systematic review is structured as follows. First, we set out our methods for searching and analysing the literature. In our findings, we present a table of knowledge, skills, attitudes and roles, followed by a description of each role. In our discussion, we synthesise our findings to describe the cybersecurity leader as a professional. We conclude with an agenda for further research.

Literature Review Methodology

To address our research question, we carried out a systematic search of information systems and information security management literature, including industry literature where appropriate.

We followed the systematic review process set out by vom Brocke et al. (2009). As a first step in this process, we identified relevant databases before identifying search terms and running our search. We created lists of top journals in the cybersecurity field, and identified databases containing those journals. Importantly, we did not limit our later search to identified top journals – the list was used solely to identify databases with relevant material.

We then selected search terms and ran our database searches. We considered a broad definition of 'cybersecurity leaders', including executives, directors and managers whose roles centre around protecting information resources. Because many business sources do not use the term 'competencies' in the same way as educational sources, we did not limit our database searches to explicit discussions of competencies, choosing instead to select for requisite knowledge, skills and attitudes during the refinement stage. We refined our search results using an inclusion criterion; that is, we reviewed the titles and abstracts, and retained only those search results which describe the competencies required by cybersecurity leaders.

Following our initial search, we conducted backward chaining and forward chaining (Webster and Watson, 2002) to find sufficient sources for a robust analysis. Industry sources also discuss organisations' requirements for cybersecurity leaders; therefore, we also conducted a Google search to select industry articles from high-quality sources. At each stage, we refined our results using the same inclusion criterion. The above search process and its results are summarised in Table 1.

01. Database search	Search string: (cybersecurity OR "cyber security" OR "information security") AND (manager OR executive OR CEO OR CISO OR "Chief Information Security Officer") Databases: AISeL, Business Source Complete (EBSCO) Peer-reviewed only 2010–present Search date: 25 October 2021 Result: 6021 search results
2. Refine: remove irrelevant results	Criterion: Describes the competencies required by cybersecurity leaders Rationale: Articles explicitly discuss competencies, whether using the word 'competency' or the related words 'skills', 'abilities', 'tasks' or 'roles' (consensus on these terms is described in Gonczi et al., 1990) Result: 8 relevant articles (out of 6021 results)

3. Backward chaining of results from item 2	Criterion: Describes the competencies required by cybersecurity leaders Rationale: As in row 2 Result: 9 additional articles
4. Forward chaining of results from item 2	Search tool: Google Scholar Search date: 25 October 2021 Criterion: Describes the competencies required by cybersecurity leaders Rationale: As in row 2 Result: 2 additional articles
5. Supplementary search for industry reports on the role of cybersecurity leaders	Search engine: Google Search date: 25 October 2021 Search terms: CISO cybersecurity organisation Criterion: Describes the competencies required by cybersecurity leaders Source: Government and reputable industry publications Result: 4 additional articles
6. Sum of results in items 2–5	23 articles

Table 1. Search results

In refining results, we selected those sources which explicitly described knowledge, skills, attitudes required by those leaders, or which described the roles they perform.

We used a content analysis approach (Hsieh and Shannon, 2005) to analyse our search results. We began with a conventional content analysis approach, extracting relevant sentences, and then assigning codes to functions and attributes of the cybersecurity leader mentioned within our articles. Because our search explicitly sought knowledge, skills, attitudes and roles, our next step took a more directed approach. We classified the emergent codes as either knowledge (K), skill (S), attitude (A), or role (R). Gonczi, Hager and Oliver (1990) described roles as the functions performed by a professional, or as higher-level tasks to which knowledge, skills and attitudes are applied. Therefore, we classified knowledge, skill and attitude codes to into higher-level categories for their relevant roles; for example, we assigned the skill *lead incident investigations* into the role of *leading incident response*.

Findings

Our 23 articles included 16 from peer-reviewed journals and conferences (including 4 conference articles and one journal article published by the Association of Information Systems). Our results also included publications regarding the role of cybersecurity leaders from the Australian Cybersecurity Centre, the Software Engineering Institute at Carnegie Mellon University, the New York Society of CPAs, Deloitte, Strategic Human Resource Management, Ernst & Young, and Forbes. 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 the role of the manager. That is, much research focuses on the actions that organisations typically take rather than focusing on the individuals who *carry out* those actions. 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 middle management or executive management, but our sample examined organisations large enough to have a board, organisations where the cybersecurity leader acts at a strategic or tactical level rather than an operational level. We did notice some variation among the results; for example, Hooper & McKissack (2016), 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 identify competency needs at a purely operational level. That is, because our research question focuses on the *leader* rather than the early-career professional, all of the knowledge, skills, attitudes and roles we identified are intended to refer to the context of management or executive leadership.

Our findings are summarised in Table 2. Please note that **(K)** denotes a knowledge code, **(S)** denotes a skill code and **(A)** denotes an attitude code. The roles appear as the higher-level categories at left.

Roles	**Attributes: Knowledge (K), Skills (S) and Attitudes (A)**
Partner with business leaders	• **Communicate with business leaders (S)** (Aguas, Kark and François 2016; Alexander & Cummings, 2016; Ashenden & Sasse, 2013; Australian Cybersecurity Centre, 2020; Dawson et al., 2010; Fitzgerald, 2007; Gupta, 2021; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Karanja & Rosso, 2017; Lanz, 2017; Lovejoy et al., 2021; Marotta & Pearlson, 2019; Maynard et al., 2018; Monzelo & Nunes 2019; Shayo & Lin, 2019; Tejay & Winkfield, 2015; Whitten, 2008) • **Collaborate with external stakeholders (S)** (Australian Cybersecurity Centre, 2020; Baskerville et al., 2014; Dawson et al., 2010; Gupta, 2021; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Karanja, 2017; Lanz, 2017; Lovejoy et al., 2021; Shayo & Lin, 2019; Whitten, 2008) • **Willingness to devote effort to collaboration (A)** (Aguas, Kark and François 2016; Shayo & Lin, 2019)
Lead the cybersecurity team	• **Communicate with cybersecurity team (S)** (Cleveland and Cleveland, 2018; Fitzgerald, 2007; Hooper & McKissack, 2016; Lovejoy et al., 2021; Marotta & Pearlson, 2019; Maynard et al., 2018; Monzelo & Nunes 2019; Shayo & Lin, 2019; Tejay & Winkfield, 2015) • **Motivate team (S)** (Choi, 2016; Dawson et al., 2010; Tejay & Winkfield, 2015) • **Develop talent pipeline (S)** (Aguas, Kark and François 2016; Australian Cybersecurity Centre, 2020; Cleveland and Cleveland, 2018; Dawson et al., 2010; Lovejoy et al., 2021; Tejay & Winkfield, 2015) • **Accepting of errors (A)** (Ashenden & Sasse, 2013; Tejay & Winkfield, 2015)
Direct cybersecurity strategy	• **Understand the organisation's strategy (S)** (Aguas, Kark and François, 2016; Alexander & Cummings, 2016; Australian Cybersecurity Centre, 2020; Fitzgerald, 2007; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Maynard et al., 2018; Monzelo & Nunes 2019; Shayo & Lin, 2019) • **Develop and implement strategy (S**) (Baskerville et al., 2014; Cleveland and Cleveland, 2018; Karanja, 2017; Lovejoy et al., 2021; Maynard et al., 2018; Monzelo & Nunes 2019) • **Align cybersecurity strategy with organisation's strategy (S)** (Aguas, Kark and François, 2016; Dawson et al., 2010; Kappers & Harrell, 2020; Karanja, 2017; Lovejoy et al., 2021; Maynard et al., 2018; Monzelo & Nunes 2019) • **Allocate resources effectively (S)** (Aguas, Kark and François, 2016; Australian Cybersecurity Centre, 2020; Cleveland and Cleveland, 2018; Dawson et al., 2010; Fitzgerald, 2007; Gupta, 2021; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Maynard et al., 2018; Shayo & Lin, 2019) • **Willingness to learn about the organisation's strategy (A)** (Aguas, Kark and François, 2016) • **Use creativity and imaginative thinking (A)** (Maynard et al., 2018)

Lead cybersecurity policy and governance	• **Develop and implement cybersecurity policies (S)** (Aguas, Kark and François, 2016; Allen et al., 2015; Australian Cybersecurity Centre, 2020; Choi 2016; Dawson et al., 2010; Gupta, 2021; Kappers & Harrell, 2020; Lanz, 2017; Monzelo & Nunes 2019; Whitten, 2008) • **Oversee plans and procedures (S)** (Allen et al., 2015; Cleveland and Cleveland, 2018; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Lanz, 2017; Maynard et al., 2018; Monzelo & Nunes 2019) • **Develop and implement a governance mechanism (S)** (Aguas, Kark and François, 2016; Allen et al., 2015; Australian Cybersecurity Centre, 2020; Hooper & McKissack, 2016; Lanz, 2017; Marotta & Pearlson, 2019; Monzelo & Nunes 2019) • **Drive continuous improvement (S)** (Aguas, Kark and François, 2016; Maynard et al., 2018; Monzelo & Nunes 2019)
Oversee the SETA program	• **Champion culture of awareness (S)** (Aguas, Kark and François, 2016; Ashenden & Sasse, 2013; Australian Cybersecurity Centre, 2020; Gupta, 2021; Kappers & Harrell, 2020; Marotta & Pearlson, 2019; Maynard et al., 2018; Monzelo & Nunes 2019; Shayo & Lin, 2019) • **Oversee security training and development program (S)** (Australian Cybersecurity Centre, 2020; Choi 2016; Cleveland and Cleveland, 2018; Dawson et al., 2010; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Marotta & Pearlson, 2019; Monzelo & Nunes 2019; Whitten, 2008)
Oversee cybersecurity risk management	• **Understand technological controls (K)** (Karanja & Rosso, 2017; Monzelo & Nunes 2019; Whitten, 2008) • **Understand risk holistically (K)** (Aguas, Kark and François, 2016; Alexander & Cummings, 2016; Australian Cybersecurity Centre, 2020; Monzelo & Nunes 2019) • **Understand current threat landscape (K)** (Aguas, Kark and François, 2016; Australian Cybersecurity Centre, 2020; Gupta, 2021; Lovejoy et al., 2021; Maynard et al., 2018; Whitten, 2008) • **Identify and prioritise assets (S)** (Aguas, Kark and François, 2016; Monzelo & Nunes 2019; Shayo & Lin, 2019) • **Identify and evaluate risks and threats (S)** (Aguas, Kark and François, 2016; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Marotta & Pearlson, 2019; Shayo & Lin, 2019) • **Oversee technology security controls (S)** (Aguas, Kark and François, 2016; Allen et al., 2015; Gupta, 2021; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Karanja, 2017; Lanz, 2017; Marotta & Pearlson, 2019; Shayo & Lin, 2019) • **Facilitate physical security (S)** (Fitzgerald, 2007; Kappers & Harrell, 2020) • **Manage compliance (S)** (Aguas, Kark and François, 2016; Allen et al., 2015; Ashenden & Sasse, 2013; Australian Cybersecurity Centre, 2020; Gupta, 2021; Hooper & McKissack, 2016; Karanja, 2017; Lanz, 2017; Lovejoy et al., 2021; Monzelo & Nunes 2019) • **Monitor and evaluate controls (S)** (Aguas, Kark and François, 2016; Australian Cybersecurity Centre, 2020; Dawson et al., 2010; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Lanz, 2017; Lovejoy et al., 2021; Marotta & Pearlson, 2019; Monzelo & Nunes 2019)

	• **Maintain organisational situational awareness (S)** (Aguas, Kark and François 2016; Allen et al., 2015; Australian Cybersecurity Centre, 2020; Baskerville et al., 2014; Gupta, 2021; Hooper & McKissack, 2016; Maynard et al., 2018; Shayo & Lin, 2019) • **Adapt to circumstances (S)** (Alexander & Cummings, 2016; Cleveland and Cleveland, 2018; Gupta, 2021; Hooper & McKissack, 2016; Lovejoy et al., 2021; Maynard et al., 2018; Shayo & Lin, 2019) • **Willingness to accept calculated risk (A)** (Aguas, Kark and François 2016; Alexander & Cummings, 2016; Allen et al., 2015; Lanz, 2017; Monzelo & Nunes, 2019)
Lead incident response	• **Plan incident response strategy (S)** (Alexander & Cummings, 2016; Baskerville et al., 2014; Cleveland and Cleveland, 2018; Kappers & Harrell, 2020; Lanz, 2017; Shayo & Lin, 2019; Whitten, 2008) • **Lead response and recovery (S)** (Alexander & Cummings, 2016; Allen et al., 2015; Australian Cybersecurity Centre, 2020; Baskerville et al., 2014; Cleveland and Cleveland, 2018; Dawson et al., 2010; Hooper & McKissack, 2016; Kappers & Harrell, 2020; Marotta & Pearlson, 2019; Whitten, 2008) • **Lead incident investigations (S)** (Allen et al., 2015; Baskerville et al., 2014; Gupta, 2021; Karanja, 2017; Lanz, 2017; Whitten, 2008)

Table 2. The competencies of a cybersecurity leader

Role: Partner with business leaders

In this role, cybersecurity leaders must act more like interpreters than security professionals. Maynard et al. (2018) observe 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" (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 (2007) remarks, "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" (p. 261). Fitzgerald (2007) also provides an interesting comparison for development over time – in that paper, the CIO's role is characterised as 'where technology meets the business' (p. 259), while the CISO is characterised as 'protecting the business' (p. 261). By 2018, Maynard et al. describe a CISO role that is more closely aligned with 'where technology meets business', emphasising the need to contextualise and advocate for their strategies.

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, Kark and François (2016) and Shayo and Lin (2019) place equal importance on the willingness to put effort into collaboration. Aguas et al. 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" (Aguas et al., 2016, p. 76).

Throughout our findings, we noticed a tension at the heart of the cybersecurity leader's role: Business leaders engage cybersecurity leaders with the aim of eliminating risk (Australian Cybersecurity Centre, 2020; Hooper & McKissack, 2016; Monzelo & Nunes 2019). Simultaneously, business leaders frequently accept risk in order to achieve business objectives and feel frustrated by risk-conscious cybersecurity leaders who advise limitations to their activities. 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 (Aguas, Kark and François 2016; Alexander & Cummings, 2016; Fitzgerald, 2007; Gupta, 2021; Lovejoy et al., 2021; Maynard et al., 2018; Shayo & Lin, 2019; Tejay & Winkfield, 2015). Skills in communication may be essential for this endeavour, but in our discussion, we will argue that the knowledge of what information to convey and the commitment to collaboration are equally essential for the cybersecurity leader to succeed.

Role: Lead the cybersecurity team

In their role as business partner, our findings suggest that cybersecurity leaders must act as interpreters of technical information for strategic leaders. In their role as leaders, our findings suggest that cybersecurity leaders must act as interpreters of strategy for technical personnel. As summarised by Lovejoy et al. (2021), "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."

Here again the literature focused heavily on skills. Ashenden & Sasse (2013) 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" (p. 404). On a related note, Shayo & Lin believe that cybersecurity leaders should "have the ability to create a culture of shared responsibility and accountability should a breach occur" (2019, p. 9). While our results did not frequently focus on such attitudinal requirements, there is evidence that cybersecurity leaders are more effective if they avoid demonising failure (Ashenden & Sasse, 2013; Shayo & Lin, 2019).

Role: Direct cybersecurity strategy

Without an explicit lens of "knowledge, skills and attitudes", we have seen that 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" (Maynard et al., 2018, p. 73). Indeed, they "must be able to ascertain what is going on in the business to adequately support the mission" (Fitzgerald, 2007, 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 organisational strategy, and then allocate resources effectively in service of that strategy.

By contrast, only one paper pointed that understanding the organisation's strategy must result from cybersecurity leaders being willing to make an effort to understand it. Furthermore, only one article mentioned that cybersecurity leaders need to "employ creativity and imaginative thinking to devise effective and relevant strategies" (Maynard et al., 2018, p. 72). However, the lack of ubiquity here may not speak to a lack of importance. Rather, it 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 and colleagues (2014), 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. By contrast, they describe the response paradigm as one in which leaders assume risks are unpredictable, and safeguards are required to 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" (Baskerville et al., 2014, p. 139). Baskerville et al. also speculate that the prevention paradigm is "dominant in contemporary commercial organizations" (2014, p. 149). Our findings indicate that the prevention paradigm may dominate the research view of the cybersecurity leader as well: While many articles in our sample pointed to the need for cybersecurity leaders to be competent strategists, only Baskerville et al. (2014) and one other paper (Maynard et al., 2018) specified that these strategies need to encompass the response mode.

As with the need for cybersecurity leaders to employ 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:

> The increasing sophistication in attacks suggests that many organizations may need to reconsider their balance between prevention and response strategies. 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-centered 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. (Baskerville et al., 2014, p. 150)

In other words, much of the extant literature does not address the response paradigm. However, Baskerville et al. (2014) and Maynard et al. (2018) contend that cybersecurity leaders need to be increasingly aware of the response paradigm – and able to select the right balance between the paradigms – to direct cybersecurity strategy effectively in the face of increasingly sophisticated threats.

Role: Direct cybersecurity policy and governance

In service of strategy, our review finds that cybersecurity leaders need to be able to implement a suite of policies, plans and procedures, and oversee them with effective governance. This link between strategy and governance is picked up by 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" (Aguas et al., 2016).

Governance is a prime example of an essential role of cybersecurity leaders that can be overlooked by organisations and educators. When combatting an active adversary like a cyber attacker, governance is a crucial tactic; indeed, breaking down silos minimises organisational exposure (Ahmad et al., 2020). And yet, many organisations still place cybersecurity leaders under Chief Information Officers (CIOs), ignoring their importance outside the realm of IT (Lanz, 2017). 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" (2017, p. 57). Cybersecurity leaders must be able to influence the whole organisation to be effective (Lanz, 2017; Marotta & Pearlson, 2019), and according to the literature, this influence must extend beyond the SETA program into governance and policy (Aguas, Kark and François, 2016; Allen et al., 2015; Australian Cybersecurity Centre, 2020; Hooper & McKissack, 2016; Lanz, 2017; Marotta & Pearlson, 2019; Monzelo & Nunes 2019).

Role: Oversee the SETA program

The need to oversee the security education, training and awareness (SETA) program came up comparatively infrequently; indeed, some 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" (Aguas et al., 2016, p. 86). In interviews with CISOs analysed by Ashenden & 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" (Ashenden & Sasse, 2013, p. 403). Clearly, cybersecurity leaders in the industry see the need for a complex set of communication skills.

Role: Oversee cybersecurity risk management

The cybersecurity leader's role as a risk manager was by far the most frequently described in the literature. Risk-management competencies came up repeatedly and with more nuance than the leadership skills, resulting in a large array of well-sourced codes. We consider that this weighting reflects a general perception of cybersecurity leaders in which managing 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" (Alexander & Cummings, 2016). 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. Deloitte's 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" (Aguas et al., 2016, 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 (Aguas et al., 2016; Allen et al., 2015; Lanz, 2017).

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" (Gupta, 2021, para 3). For Gupta, organisations must cultivate a defensive posture for a constantly changing landscape – one with an active opponent. An information security manager cited in Baskerville et al. (2014) uses an alternative metaphor, one which 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. (participant cited in Baskerville et al., 2014, p. 149)

These cybersecurity leaders are both expressing that they cannot effectively manage risk solely through traditional risk assessment and mitigation, or even solely through situational awareness 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 of '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 the prevention mode and the response mode. We will revisit this question in the discussion.

Role: Lead incident response

The roles described above mainly pertain to 'business as usual'. During business as usual, one could argue that a cybersecurity leader behaves much like any other business leader, albeit a leader with more awareness of potential threat actors and a constantly shifting threat landscape. By 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 test and rehearse them as well (Alexander & Cummings, 2016; Shayo & Lin, 2019). In crisis situations, cybersecurity leaders need to show a "flexible problem-solving approach" and remain calm enough to "facilitate the appropriate response" (Whitten, 2008, p. 16). Additionally, Whitten asserts that the "problem-solving attribute should also entail investigative skills that aid in tracking a security issue trail" (2008, p. 16). In this role, cybersecurity leaders need to be able to problem-solve and make decisions in real time, and analyse scenarios 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. (2014) 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 one characterised by traditional risk management, and response mode as characterised by incident response. Surprisingly, however, Baskerville and colleagues 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 (2014). It is notable that even the competencies of incident response appear to have dimensions related to both prevention and response modes.

Discussion

The role of the cybersecurity leader: a balancing act

Our research question was "*What competencies do cybersecurity leaders need to carry out their roles?*" We list the competencies found in the literature in Table 2, but in summary, the overall 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 (Baskerville et al., 2014). 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 (Aguas et al., 2016).

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 – bridges with business leaders, the cybersecurity team, and other departments throughout the organisation. Externally, they need to build information-sharing networks with vendors, clients and regulators, and even with competitors (Hooper & McKissack, 2016; Gupta, 2021; Lanz, 2017). 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, the cybersecurity leader must balance their efforts and resources between prevention mode and response mode (Baskerville et al., 2014). Cybersecurity leaders in many industries are forced to spend a great deal of time on regulatory compliance (Lovejoy et al., 2021) – that is, in prevention mode – but the cybersecurity leader needs 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, or clientele, overlooking response mode entirely could have catastrophic consequences.

It is this balancing act that returns us to the concept of knowing-in-action posed by Schön (1983). If we return to the definitions from Gonczi et al. (1990), 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. 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* (Schön, 1983, p. 49); Eraut notes some challenges with Schön's terms *reflection-in-action* and *reflection-on-action* and describes the process as rapid or deliberative metacognition, depending on speed (Eraut, 1994, p. 149). Eraut also uses the term *control knowledge* for a generalised form of this process (1994, p. 81), which includes self-evaluation and strategic thinking.

Based on our findings, we argue that a cybersecurity leader needs to employ control knowledge and metacognition in order 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 employ 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 combat leadership, continually advancing an organisation's goals while countering an active adversary.

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. Further, 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.

Research agenda

Existing research has examined many aspects of the cybersecurity leader's role. However, the body of literature examining the role of cybersecurity leaders is still relatively small. The lack of literature may follow from the dominant focus in cybersecurity research: researchers in cybersecurity mainly focus on the technological controls rather than the organisational practice of cybersecurity, and even within the body of research on practice, education is not a central focus. Therefore, relatively few papers profile the competencies required by any one cybersecurity professional. To progress our understanding further, we propose the following research agenda. Further research on the individual role could investigate how the individual affects and is affected by the practice of the organisation as a whole, but here, we propose research that will help organisations hire, educate and develop individual leaders.

Finding the missing competencies

We believe that the list of competencies generated by the literature is sound, but not yet complete, as a generating a complete list of competencies hasn't been the focus of prior research. Further research could create a comprehensive picture of the competencies required by cybersecurity leaders by gathering data about the knowledge, skills and attitudes required for those roles. 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 quickly when compared with other roles, and a consensus of industry experts can be a valuable way to add detail to our existing understanding while forecasting upcoming changes.

We anticipate two sets of findings. First, we anticipate that future research will reveal necessary competencies related to ethics, privacy, and legal requirements. While integrity and a knowledge of ethics received three passing mentions in our sample, they were not listed as explicitly required competencies. We expect that ethical, legal and regulatory requirements are lightly touched upon 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 ethics, 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. Table 3 below summarises the results from Table 2, omitting the citations. In Table 3, the annotation "*Implied"* denotes knowledge or attitudes that were not stated in the literature but which we judge were implied. We observed the literature tended to focus heavily on skill requirements rather than knowledge or attitude requirements, but in these 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). While not explicitly stated, understanding principles of communicating with different audiences (knowledge) is an essential accompaniment to the skill and the attitude.

Role	Knowledge	Skill	Attitude
Partner with business leaders	• *Implied*: Understand what information is important to which audiences • Implied: Understand how to foster relationships	• Communicate with business leaders • Collaborate with external stakeholders	• *Implied*: Commitment to sharing information • Willingness to devote effort to collaboration
Lead the cybersecurity team	• *Implied*: Understand people leadership • *Implied*: Understand what information is important to which audiences	• Communicate with cybersecurity team • Motivate team • Develop talent pipeline	• Accepting of errors • *Implied:* Willingness to devote effort to communicating, motivating and mentoring
Direct cybersecurity strategy	• Understand the organisation's strategy • *Implied*: Understand principles of business strategy • *Implied*: Understand budgeting • *Implied*: Understand resource management	• Develop and implement strategy • Align cybersecurity strategy with organisation’s strategy • Allocate resources effectively	• Willingness to learn about the organisation's strategy • Use creativity and imaginative thinking
Direct cybersecurity governance and policy	• *Implied*: Understand the role of policies, plans and procedures • *Implied*: Understand the principles of governance	• Develop and implement cybersecurity policies • Oversee plans and procedures • Develop and implement a governance mechanism • Drive continuous improvement	• *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	• Oversee security training and development program • Champion culture of awareness	• *Implied:* Willingness to devote effort to implementing training program • *Implied:* Commitment to creating a culture of awareness
Oversee cybersecurity risk management	• Understand technological controls • Understand risk holistically • Understand current threat landscape • *Implied*: Understand relevant regulations • *Implied*: Understand adversarial thinking	• Identify and prioritise assets • Identify and evaluate risks and threats • Oversee technology security controls • Facilitate physical security • Manage compliance • Monitor and evaluate controls • Maintain organisational situational awareness • Adapt to circumstances	• Willingness to accept calculated risk • *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 • Lead response and recovery • Lead incident investigations	• *Implied:* Willingness to devote effort to planning incident response strategy • *Implied:* Capacity to respond during an emergency • *Implied:* Willingness to devote effort to investigations

Table 3. Projected competencies of cybersecurity leaders

The tendency of literature to identify skills rather than attitudes or knowledge is not surprising. When employers design position descriptions, and educators design curricula, the desire for quantifiable outcomes encourages a focus on skills, which are often observable and measurable. Knowledge and particularly attitudes are virtually impossible to measure directly. However, as illuminated by Gonczi et al. (1990), 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 – already include a mixture of knowledge, skills and attitudes in their competency requirements. Therefore, we anticipate that future findings regarding the cybersecurity leader will feature attitudes and knowledge, particularly those listed as 'implied' in Table 3.

In summary, our expected version of Table 3 will include privacy, ethical, 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, and future research could address the methods educators need to use to attain these objectives. While it will be difficult for educators to measure knowledge and attitudes, we expect some of them to emerge as very high-priority competencies.

Prioritising competency requirements

In addition to improving the list of competencies, it would also be valuable to discover which competencies have the most significant impact on the performance of a cybersecurity leader. Educational curricula are often shaped by experts' tacit knowledge of which competencies to prioritise, but if educators don't 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 postgraduate). 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. Industry experts would also provide valuable insight in identifying the crucial competencies, though the act of ranking lends itself to a more quantitative (or at least mixed-method) approach. A Delphi study would be instructive.

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 it risk tolerance. Competencies related to information sharing include the skill of and commitment to communicating with business leaders, as well as the skill of and commitment to communicating with the cybersecurity team. Our findings suggest that information gathering and sharing can extend to regulators, suppliers, and even competitors, with the ultimate aim of blocking cyber-threat actors (Hooper & McKissack, 2016; Lanz, 2017; Shayo & Lin, 2019). 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 to analyse, what 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, athletes, or military leaders would – cybersecurity leaders can plan and prioritise their activities based on the strategy and tactics they expect their opponents to employ.

Investigating the framing

It is possible that multiple frames are limiting the way in which we conceptualise the cybersecurity leader's role. A frame or paradigm is valuable in 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.

In our findings, we identified one paradigm – prevention mode – which 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's 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 prevention and response mode. While practitioners are familiar with the prevention-mode dimensions of most competencies, the field does not yet have an understanding of the response-mode dimensions. For example, policies, plans and procedures are typically prevention focused, but what would policies and procedures look like if they were incident-centred? What knowledge, skills and attitudes would the cybersecurity leader need to re-focus policy on response mode? 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 while both modes are essential, cybersecurity leaders may need to focus more heavily on the 'response mode' dimensions of their competencies in the future due to the increase in sophisticated attacks.

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

Table 4. Research questions in cybersecurity leadership

Limitations

This systematic review excluded research in languages other than English, and it is limited by the number of databases searched. 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.

Contribution

This article contributes to theory in two ways. First, this article provides grounds for further research on the role of the cybersecurity leader. Using a systematic review methodology (vom Brocke et al., 2009; Webster and Watson, 2002), and categorising competencies into knowledge, skills and attitudes for each role, we exposed specific competencies that are likely to be necessary for cybersecurity leaders but are absent from the literature. We have also identified a frame (prevention mode) that is limiting the field's conceptualisation of the role, thereby exposing a research gap for competencies in response mode. There is a heavy bias toward prevention in the research, but prevention alone is not sufficient to keep organisations safe – in order to be truly resilient, organisations must be able to respond to attacks. We conclude that the unique role of the cybersecurity leader warrants targeted qualitative research.

Second, this improved set of competencies in Table 3 provides researchers with a targeted set of learning objectives for cybersecurity leadership education, enabling research into the best educational methods to achieve those objectives.

The improved set of learning outcomes is also valuable for educational *practice* because it can form the basis of curriculum design for cybersecurity management or information security management courses. Outside of education providers, the improved set of competencies is valuable for organisations looking to design or improve their cybersecurity function, and for individuals who wish to move into cybersecurity leadership. Indeed, identifying these competencies is critical to recruitment and professional development – both for organisations and aspiring leaders.

References

Aguas, T., Kark, K., & François, M. (2016). *The new CISO: Leading the strategic security organization*. Deloitte Insights. https://www2.deloitte.com/content/www/us/en/insights/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

Ahmad, A., Maynard, S. B., Motahhir, S., & Alshaikh, M. (2020). Teaching Information Security Management Using an Incident of Intellectual Property Leakage. *ACIS 2020 Proceedings*. https://aisel.aisnet.org/acis2020/36

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370. https://doi.org/10.1007/s10845-012-0683-0

Alexander, A., & Cummings, J. (2016). The Rise of the Chief Information Security Officer. *People & Strategy*, *39*(1), 10–14.

Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the Chief Information Security Officer Organization. *Software Engineering Institute*. https://doi.org/10.1184/R1/6584423.v1

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, *39*, 396–405. https://doi.org/10.1016/j.cose.2013.09.004

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

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Choi, M. (2016). Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. *Sustainability*, *8*(7), 638. https://doi.org/10.3390/su8070638

Cleveland, S., & Cleveland, M. (2018). Toward Cybersecurity Leadership Framework. *MWAIS 2018 Proceedings*. https://aisel.aisnet.org/mwais2018/49

Dawson, M., Burrell, D., Rahim, E., & Brewster, S. (2010). Examining the Role of the Chief Information Security Officer. *Journal of Information Systems Technology and Planning*, *3*, 1–5.

Eraut, M. (1994). *Developing Professional Knowledge and Competence*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/unimelb/detail.action?docID=167243

Fitzgerald, T. (2007). Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other. *Information Systems Security*, *16*(5), 257–263. https://doi.org/10.1080/10658980701746577

Gonczi, A., Hager, P., & Oliver, L. (1990). *Establishing competency-based standards in the professions*. Department of Employment, Education and Training. https://www.voced.edu.au/content/ngv%3A29478

Gupta, D. (2021, August 17). *Council Post: The Role Of A CISO In Building A Modern Cybersecurity Culture*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/08/17/the-role-of-a-ciso-in-building-a-modern-cybersecurity-culture/

Hallett, J., Larson, R., & Rashid, A. (2018). *Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks*. 9. https://www.usenix.org/conference/ase18/presentation/hallett

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585–591. https://doi.org/10.1016/j.bushor.2016.07.004

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Kappers, W. M., & Harrell, N. (2020). From Degree to Chief Information Security Officer (CISO): A Framework for Consideration. *The Journal of Applied Business and Economics*, *22*(11), 260–288.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*, *25*(3), 300–329. https://doi.org/10.1108/ICS-02-2016-0013

Karanja, E., & Rosso, M. A. (2017). The Chief Information Security Officer: An Exploratory Study. *Journal of International Technology & Information Management*, *26*(2), 23–47.

Lanz, J. (2017). The Chief Information Security Officer: The New CFO of Information Security. *CPA Journal*, *87*(6), 52–57.

Loman, M., Gallagher, S., & Ajjan, A. (2021, July 4). Independence Day: REvil uses supply chain exploit to attack hundreds of businesses. *Sophos News*. https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/

Lovejoy, K., Burg, D., Maddison, M., & Watson, R. (2021). *Cybersecurity: How do you rise above the waves of a perfect storm?* Ernst & Young. https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

Marotta, A., & Pearlson, K. (2019). A Culture of Cybersecurity at Banca Popolare di Sondrio. *AMCIS 2019 Proceedings*. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/24

Maynard, S., Onibere, M., & Ahmad, A. (2018). Defining the Strategic Role of the Chief Information Security Officer. *Pacific Asia Journal of the Association for Information Systems*, *10*(3). https://doi.org/10.17705/1pais.10303

Monzelo, P., & Nunes, S. (2019). The Role of the Chief Information Security Officer (CISO) in Organizations. *CAPSI 2019 Proceedings*. https://aisel.aisnet.org/capsi2019/36

Schön, D. A. (1983). *The Reflective Practitioner: How Professionals Think in Action*. Routledge. https://doi.org/10.4324/9781315237473

Shayo, C., & Lin, F. (2019). An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. *Journal of Computer Science and Information Technology*, *7*(1), 1–20. https://doi.org/10.15640/jcsit.v7n1a1

Tejay, G., & Winkfield, M. (2015). How CISOs Can Become Effective Leaders? A Path-Goal Approach. *SIG LEAD 2015 Proceedings*. https://aisel.aisnet.org/siglead2015/1

vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. *ECIS 2009 Proceedings*. https://aisel.aisnet.org/ecis2009/161

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

Whitten, D. (2008). The Chief Information Security Officer: An Analysis of the Skills Required for Success. *Journal of Computer Information Systems*, *48*(3), 15–19. https://doi.org/10.1080/08874417.2008.11646017

Winder, D. (2021, July 5). *$70 Million Demanded As REvil Ransomware Attackers Claim 1 Million Systems Hit*. Forbes. https://www.forbes.com/sites/daveywinder/2021/07/05/70-million-demanded-as-revil-ransomware-attackers-claim-1-million-systems-hit/