# What Do We Need to Know about the Chief Information Security Officer?

## A Literature Review and Research Agenda

Zeynep Sahin
Department of Business Information Technology
Pamplin College of Business
Virginia Tech
Pamplin Hall
880 W Campus Drive Suite 1007
Blacksburg, VA 24061
USA
Email: zeyneps@vt.edu

Anthony Vance
Department of Business Information Technology
Pamplin College of Business
Virginia Tech
Pamplin Hall
880 W Campus Drive Suite 1007
Blacksburg, VA 24061
USA
Email: anthony@vance.name

# What Do We Need to Know about the Chief Information Security Officer? A Literature Review and Research Agenda

## Abstract

Since its establishment in the 1990s, the role of chief information security officer (CISO) has become critical to organizations in managing cybersecurity risks. However, despite widespread recognition of the importance of this role in industry, research about CISOs and the problems they face in protecting organizations is nascent. We review the academic and practitioner literature on CISOs to identify existing themes and highlight a range of challenges related to CISOs in which further research is needed, such as establishing legitimacy within C-suite executive teams, appropriate accountability for cybersecurity incidents, CISO turnover, and promoting security in the face of human factors, business realities, and budget constraints. We also propose a research agenda to address these challenges using potential theoretical lenses. In these ways, this study lays the groundwork for future research on CISOs and their essential role in ensuring the cybersecurity of organizations.

Keywords: Chief information security officer (CISO), board of directors, executives, cybersecurity governance, literature review, research agenda

## 1. Introduction

Since the creation of the chief information security officer (CISO) role in the 1990s (Townsend 2021), it has become critical to organizations in mitigating cybersecurity risks (Moon et al. 2018; Steinbart et al. 2018). As of 2024, almost 75% of Fortune 500 companies have a CISO, and virtually all the rest have an equivalent cybersecurity executive role (Morgan 2024). Recognizing the severe consequences of security incidents for organizations, regulators have adopted rules that elevate the CISO role. For example, in 2023, the US Securities and Exchange Commission adopted a cybersecurity rule that requires public companies to designate in their annual reports the management position responsible for cybersecurity risk (typically the CISO), the relevant expertise of this person, and whether this person reports to the board of directors (SEC 2023). As a result, CISOs are increasingly relied on by the chief executive suite (C-suite) and board of directors to inform and execute cybersecurity strategy (Anderson et al. 2022; Da Silva 2022).

However, despite widespread recognition of the importance of this role in industry, research on CISOs and the problems they face in protecting organizations remains nascent. As a result, the challenges and opportunities facing CISOs are little understood by academics, and practice is in need of research that informs challenges facing CISOs (Da Silva and Jensen 2022; Mulgund et al. 2023). Some of these challenges are a lack of recognition of CISOs as legitimate C-suite leaders (BitSight 2019; Lowry et al. 2022), misalignment between cybersecurity and organizational strategy (Loonam et al. 2020), and insufficient allocation of resources for security efforts (Bodin et al. 2005; Johnson and Goetz 2007).

Given the growing importance of the CISO role and the need to understand and address its related challenges, this literature review aims to: (1) describe and integrate academic and practitioner research to report current knowledge about the CISO role, and (2) identify and suggest areas for future research on CISOs to address issues that have important implications for organizations. Accordingly, we investigate the following research questions:

*RQ1: What are the existing themes in the literature on the CISO role?*

*RQ2: What are important opportunities for research on CISOs?*

To explore these research questions, we conducted a systematic review of studies about CISOs in which we identified 30 peer-reviewed academic articles. Given the limited number of academic articles on CISOs, we supplemented these with 29 industry whitepapers that provide primary data on the CISO role. The findings of this review revealed three prominent themes: (1) the place of CISOs in organizational hierarchies and reporting structures, (2) necessary skills and training for CISOs, and (3) CISO roles and responsibilities. We also identified gaps and persistent challenges in the CISO literature, from which we propose a research agenda of several research opportunities for scholars.

This article makes several contributions to research and practice. First, our review presents a unified view of the current state of research on CISOs. This paper not only identifies key themes in the research on CISOs but also highlights research gaps related to managerial and organizational challenges facing CISOs, which are recognized but not directly studied in the literature. Second, we propose a research agenda that includes associated research questions for scholars to address these challenges. Additionally, to inform future research, we suggest theoretical lenses that have potential to provide greater understanding of issues involved. Third, our research offers practical insights for various stakeholders. For CISOs, it proposes solutions to the challenges they face and research directions to address unexamined challenges. For organizations, it provides insights into how CISOs can be better empowered and retained, leading to better cybersecurity outcomes. Finally, for regulators, this paper informs policies and rules to promote the growth and success of the CISO role.

## 2. Background

Although there is no universally accepted definition of the CISO role (Hielscher et al. 2023; Karanja 2017), it is generally recognized as the executive ultimately responsible for managing the cybersecurity risk of the organization (Hielscher et al. 2023; Johnson and Goetz 2007; Karanja and Rosso 2017; Maynard et al. 2018; Moon et al. 2018). The need for an executive leader to manage cybersecurity risk was recognized as early as 1981 by Donn Parker, who noted:

> Another new concept is the information protection officer at the staff vice-president level who has the responsibility for information protection across the entire organization. This function recognizes the widespread use of computers throughout the organization… (1981, p. 89).

However, the implementation of this idea was not realized until 1994, when Citibank created the CISO role in the wake of hackers stealing $10 million in the first publicized online bank robbery (FBI 2014). Citibank's board of directors instructed the CEO to create the "Chief Information Security Officer" role to ensure that such a heist did not happen again and to assure Citibank's major corporate clients of the security of their systems (Townsend 2021). Since then, the CISO role has proliferated across corporations worldwide (Morgan 2024).

As the CISO role has become widespread, its strategic importance has increased in corporations. Part of this importance is due to the increasing frequency of high-profile security incidents and management's growing recognition of cybersecurity risks (Hooper and McKissack

2016). Regulation in the United States has also elevated the importance of the CISO role. For example, in 2017, the New York State Department of Financial Services enacted its influential Cybersecurity Regulation applicable to financial firms with ties to the state, which required that firms designate a CISO to oversee the cybersecurity program and to report in writing to the board of directors at least annually (NYFDS 2017). These rules were updated in 2023 to require CISOs to promptly report material cybersecurity issues directly to the board or CEO (NYDFS 2023). In 2022, the US Federal Trade Commission instituted similar rules for all financial services firms operating in the United States (FTC 2022), and in 2023, the US Securities and Exchange Commission (SEC) further required that all public companies listed on US stock exchanges state in their annual reports whether they have a CISO or equivalent role, the expertise of this person, and whether this person reports to the board of directors (SEC 2023). These and other regulations were aimed at elevating the prominence and strategic importance of CISOs to their firms and stakeholders (Aiello et al. 2023).

Academic interest in the role of CISOs began in 2007[1] with the works by Johnson and Goetz (2007), Rao and Ramachandran (2007)[2], and Whitten (2008), who studied cybersecurity governance and the role of CISOs. However, research on CISO remained sparse until 2017, when an increase of academic studies on CISOs coincided with regulations specifically relating to CISOs (such the NYDFS cybersecurity rules) and increasing security incidents. As shown in Figure 1, the majority of publications on CISOs have appeared after the year 2017. The historical development and evolving regulatory requirements of the CISO role highlight the growing

[1] We excluded Bodin et al. (2005) from our review because it introduces a tool for CISOs, rather than studying the role itself. Please see our description of our literature review scope in the following section.

[2] We likewise exclude Rao and Ramachandran (2007) from our literature review because it does not present empirical findings.

strategic significance of this position. However, despite the rising importance of the CISO role, there is comparatively little research on CISOs and the challenges they face.

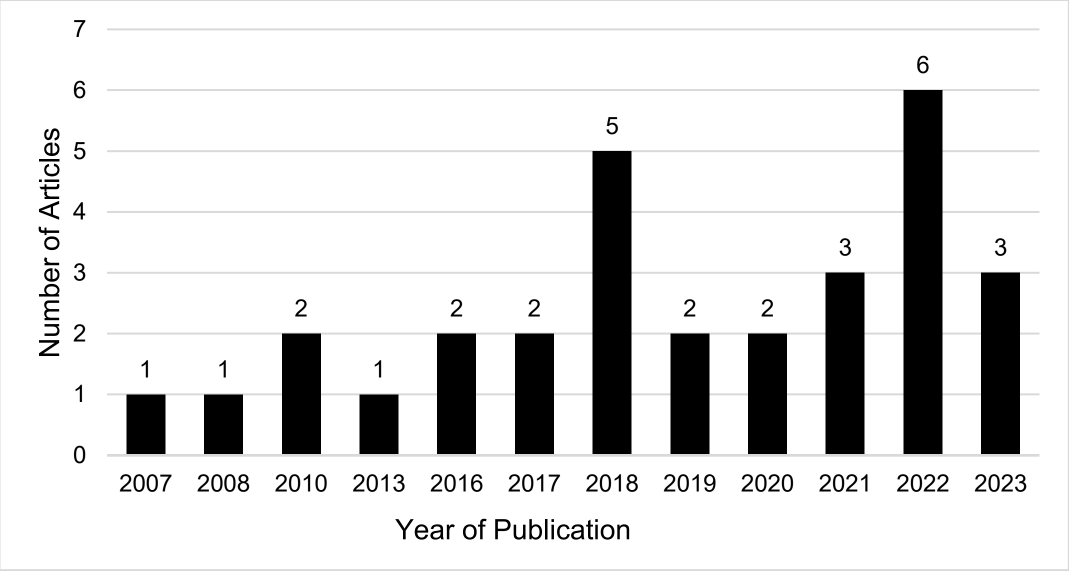

Figure 1 Number of research articles on the CISO role by year

This study differs from previous literature reviews by Anderson et al. (2022), Triplett (2022), and Maynard et al. (2018) which provided valuable insights on cybersecurity leadership. Our study is *narrower* than theirs in *scope* because they considered a range of cybersecurity leaders, including managers, executives, and directors, whereas we specifically focus on CISOs and exclude non-CISO executive positions and mid-level management roles like cybersecurity managers and directors. Conversely, our study is *broader* in *content* because while they examined the role and competencies of cybersecurity leaders (Anderson et al. 2022), the role of cybersecurity leaders in addressing human factors in promoting security (Triplett 2022), and characteristics required for CISOs to become strategists (Maynard et al. 2018), our research provides a comprehensive review of the CISO role unbounded by a single focus or emphasis. Our literature review findings expand beyond those of past reviews to include themes listed in

Table 1. Furthermore, unlike these past reviews, we also provide a research agenda that corresponds to our broader scope of issues facing CISOs (also listed in Table 1).

Table 1 Literature review findings and proposed research agenda

| Themes of literature review on the CISO role |
|---|
| Theme 1: CISOs' place in the organizational hierarchy and reporting structure<br>a. CISO reporting to the CIO<br>b. CISO reporting to an executive outside of IT<br>c. CISO reporting to CEO<br>d. Right CISO reporting structure depends on many factors<br>e. Importance of relationships over hierarchy in the success of CISOs |
| Theme 2: Necessary skills and training for CISOs<br>a. Balancing technical capability and business skills<br>b. Soft skills required for the CISO role<br>c. Career path to CISO |
| Theme 3: CISO roles and responsibilities<br>a. Multifaced roles and responsibilities of CISOs<br>b. Evolving responsibilities of CISOs |
| **Research Agenda of addressing challenges facing CISOs** |
| Opportunity 1: CISOs' challenges in establishing legitimacy and appropriate accountability |
| Opportunity 2: The CISO turnover problem |
| Opportunity 3: CISOs' challenges in ensuring security in the face of human factors, business realities, and budget constraints |

## 3. Literature Review Methodology

Following the typology of literature reviews of Templier and Paré (2015), our literature review falls under the "narrative reviews" type, which "assemble and synthesize extant literature and provide readers with a comprehensive report on the current state of knowledge in the area under investigation" (p. 118). We follow the literature review methodology of Balozian and Leidner (2017) and the guidelines for conducting literature reviews provided by Templier and Paré (2015), which make our study a structured narrative review. This approach enables us to identify relevant articles on the CISO role in a systematic and transparent manner, which facilitates the repeatability of findings and enhances the dependability of the results obtained from the literature search process (Pare et al. 2016; Webster and Watson 2002). Our literature search process is depicted in Figure 2.

We first searched for peer-reviewed academic articles with the words “chief information security officer” or “chief security officer” appearing in the article title, abstract, or keywords in the following academic databases: ProQuest One Business, EBSCO Academic Search Complete, EBSCO Business Source Complete, ScienceDirect, and the AIS Electronic Library. Our search criteria included articles that (1) directly discussed the CISO role, (2) were published in peer-reviewed outlets, and (3) were written in English. We excluded articles that only mentioned the CISO role or were short conference papers with no findings. Dissertations, books, and government documents were also excluded. We did not restrict the article search to any specific time frame, and the last search performed was in September 2023. Following these criteria, we identified 18 unique articles that fit the scope of our study.

We also searched Google Scholar for the words “chief information security officer” or “chief security officer.” This identified an additional 11 articles not previously found in our search of the aforementioned databases. We also performed forward and backward searches and checked the references of the identified articles to ensure the inclusion of all relevant studies (Templier and Paré 2015; Webster and Watson 2002). As a result, we found one additional article. In total, we identified 30 academic peer-reviewed articles examining the CISO role (see Appendix A).

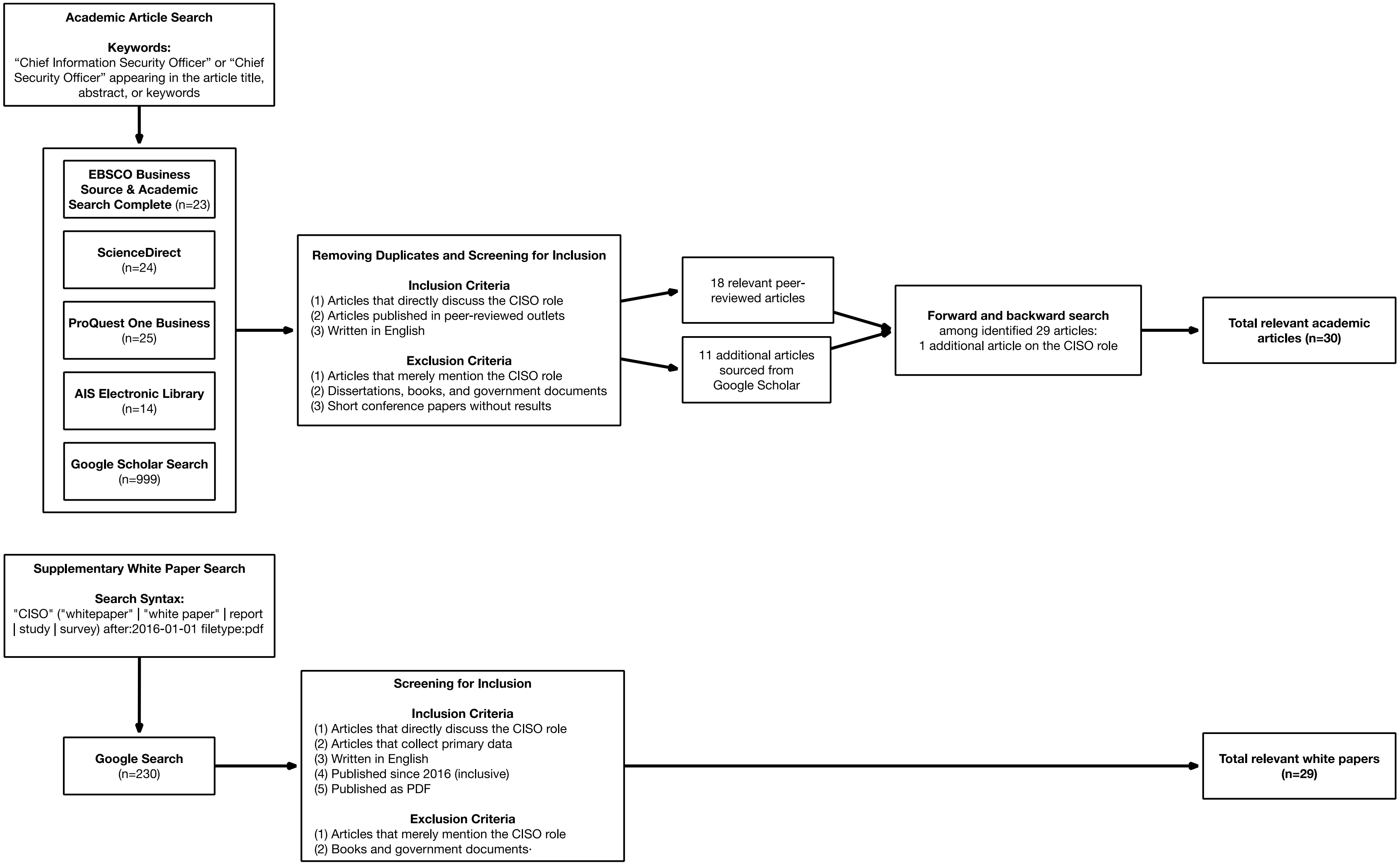
Academic Article Search
Keywords:
“Chief Information Security Officer” or “Chief Security Officer” appearing in the article title, abstract, or keywords
EBSCO Business Source & Academic Search Complete (n=23)
ScienceDirect (n=24)
ProQuest One Business (n=25)
AIS Electronic Library (n=14)
Google Scholar Search (n=999)
Removing Duplicates and Screening for Inclusion
Inclusion Criteria
(1) Articles that directly discuss the CISO role
(2) Articles published in peer-reviewed outlets
(3) Written in English
Exclusion Criteria
(1) Articles that merely mention the CISO role
(2) Dissertations, books, and government documents
(3) Short conference papers without results
18 relevant peer-reviewed articles
11 additional articles sourced from Google Scholar
Forward and backward search
among identified 29 articles:
1 additional article on the CISO role
Total relevant academic articles (n=30)
Supplementary White Paper Search
Search Syntax:
"CISO" ("whitepaper" | "white paper" | report | study | survey) after:2016-01-01 filetype:pdf
Google Search (n=230)
Screening for Inclusion
Inclusion Criteria
(1) Articles that directly discuss the CISO role
(2) Articles that collect primary data
(3) Written in English
(4) Published since 2016 (inclusive)
(5) Published as PDF
Exclusion Criteria
(1) Articles that merely mention the CISO role
(2) Books and government documents·
Total relevant white papers (n=29)

Figure 2 Literature search process

Finally, due to the scarcity of research on the CISO role in academic literature, we included industry whitepapers that use primary data. This addition complements the academic literature and expands the corpus of articles, increasing our knowledge about the CISO role. Our inclusion criteria were whitepapers that (1) directly discussed the CISO role, (2) collected primary data, (3) were written in English, and (4) were published since 2016 (inclusive) to ensure currency. We used the Google search syntax shown in Figure 1 and limited our results to PDF files to find completed publications intended for distribution. The last search was performed in November 2023. This process resulted in 29 whitepapers (see Appendix B).

## 4. Overview of Theories and Methodologies

Of the 30 academic articles identified, eight used a theoretical lens to examine some aspects of the CISO role, as summarized in Table 2. Each of the eight papers applied a different theoretical perspective, mainly from the management discipline, covering concepts ranging from legitimacy and identity work to leadership style. However, there was an absence of explicit theoretical development and progression from one study to another. This presents an opportunity for future research to create a more cohesive body of work that builds on these initial studies and offers practical insights.

Table 2 Theories used in the CISO literature

| Theory and key citations | Description | Application | Citing Article |
|---|---|---|---|
| Agency theory (Eisenhardt 198 9) | Addresses problems that may emerge from the agent–principal relationship, including conflicts of interest and disagreements | Examined the relationships between the CISO (agent)and CEO (principal), and its influence on IT security management | (Karanja 2017) |
| Complexity theory (Anderson 1999; Brodbeck 2002) | Describes how organizations learn and adapt to their | Used to explain how the reporting line of the CISO changes as organizations' cybersecurity situations | (Shayo and Lin 2019) |

| Theory and key citations | Description | Application | Citing Article |
|---|---|---|---|
| | constantly changing environment | change, including their cybersecurity maturity levels and power dynamics | |
| Hobbesian philosophy (Hobbes 1845; Hobbes and Gale 1839) | Argues for centralized power and authority to prevent chaos and maintain social order | Explored the functions and purposes of CISOs within their organizations, including delving into the punitive aspects of cybersecurity and the broader implications of cybersecurity governance in a Leviathan state | (Da Silva 2022) |
| Identity work (Snow and Anderson 1987) | Describes different narrative tactics individuals use to form and uphold their identities | Examined various types of identity work carried out by CISOs that reinforce the CISO-as-soothsayer narrative and connect them to broader security topics | (Da Silva and Jensen 2022) |
| Interaction theory (Markus 1983) | Clarifies how social interactions influence social structures, individual behaviors, and attitudes | Explained how factors related to organizational leaders and factors inherent to the CISO function can influence the CISO reporting line | (Shayo and Lin 2019) |
| Leadership theory (Northouse 2018) | Offers various strategies and outlines leadership responsibilities to improve leadership | Explained different leadership styles required for different stages of NIST's cybersecurity framework | (Cleveland and Cleveland 2018) |
| Legitimacy theory (Bitektine and Haack 2015) | Explains the process of how subjects can gain legitimacy within a social context | Extended to explain contextual factors that enable CISOs to cultivate legitimacy with the C-suite and the board of directors | (Lowry et al. 2022) |
| Organizational discourse analysis model (Hardy et al. 2000) | Explains how discourse can be utilized as a strategic resource to change organizational culture | Used to explain how CISOs' attitude and style in communicating cybersecurity requirements influence their ability to positively influence security behavior | (Ashenden and Sasse 2013) |
| Social capital theory (Nahapiet and Ghoshal 1998) | Posits that social capital is developed through effective interpersonal relationships, which can lead to trust, a shared understanding of beliefs, norms, and values | Explained how social alignment between CISOs and business leaders can lead to improved information systems security effectiveness and organizational performance | (Moon et al. 2018) |

Table 3 presents the research methods used in academic literature on the CISO role. Interviews are the most frequently employed data collection method, likely due to the unexplored nature of CISO research and the limited availability of prior studies. To analyze qualitative data, various analytical approaches were applied, including discourse analysis (Ashenden and Sasse 2013), case studies (Shayo and Lin 2019), and grounded theory (Lowry et al. 2022). Surveys were the next most common method, followed by the literature review and Delphi method.

Table 3 Methodologies used in the academic CISO Literature

| Method | # of Articles | Articles |
|---|---|---|
| Interview | 11 | (Ashenden and Sasse 2013; Da Silva 2022; Da Silva and Jensen 2022; Dor and Elovici 2016; Kayworth and Whitten 2010; Loonam et al. 2020; Lowry et al. 2022; Monzelo and Nunes 2019; Mulgund et al. 2023; Shayo and Lin 2019; Whitten 2008) |
| Survey | 3 | (Cano and Almanza 2023; Moon et al. 2018; Steinbart et al. 2018) |
| Literature review | 3 | (Anderson et al. 2022; Maynard et al. 2018; Triplett 2022) |
| Archival document analysis | 2 | (Hooper and McKissack 2016; Johnson and Goetz 2007) |
| Multimethod (Delphi study + quantitative content analysis) | 2 | (Smit et al. 2021; van Yperen Hagedoorn et al. 2021) |
| Multimethod (Delphi study + survey) | 1 | (Kappers and Harrell 2020) |
| Delphi study | 1 | (Dhillon et al. 2021) |
| Event study | 1 | (Karanja and Rosso 2017) |
| Qualitative content analysis | 1 | (Karanja 2017) |
| Action research | 1 | (Hielscher et al. 2023) |
| Text mining | 1 | (Zwilling 2022) |

In the practitioner literature, surveys were mostly used, followed by interviews and a multimethod approach combining the two (Table 4). Whitepapers mainly focused on global samples that included CISOs, board members, and other executives from various countries, whereas the data sources for academic articles were predominantly from organizations based in the United States.

Table 4 Methodologies used in the whitepapers

| Method | # of Articles | Articles |
|---|---|---|
| Survey | 19 | (Aguas et al. 2016; Aiello et al. 2021; Aiello et al. 2023; Aiello and Thompson 2020; BT 2021; ECSO 2021; EY 2020; Fortinet 2019; Gartner 2020; Haworth 2020; Infosys 2019; Kaspersky 2019; KPMG 2019; Milica 2021; Oltsik 2020; Proofpoint 2020; PwC 2020; PwC 2021; Salt 2023) |
| Interview | 7 | (Eichenwald et al. 2021; F-Secure 2021; GAO 2016; KPMG 2021; McGraw et al. 2017; Phelphs et al. 2019; Ponemon 2017) |
| Multimethod (Interview + survey) | 3 | (Guenther 2019; Kaspersky 2018; Milica 2022) |

## 5. Themes of the CISO Literature

From our review, we identified three broad themes in the academic literature related to CISOs: (1) CISOs' place in the organizational hierarchy and reporting structure, which involves debates over the CISO role's placement within the organizational hierarchy; (2) necessary skills and training for CISOs detailing what is required for their success; and (3) the CISO's roles and responsibilities, highlighting the multifaceted and changing nature of the position. The frequency of these themes across the articles in our review is shown in Table 5. In this section, we will discuss each theme in turn.

Table 5 Frequency of CISO themes across the academic and practitioner literature

| Literature type | Theme 1: CISOs' Place in Organizational Hierarchy and Reporting Structure | Theme 2: Necessary Skills and Training for CISOs | Theme 3: The CISO Roles and Responsibilities |
|---|---|---|---|
| Academic | 14 | 13 | 20 |
| Practitioner | 20 | 19 | 25 |
| Total | 34 | 32 | 45 |

Note: Articles may address multiple themes.

### 5.1. CISOs' Place in Organizational Hierarchy and Reporting Structure

A prominent theme that emerged in our review was the seemingly innocuous question of what the reporting line for the CISO should be. Yet, both academic and practitioner articles in our review highlighted the importance of the reporting line for the success of the CISO and the security of the organization (e.g., F-Secure 2021 and Steinbart et al. 2018). For example, a survey revealed that approximately 59% of 1400 global CISOs believe that their reporting line hinders their job performance and effectiveness within their organizations (Milica 2021).

Part of the issue is that the CISO role should be at a sufficiently senior level in the organizational chart in order to be recognized by other C-suite executives, which allows for easy collaboration among them (Aiello and Schneidermeye 2016; KPMG 2021). A senior position also empowers the CISOs to influence other senior managers and enforce security policies (Kaspersky 2018). Conversely, placing the CISO role several levels down from the C-suite can hamper the effectiveness of the CISO by inhibiting their ability to join the decision-making process and have the requisite authority to implement cybersecurity initiatives (Eichenwald et al. 2021).

Despite general agreement on the need for seniority of the CISO, we found diverse opinions about to whom the CISO should report. We note that this debate precedes the advent of the role of CISO. Parker (1981) described various possible reporting relationships for the "computer security function," and Straub (1988) reported different placements of the "computer security officer" (a precursor to a CISO role) in organizations and argued for the need for this role to be independent and "positioned as high in the organization as possible" (p. 190). These arguments have continued to the present (as described below), indicating that this perennial debate has yet to find an adequate resolution.

### *5.1.1. CISO–CIO*

One of the more common reporting line configurations is the CISO reporting to the CIO, especially for organizations that have long had a CISO (Karanja and Rosso 2017). When organizational leaders are technophobic, CISOs often report to CIOs because of the expectation of top management that the CIO will oversee technical as well as cybersecurity issues (Lanz 2017). Some articles highlight the advantages of CISO reporting the CIO, such as both the CIO and CISO understand technical jargon and there is an opportunity for closer collaboration and integration of security within IT functions, without hindering IT service (Shayo and Lin 2019). Moreover, Loonam et al. (2020) suggested that having CISOs report to the CIO can be beneficial in terms of obtaining buy-in from senior leaders for security initiatives. This is because CIOs are trusted partners at the top management level and are knowledgeable about both business and technology.

However, Kappelman et al. (2019) and Johnson et al. (2023) indicated a decrease in the CISO–CIO reporting configuration in recent years, which may be due to several criticisms raised in the literature. First, having the CISO report to the CIO poses a potential conflict of interest because the CISO audits the work of the CIO and therefore may be pressured by the CIO to overlook or fail to report vulnerabilities related to the CIO's initiatives (Aiello and

Schneidermeye 2016). For this reason, the CISO–CIO reporting configuration could make organizations less secure. As observed by Melissa Hathaway, former senior director of cyberspace for the National Security Council,

> The CISO is responsible for keeping the enterprise safe, and the CIO is responsible for keeping the enterprise running 24/7, so there can be an inherent conflict. [Cybersecurity] should be a shared decision in the C-suite with the CEO playing a key role. (Alexander and Cummings 2016, p. 11).

Additionally, the CISO–CIO reporting line can be overwhelming for CIOs who already have many responsibilities (Beatty et al. 2005; Shayo and Lin 2019). Moreover, CIOs might be hesitant to have the CISO report to them, fearing potential job loss in the event of a security incident. Similarly, the entire C-suite might prefer that the CISO report to lower organizational tiers to insulate them from security incidents (Shayo and Lin 2019). In addition, according to the literature, the CISO–CIO reporting line may lead to security budgetary constraints, because both the IT and security functions could draw from the same budget, and with numerous IT needs, the security budget might suffer (Hooper and McKissack 2016; Johnson and Goetz 2007). In addition, in a scenario where the CISO indirectly reports to the CEO—with the CISO reporting to the CIO and the CIO reporting to the CEO—the CISO might be less likely to disclose security shortcomings, since such disclosures could portray the CIO in a negative way, which in turn might result in the CEO allocating a smaller security budget, given their lack of awareness about the firm's true security posture (Karanja 2017; Kayworth and Whitten 2010). This could persist until a major security incident draws their attention (Hooper and McKissack 2016).

### *5.1.2. CISO Reporting to an Executive Outside of IT*

Although the CISO–CIO reporting line is historically popular, Aiello et al. (2021) reported that in a global survey of 354 CISOs, 62% reported to a role other than the CIO, such as the chief operating officer (COO), chief risk officer (CRO), or general counsel. Steinbart et al. (2018) drew parallels to the findings of San Miguel and Govindarajan (1984), who indicated that controllers with independent reporting relationships are more focused on efficiency and effectiveness in auditing activities. Steinbart et al. (2018) argued that a similar effect is seen in cybersecurity management. They suggested that when a CISO reports to an executive outside of the technology function, it leads to a shift in internal auditors' focus—away from mere compliance and toward substantive process improvements. Therefore, they advocated that CISOs have an independent reporting line and asserted that, since cybersecurity risks are enterprise-level risks, not just technical issues, CISOs should report directly to the CEO, the CRO, or another executive tasked with managing risks.

### *5.1.3. CISO–CEO*

Kappelman et al. (2019) and Johnson et al. (2023) described an increase in the CISO–CEO reporting line in recent years, which has several advantages. This CISO–CEO reporting structure is commonly seen in organizations where CISOs work independently and focus on high-level security strategies (Hooper and McKissack 2016). According to Shayo and Lin (2019) several factors determine whether the CISO reports directly to the CEO. These include the organization's cybersecurity maturity level, how both CISOs and CEOs perceive security threats, the CISO's understanding of the business, and the CEO's knowledge of cybersecurity. Newly created CISO positions tend to report to the CEO more frequently, while pre-existing ones report to the CIO (Karanja and Rosso 2017). Additionally, companies tend to hire their first CISOs after experiencing a security breach and establish a direct reporting line with the CEO or CIO (Karanja 2017).

### *5.1.4. The Right CISO Reporting Structure Depends on Many Factors*

Some academic articles argue that there is no one-size-fits-all reporting structure for the CISO role that would work for all organizations. According to Shayo and Lin (2019), the ideal reporting structure for the CISO role depends on various firm characteristics, such as the organization's industry, cybersecurity maturity level, culture, risk exposure, power dynamics, trust orientation, and resource capabilities. It also depends on executive characteristics, such as the CEO's approach to cybersecurity and the CISO's understanding of the business and its ability to communicate in business terms. Additionally, drawing on complexity theory, they posit that the reporting structure needs to be adjusted according to changes in cybersecurity posture. This idea was supported by Johnson and Goetz (2007) who argued that structuring the security function depends on changes to the company's operational and regulatory environment, business goals, and external threats. Other factors that can influence the reporting structure of the CISO role include geography, company size, CISO tenure, and IT complexity (Kaspersky 2018).

### *5.1.5. Importance of Relationships over Hierarchy in the Success of CISOs*

In contrast to arguments for specific reporting lines for the CISO, other studies have contended that the strength of the CISO's relationships within the organization is much more important. For example, drawing on social capital theory, Moon et al. (2018) proposed a research model that explains how the relational leadership of CISOs results in social alignment with business executives, which leads to integrated knowledge, which in turn positively impacts the effectiveness of cybersecurity management. Similarly, Gartner (2020) emphasized the importance of relationships over an optimum reporting line, stating that the quality of relationships among the CISO, board, and executives is the most important factor of the CISO's effectiveness. In addition, Ashenden and Sasse (2013) found that CISOs' influence is also a function of their relationships with employees of the organization.

In summary, the optimal reporting structure for the CISO role is a highly debated topic, and many CISOs today believe that their reporting lines influence their success. Although CISOs have predominantly reported to CIOs due to technical affinity, this can lead to conflicts of interest. For this reason, there is an emerging trend of CISOs reporting to roles outside of the CIO, such as COOs or CROs, which underscores the shift toward treating security risks as enterprise-level concerns. There is a growing sentiment that CISOs should be at the executive level for effective collaboration with C-suite executives, with an increasing number of CISOs reporting directly to CEOs. However, the ideal reporting structure depends on specific company and industry characteristics, and the quality of relationships with upper management and employees often plays a more crucial role in determining CISO success than mere hierarchical placement.

## 5.2. Necessary Skills and Training for CISOs

Another major theme that emerged from our literature review is necessary skills and training for CISOs to be effective, appearing in 13 academic and 19 practitioner articles. This is reasonable because of the criticality of the CISO role, as well as its developing nature.

### *5.2.1. Balancing Technical Capability and Business Skills*

To combat sophisticated security threats, CISOs must possess a deep understanding of technology and how to secure it (Aiello et al. 2023; Zwilling 2022). Although technical knowledge is essential, it is only a part of the CISO role (Kouns and Kouns 2011). Because it is difficult, if not impossible, to separate the technical and business aspects of cybersecurity today, CISOs need to understand the business risks of the organizations they protect (F-Secure 2021). In particular, it is necessary for CISOs to be able to evaluate the cybersecurity, legal, regulatory, and business impacts of security initiatives to support business executives in decision-making, resources allocation, and risk management (Aguas et al. 2016; Anderson et al. 2022; Kouns and Kouns 2011). In addition, CISOs' understanding of business risks is foundational to forming strong relationships with C-suite executives (F-Secure 2021). CISOs with strong business skills also result in better alignment of cybersecurity and business goals (Kappers and Harrell 2020). Boards also expect business-oriented reports from CISOs (Vijayan 2017).

Anderson et al. (2022) state that risk management is the most frequently mentioned skill for CISOs and that they are generally characterized as risk managers. For this reason, CISOs may be more attuned to business risks and needs than some CIOs. However, "cybersecurity leaders must understand risk holistically, even while others may conceptualize cyber risk narrowly as a technological problem" (Anderson et al. 2022, p. 10). Unfortunately, "while most CISOs have strong technical skills, with computer science and computer engineering backgrounds, they have been found to lack business and leadership acumen especially when it comes to increasing visibility into threats, listening to the voice of the end users of business applications, and articulating clearly understood solutions to senior management and the board" (Shayo and Lin 2019, p. 3).

Furthermore, many CISOs mainly focus on the technical aspects of cybersecurity and therefore miss the wider range of business risks and the opportunity to build relationships with C-suite executives (Alexander and Cummings 2016; Lowry et al. 2022). Underscoring this point, Moon et al. (2018) showed that the CISO's technical expertise can negatively impact the creation of integrated knowledge between business and cybersecurity leaders and information security system (ISS) effectiveness. They stated, “The more technical knowledge the CSO possessed, the weaker the relationship between integrated knowledge and ISS effectiveness” (p. 62).

Furthermore, the increasing sophistication and changing nature of the threat landscape necessitate organizations to develop agile security strategies, which, in turn, require CISOs to function as strategists (Anderson et al. 2022; Maynard et al. 2018). There is general consensus in the literature that CISOs should have a good understanding of their organization’s strategy, create and execute a cybersecurity strategy that aligns with the overall organizational strategy, and efficiently allocate resources to support that strategy (Anderson et al. 2022; Fitzgerald 2007; Loonam et al. 2020; Maynard et al. 2018). However, in an industry survey, only 40% of 130 IT security professionals indicated that the CISO/CSO or the security team develop their cybersecurity strategies, and 60% reported that IT, executive leadership, or compliance departments develop cybersecurity strategies (Navisite 2021).

### *5.2.2. Soft Skills Required for the CISO Role*

As the CISO position becomes more strategic and leadership-focused, soft skills, referring to the essential skills for successful interpersonal interactions, have become necessary for CISOs (Anderson et al. 2022; Cano and Almanza 2023; Smit et al. 2021; van Yperen Hagedoorn et al. 2021). Several academic studies have identified soft skills that are particularly important for CISOs. For example, according to a Delphi study with Dutch CISOs conducted by Smit et al. (2021), the three most important soft skills are leadership, communication, and interpersonal skills. Since CISOs are characterized as educators, strategists, negotiators, interpreters, leaders, facilitators, and change agents (Cano and Almanza 2023; Kouns and Kouns 2011), the ability to communicate is essential for success in this role (Anderson et al. 2022; Cano and Almanza 2023; Hooper and McKissack 2016; Petersen 2006). Moreover, effective communication is vital to align security and business objectives and to avoid relegating security to a purely technical function (Maynard et al. 2018).

Other crucial soft skills include the ability to maintain a calm, decisive, and authoritative mien in a time of crisis (Dawson et al. 2010), along with "a strong work ethic, positive attitude, time management abilities, problem-solving skills, team player, self-confidence, and flexibility/adaptability" (Kouns and Kouns 2011, pp. 57-59). In addition, given their executive leadership role, it is important for CISOs to be able to present effectively, excel in public speaking, and possess strong political skills (Whitten 2008).

### *5.2.3. Career Path to CISO*

Practitioner articles argue that CISOs do not have to come from the same background (Neville-Neil 2019), as there are different types of CISOs, including "legacy CISO, compliance CISO, cyber specialist CISO, enterprise CISO, product CISO" (Aiello and Schneidermeye 2016, p. 4), as well as "traditional security leader, risk/trust leader, and CISO plus, who has technical and risk management skills" (Aiello and Thompson 2020, p. 8). Skills and backgrounds also vary by industry. For instance, the financial services sector prefers CISOs who blend security with business strategy or have a keen understanding of regulatory issues, while the defense sector typically seeks "techie-turned executives," who are engineering-focused technological experts (Alexander and Cummings 2016). Despite these differences, a survey revealed that nearly half of 262 CISOs from different global regions identified themselves as "technical cyber leaders" with backgrounds in software and engineering-related fields (Aiello et al. 2023, p. 8). These CISOs spent significant portions of their careers in technical roles. In contrast, only 1% of CISOs devoted a substantial part of their careers to compliance, suggesting that regulatory compliance alone does not lead to the CISO position.

Individuals aspiring to advance into the CISO role face difficulty finding leadership education that is specifically tailored to the required skill set of this role (Anderson et al. 2022; Kappers and Harrell 2020). Thus, generally, industry certificates, such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), and Certified Information Security Manager (CISM), might be the only recognition of these skills (Kappers and Harrell 2020). However, these certifications are not enough to fulfill any C-suite role, as they solely focus on the technical aspects of cybersecurity (Anderson et al. 2022). Therefore, educational institutions must also address business and strategic skills in their training of cybersecurity students (Kappers and Harrell 2020).

## 5.3. CISO Roles and Responsibilities

In this section, we discuss the third theme, CISO roles and responsibilities, which is the most frequently addressed theme in academic articles and whitepapers. This highlights the importance of understanding the clear boundaries and expectations of CISOs, given the dynamic and complex nature of the cybersecurity field.

### *5.3.1. Multifaced Roles and Responsibilities of CISOs*

Conventionally, the responsibilities of CISOs include managing cybersecurity policies; ensuring adherence to regulatory requirements and standards; supervising security education, training, and awareness (SETA) programs; handling risk management, incident response, and disaster recovery plans; and collaborating with business executives (Anderson et al. 2022; Hooper and McKissack 2016; Kayworth and Whitten 2010; Monzelo and Nunes 2019; Whitten 2008). Kayworth and Whitten (2010) distilled the work of the CISO into three goals: "finding a balance between protecting information assets and facilitating business operations, ensuring adherence to regulations, and preserving alignment with the company's culture" (p. 163).

The academic literature characterizes the CISO role in various ways, such as “CISO as strategic advisor,” in which CISOs advise and educate executives and boards on cybersecurity (Cano and Almanza 2023); “CISO as educator” (Da Silva 2022), in which they guide understanding of cybersecurity; “CISO as soothsayer,” which involves interpreting the mystical, unknown, and fearful aspects of cybersecurity to those unfamiliar with the field (Da Silva and Jensen 2022). For business leaders, cybersecurity can seem like a foreign language. Thus, CISOs must serve as translators of cybersecurity risks into terms that resonate with business objectives (Anderson et al. 2022; Fitzgerald 2007; Hooper and McKissack 2016). This role of translator is necessary to garner the support of business leaders and secure funding for security projects (Maynard et al. 2018).

### *5.3.2. Evolving Responsibilities of CISOs*

Alexander and Cummings (2016) noted that “the only constant for today’s CISOs is change” (p. 11). The roles and responsibilities of CISOs are constantly changing as the technology, threat environment, and regulatory requirements evolve. The expansion of responsibilities has been identified as a stressor for CISOs (Mulgund et al. 2023). In particular, the CISO role has shifted to become more business-focused, with a greater emphasis on collaboration with business executives and the board of directors, rather than just the CIO (Cano and Almanza 2023; Rosiek 2018).

According to Kaspersky (2019), the most significant change is the shift from tactical defense to strategic risk management. CISOs are increasingly expected to function as a strategist who constantly monitors and analyzes emerging threats and actively searches for new opportunities to avoid and respond to security incidents rather than just reacting operationally (Cano and Almanza 2023; Maynard et al. 2018). CISOs also ensure that security strategies are aligned with business goals, prioritizing resources accordingly (Anderson et al. 2022; Cano and Almanza 2023; Kappers and Harrell 2020).

Moreover, with the digitalization of organizations, CISOs have become stewards of digital trust (PwC 2021). In particular, with the surge of data usage and associated data protection enforcement worldwide, CISOs' roles and responsibilities in privacy protection and regulated activities have expanded. For example, an interview study of 28 CISOs from the United States and Europe revealed that the majority of US and European CISOs have experienced a significant increase in their responsibilities related to privacy regulatory enforcement activities (F-Secure 2021).

## 6. Research Agenda

Most of the articles reviewed in the previous section recognize challenges facing CISOs, but do not investigate them in depth or provide needed solutions. In this section, we outline a research agenda to address important gaps in the first and third themes ("CISOs' place in the organizational hierarchy and reporting structure" and "CISO roles and responsibilities") discussed in Sections 5.1 and 5.3 above.[3] We suggest potential future research questions and propose useful theories, explaining how they can be applied to address the identified challenges.

### 6.1. CISOs' Challenge in Establishing Legitimacy and Appropriate Accountability

Extending the first theme of the literature review, this section proposes future research directions regarding the challenges CISOs face due to a lack of consensus about their integral

[3] This is not to suggest that there are no worthwhile opportunities for future research within Theme 2 "Necessary skills and training for CISOs." However, without stable and empowered positions, power and authority, etc., CISOs struggle to employ their skills (Kaspersky 2018; Lowry et al. 2022) and can be scapegoated due to security incidents (Karanja 2017; Shayo and Lin 2019). Therefore, researching these issues should be prioritized to ensure that full benefit of CISOs' skills and training is realized.

role and authority within the C-suite executive team. This uncertainty leads to organizational and political challenges, particularly in terms of perceived legitimacy and accountability in the event of security failures, representing important research gaps.

#### *6.1.1. CISOs' Perceived Legitimacy in Organizations*

CISOs' lack of power, credibility, and role identity in their organizations poses serious challenges in performing their roles (Ashenden and Sasse 2013; Hielscher et al. 2023; Mulgund et al. 2023). While CISOs have the word "chief" in their title, they are seen primarily as second-tier executives principally concerned with managing downside risk. There is also no consensus on the strategic role of CISOs within the C-suite executive team (Lowry et al. 2022). CISOs are generally subordinates of CIOs (Haislip et al. 2021) or positioned two or more levels below C-suite executives (Shayo and Lin 2019), and thus, enjoy less credibility and power among C-level executives (Ashenden and Sasse 2013; Karanja 2017; Karanja and Rosso 2017; Shayo and Lin 2019). Lowry et al. (2022) indicated that CISOs can gain legitimacy with boards and executives by building relationships with them. In a virtuous cycle, as CISOs gain legitimacy with boards through proactive interactions and engagement, boards update their perceptions of the legitimacy of the CISOs, which leads to further interactions and opportunities for engagement. This in turn strengthens CISOs' efforts to gain legitimacy within the executive suite, and vice versa.

However, frequent turnover and short tenures among CISOs hinder their ability to build relationships with boards and executives (Haworth 2020; Kaspersky 2018; Sullivan 2022), which can complicate their legitimization process (Lowry et al. 2022). This pattern underscores the need for research into how turnover impacts CISO legitimacy. To address this research question, legitimacy theory can be used, which posits that individuals can earn legitimacy by gaining the trust of their aspirational peer groups through building relationships (Bitektine and Haack 2015; Tost 2011).

Nevertheless, recent studies from both academic (Lowry et al. 2023) and practitioner (Haworth 2019; Haworth 2020) perspectives involving board of directors and CISOs revealed that CISOs struggle to build relationships with boards. This is due to limited access, communication gaps, and a mutual lack of expertise in both cybersecurity and business. Furthermore, these studies stated that there is confusion among board members regarding their oversight of cybersecurity. Since cybersecurity is a relatively new topic for boards, they are unsure about how to best collaborate with CISOs (Hielscher et al. 2023; Mulgund et al. 2023). This issue raises another research question about the relationship dynamics between CISOs and boards that future studies should examine.

Agency theory, which primarily focuses on the dynamics between a principal (those who delegate authority) and an agent (those to whom authority is delegated) who collaborate but have distinct approaches and interests, is particularly useful in situations where it is difficult for the principal to oversee the actions of the agent (Eisenhardt 1989). In this regard, agency theory can be used to assess how information environments function in reducing information asymmetry and conflicts of interest and enhance trust and accountability in decision-making (Eisenhardt 1989; Fama 1980). In the context of CISO–board relations, in which boards act as principals and CISOs as agents, future research should probe effective governance practices. This includes establishing clear reporting lines and communication channels between the board of directors and the CISOs.

Future studies should also investigate the impact of the CISO's presence in the C-suite executive team on cybersecurity outcomes. In this regard, upper echelon theory (UET) can be a useful theoretical lens. UET posits that executives' influence on organizational outcomes depends on their power and experience (Carpenter et al. 2004; Hambrick 2007; Hambrick and Mason 1984). Given that CISOs possess unique domain expertise but often lack adequate authority to effectively employ their knowledge, they are not able to fully leverage their expertise in corporate decision-making (Ashenden and Sasse 2013; Karanja 2017; Maynard et al. 2018). UET also posits that reporting lines can enhance interactions and foster synergistic cognitive capabilities among executives, ultimately leading to improved organizational outcomes. Therefore, drawing on UET, future studies should examine how CISOs' involvement in C-suite executive teams influences cybersecurity outcomes. These research opportunities are summarized in Table 6.

Table 6 Future research directions for establishing CISO role legitimacy

| Gaps in the Research | Suggested Theories | Research Questions |
|---|---|---|
| CISO turnover, the CISO legitimating process | Legitimacy Theory | How does CISO turnover influence CISO legitimacy? |
| Factors that influence the CISO–board relationship | Agency Theory | How can the relationship between the CISO and board of directors be improved? |
| CISOs' presence in the C-suite executive team and its impact on cybersecurity outcomes | Upper Echelon Theory | How does CISOs' involvement in C-suite executive teams influence cybersecurity outcomes? |

### *6.1.2. CISOs as Scapegoats*

Both academic and practitioner articles indicate that there is no clear consensus on the CISOs' integral role within the top management team, their exact role and authority within a company, or the extent of their responsibility when security failures occur (Karanja 2017). Consequently, there are concerns about CISOs being unfairly blamed for cybersecurity incidents and facing potential legal actions due to such incidents (Salt 2023). The recent surge in high-profile legal cases involving CISOs has heightened stress levels among these professionals (DOJ 2023; Room 2023; Salt 2023). Many CISOs believe that, while CEOs take responsibility for business risks, they do not take responsibility for security risks (F-Secure 2021), making CISOs easily blamed and dismissed because of security incidents (Drinkwater 2016). According to a survey by ThreatTrack (2015), 44% of 200 C-level executives indicated that CISOs should be held accountable for any data security breach, which leads to the "CISO as scapegoat characterization" (p. 3). Although academic and practitioner articles have acknowledged the vulnerability of CISOs to becoming scapegoats for security incidents, currently, no research specifically addresses this issue. This raises a research question about how various factors may influence CISOs' accountability for cybersecurity incidents, including the characteristics of CISOs themselves (e.g., competence, autonomy, and control over security management), external factors (e.g., regulations on cybersecurity risk ownership and industry type), and organizational factors (e.g., organizational culture, politics, cybersecurity maturity, and CISOs' reporting line).

One theoretical lens that could predict CISOs' accountability for a security incident is attribution theory. This theory posits that people can attribute causes to an event based on either internal factors, such as competence, autonomy, and control over the event, or external factors, such as situational or environmental factors (Heider 1982; Kelley 1967; Malle 2011). In the context of CISOs' accountability for security incidents, accountability could be assessed based on whether a security incident is perceived as being within their control—internal factors such as the CISOs' competence, autonomy, and control over security measures—or influenced by external circumstances that are beyond or less within their control, such as sophisticated cyberattacks or lack of upper management support to prevent the incident. Importantly, the SEC (2023) holds boards responsible for oversight of cybersecurity in the U.S., and National Cyber Security Centre in the U.K. states that "the board is responsible for ensuring that risks to delivering the strategy are identified, evaluated, and mitigated in line with the business risk appetite" (NCSC 2023, p. 12). When a security incident occurs, stakeholders (including boards, executives, customers, and government agencies) are likely to analyze the situation based on these attributions. If the incident is attributed to CISO's lack of competence or poor decision-making—internal factors—the CISO may be assigned the blame. Conversely, competent CISOs might be assigned less blame, as they are likely to have taken all necessary precautions. Alternatively, if external factors such as unforeseeable and unavoidable challenges are deemed the primary cause, the CISO's culpability might be viewed as mitigated. Nevertheless, the literature reviewed above points out that even competent CISOs may be scapegoated and terminated even when taken necessary precautions.

Furthermore, accountability theory (Markman and Tetlock 2000) can also inform our understanding of CISOs' accountability for security incidents. Key considerations can include (1) the cognitive and political threshold—the point at which an incident is deemed unpredictable based on existing knowledge; (2) the appraisal of evidence—this involves assessing threats before and after incidents, with an emphasis on accountability for ignored known vulnerabilities; (3) the informing of the evaluative audience—how CISOs communicate risks to stakeholders, such as executives and board members, where stakeholders who are better informed may have more understanding of incidents; (4) the policymakers' balancing act, which involves assessing the risk of unjust blame versus failure to hold poorly performing CISOs accountable. These elements can shape CISOs' perceived accountability within their organizations. In summary, the accountability of CISOs for security incidents is influenced by a complex interplay of cognitive, political, and organizational factors. Each of these factors can provide a useful focus for future research aimed at improving cybersecurity risk accountability. We summarize these research gaps and research opportunities in Table 7.

Table 7 Future research directions for CISOs' accountability for security incidents

| Gaps in the Research | Suggested Theories | Research Questions |
|---|---|---|
| Specific factors influencing CISOs' accountability for cybersecurity incidents | Attribution theory | How do internal (e.g., CISO characteristics and control over security governance) and external factors (e.g., cybersecurity regulations, industry type) influence CISOs' accountability for cybersecurity incidents? |
| | Accountability theory | What role do cognitive, political, and organizational factors play in shaping the perceived accountability of CISOs within their organizations for cybersecurity incidents? |

### 6.2. The CISO Turnover Problem

Extending the third theme of the literature review, this section proposes future research directions relating to the problem of CISO turnover. The CISO literature reveals that recruiting and retaining CISOs is a growing concern due to the high turnover rates, shortage of CISO talent, and increasing demand  (Aiello et al. 2023; Johnson and Goetz 2007; Rosiek 2018). According to an industry survey, the average CISO tenure is 26 months (Haworth 2020). The departure of a CISO can have several adverse effects on an organization. Given that these executives possess deep insights into the organization's essential security systems, their exit can lead to significant knowledge loss, making the organization vulnerable to cybersecurity threats and potential cyberattacks (Rosiek 2018). Additionally, it may cause disruptions in ongoing cybersecurity projects and necessitate the restructuring of cybersecurity strategies (Johnson and Goetz 2007). Despite recognition in academic articles and whitepapers of the critical issue of CISO turnover, there remains a conspicuous gap in scientific research regarding its determinants and consequences. This absence of empirical study is a pressing concern, demanding scholarly attention to mitigating the risks associated with the CISO churn.

Turnover theory can be used to address this research question. This theory suggests that employees' intention to leave their organization is influenced by a combination of factors, such as job satisfaction; organizational commitment; job characteristics, such as workload and job autonomy; and external factors, such as labor market conditions and job offers (Hom et al. 2017; March and Simon 1958). By using turnover theory, researchers can explore the organizational and external factors leading to CISO turnover, which can provide insights into strategies to reduce CISO churn. Additionally, UET can be another potential theory for investigating the reasons behind CISO turnover. According to UET, the visible traits of organizational leaders, such as age, tenure, education, personality, and position in the company hierarchy, are indicators of their distinct cognitive approaches, beliefs, and values (Hambrick and Mason 1984). These factors can, in turn, impact organizational results, such as employee turnover (Carpenter et al. 2004). Thus, by using UET, researchers can examine how CISO characteristics influence their intention to turnover, as well as its impact on other organizational outcomes, such as security program effectiveness and CISOs' job performance. We summarize these future research directions in Table 8.

Table 8 Future research directions for the problem of CISO turnover

| Gaps in the Research | Suggested Theories | Research Questions |
|---|---|---|
| Antecedents and consequences of CISO turnover, and strategies to reduce the CISO churn | Turnover theory | What are the determinants of CISO turnover?<br>How can CISO turnover be reduced? |
| | Upper echelon theory | How do CISO characteristics influence their turnover intention? |

### 6.3. CISOs' Challenge in Ensuring Security in the Face of Human Factors, Business Realities, and Budget Constraints

Extending the third theme of the literature review in a different direction, this section proposes examining challenges CISOs face in performing their roles, namely fostering a security culture, balancing security with business needs, and addressing budget constraints.

#### *6.3.1. Challenges CISOs Face in Fostering a Security Culture*

Addressing the human factor in cybersecurity presents a persistent challenge for CISOs (Kouns and Kouns 2011; Triplett 2022). In a study conducted by Hielscher et al. (2023), CISOs reported several challenges in creating "human-centered security" within their organizations. These challenges included a lack of understanding of basic human behavior and organizational culture, insufficient support from top management, and failure to communicate effectively with employees and the board of directors. Moreover, CISOs' efforts to promote a security-conscious culture often clash with employee resistance, particularly from middle management, who are pivotal to daily operations (Ashenden and Sasse 2013; Johnson and Goetz 2007).

These findings reveal that cybersecurity is not just an issue that concerns technology and technical experts; it involves the entire organization, its culture, and its leadership (Triplett

2022). In this sense, the support and involvement of top management leadership is paramount; lacking their backing, even well-designed security initiatives may fail to permeate organizational culture, as “senior management sets the tone of the firm’s risk culture through behaviors and attitudes” (Vincent et al. 2019, p. 118). Despite this recognition, research on how CISOs can effectively secure support and commitment from top management is lacking. Future studies should address how CISOs can gain the support and involvement of business leadership, including boards and executives, in creating a security culture.

To investigate these problems, Schein’s (2010) framework on organizational culture and leadership offers valuable insights (Somers 2023). Schein (1999) identifies three cultural levels: visible “artifacts” like policies, deeper “espoused values” that rationalize actions, and core “assumptions” that drive behavior. He emphasizes that leadership is crucial in shaping these elements and, by extension, the entire organizational culture. In this perspective, executives—including the CISO—have a key role in fostering a robust cybersecurity culture. By leveraging recent regulations on board oversight of cybersecurity (Aguilar 2014; SEC 2023), CISOs can enlist support from executives and board members, positioning cybersecurity as a key component of organizational governance and strategic planning. This can help in reshaping assumptions and reinforcing the importance of cybersecurity across the organization. We summarize these future research directions in Table 9.

Table 9 Future research directions for the CISO role in creating security culture

| Gaps in the Research | Suggested Theories | Research Questions |
|---|---|---|
| Strategies for CISOs to effectively obtain support and commitment from business leadership to establish a culture of security | Organizational culture theory | How can CISOs gain business leadership’s support and involvement in creating a security culture? |

### *6.3.2. CISOs' Struggle in Balancing Cybersecurity and Business Needs*

Anderson et al. (2022) described the CISO role as "a balancing act" (p. 11) and suggested that CISOs should strive to find a balance between protecting and sharing information as well as between security and innovation, which sets the CISO role apart from other leadership positions within the IT field. Practitioner articles suggest that CISOs must align IT security with business goals and strategies (Ponemon 2017) and play a pivotal role in integrating security priorities into everyday business operations, thereby driving organizational security needs without hindering functionality (Oracle 2019).

However, finding the right balance has been a significant challenge for CISOs (Kayworth and Whitten 2010; Moon et al. 2018) due to a siloed mindset common among technically oriented CISOs (Hielscher et al. 2023), combined with their challenges in interacting with business executives and boards and a lack of communication channels with them  (Aguas et al. 2016). To better understand the conceptual factors influencing this balance and to identify strategies for navigating these challenges effectively, academic studies should address how CISOs can be perceived as a business enabler and add value to the business strategy and how CISOs can balance security needs and business realities.

To address this issue, CISOs can apply participatory development approaches to security initiatives, tailoring security initiatives and policies to business needs and goals so that the security function is perceived as supportive of business operations rather than obstructive. In this context, Work systems theory (WST;(Alter 2008; Alter 2013) offers valuable insights. WST is a conceptual framework that views organizations as complex systems composed of interrelated components, including people, processes, technology, and the environment, all working together to achieve specific goals. This theory advocates for participatory design principles that emphasize the importance of users' and other stakeholders' involvement and feedback in the design, development, implementation, and improvement of work systems. By applying WST, researchers can explore how CISOs might view security practices as sociotechnical systems that incorporate not only technical elements but also input from stakeholders reflecting social and organizational needs. We summarize these future research directions in Table 10.

Table 10 Future research direction for the CISO role in balancing security requirements and business realities

| Gaps in the Research | Suggested Theories | Research Questions |
|---|---|---|
| The role of CISOs in balancing cybersecurity and business needs | Work system theory | How can CISOs be a business enabler and add value to the business strategy?<br>How can CISOs balance security needs and business realities? |

### *6.3.3. Promoting Security in the Face of Budget Constraints*

Academic and practitioner research has highlighted that CISOs face the dual challenge of addressing rising security threats with limited budgets and communicating their financial needs to business leaders (Kaspersky 2018; Mulgund et al. 2023). This difficulty is exacerbated by the challenge of demonstrating the tangible return on investment for security measures, often recognized only after a breach, leading to budget constraints (Bodin et al. 2005; Kaspersky 2018; Salt 2023). As a result, CISOs often face the question of "How much security is enough?" (Johnson and Goetz 2007, p. 18). Dor and Elovici (2016) presented a framework for making cybersecurity investment decisions, which includes the role of CISOs and can be utilized by them. However, further research is needed to identify the underlying organizational and political factors that may hinder CISOs from accessing organizational resources. Additionally, future studies should examine strategies for CISOs to overcome budget constraints and how these constraints affect the effectiveness of cybersecurity management.

Resource dependence theory can explain the factors that hinder CISOs from accessing organizational resources. This theory suggests that organizations depend on resources to survive and achieve their goals, and that control over resources creates power relationships between organizations (Pfeffer and Salancik 2003). In the context of CISOs' challenge in budget constraints, CISOs may struggle to access organizational resources due to power imbalances and political dynamics within their organizations.

Given that budget constraints can be influenced by organizational and political factors, future studies can also adopt a contingency perspective to understand the factors leading to budget constraints and to explore ways to overcome them. This theory posits that there is no universally best method for managing an organization or for effective leadership; rather, the most effective approach depends on the specific circumstances of each organization (Seyranian 2009). In the context of budget constraints for security initiatives, this theory implies that CISOs need to comprehend the unique needs and circumstances of their organizations and devise strategies to access the necessary organizational resources.

Furthermore, to address the research question of how budget constraints influence the effectiveness of cybersecurity management, resource-based view theory could be utilized. This theory suggests that an organization's resources are the key determinants of its success (Barney 1991). In the context of cybersecurity management, budget constraints can limit CISOs' ability to acquire the required technology and hire staff to effectively manage cybersecurity, which can result in less effectiveness and competitiveness in the growing thereat environment. We summarize these opportunities for future research in Table 11.

Table 11 Future research directions to understand the antecedents and consequences of CISOs' budget constraints

| Gaps in the Research | Suggested Theories | Research Questions |
|---|---|---|
| Factors hindering CISOs to access organizational resources | Resource dependence theory | What organizational and political factors hinder CISOs from accessing organizational resources? |
| Various strategies that CISOs can use to mitigate budget constraints | Contingency theory | How can CISOs overcome budget constraints considering organizations' unique needs and circumstances? |
| The influence of budget constraints on security outcomes | Resource-based view theory | How do budget constraints influence the effectiveness of cybersecurity management? |

## 7. Discussion

Despite the crucial role of CISOs in securing their organizations, as well as the increasing regulatory pressure on organizations to elevate the CISO position, more research is needed on this role. Thus, this study presents a literature review to describe the current state of knowledge on the role of CISO and identifies a related range of issues that should be investigated in future research.

Our research makes several contributions. First, it helps cybersecurity researchers better understand the current state of emerging research on the CISO role, which can have important implications for CISOs, organizations, and regulators. We followed a narrative literature review approach to examine current peer-reviewed academic articles and a broad range of industry whitepapers that collect primary data. Our analysis and synthesis of the literature revealed three themes that emerged from both academic articles and whitepapers (Table 1). This provided a comprehensive and thorough overview of the literature on the CISO role. We also provided an overview of the theories and methodologies used in the existing literature.

Second, we propose a research agenda that identifies the core issues related to CISOs. Highlighting their battle for legitimacy and appropriate accountability, we pave the way for further research aimed at bolstering their status and influence within corporate hierarchies. We bring to light the critical problem of frequent CISO turnover, a threat to organizational stability and security. Moreover, our work acknowledges the intricate balance that CISOs must maintain in advocating for robust security practices amid the complex interplay of human behavior, corporate objectives, and budget limitations. Our proposed future research questions are positioned to inspire a body of work that not only elevates the understanding of these dynamics but also equips CISOs with the knowledge to navigate them effectively, thus contributing to the reinforcement of cybersecurity across industries.

Third, this study goes beyond merely listing the challenges facing CISOs and posing related research questions derived from these challenges. We also offer theoretical perspectives that are not only robust but also flexible enough to guide future research on CISOs. These perspectives are intended to provide a solid foundation and clear direction for future studies, equipping researchers with the theoretical grounding necessary to extend the academic discourse on the role of CISOs.

Our research has significant implications for practice in three key areas. First, CISOs can benefit from our study, as it sheds light on the challenges they face. By highlighting these challenges and proposing future research directions, our study aims to provide insights and guidance that will help CISOs improve their effectiveness within their organizations. This will, in turn, offer significant insights to gain legitimacy within the C-suite executive team, face less personal liability regarding security incidents, better align security initiatives with business objectives, foster a strong security culture, and secure the necessary resources for optimal cybersecurity management. Ultimately, by tackling these challenges, CISOs can contribute to enhanced organizational resilience against security threats and support their organizations' overall success.

Second, our study can contribute to organizations by proposing ways to empower and retain CISOs that possess unique expertise in protecting information assets. By identifying and addressing challenges that CISOs face, our research aims to provide insights for organizations to better support their CISOs. This support can include increasing resources for professional development and supporting security initiatives, facilitating communication channels with business leaders, and promoting a culture of collaboration and accountability throughout the organization. By empowering and retaining skilled CISOs, organizations can benefit from enhanced cybersecurity strategies, more effective security programs, and improved risk management. Ultimately, this leads to better organizational outcomes, including minimized disruptions to operations and stronger protection of critical data and assets.

Last, our research has implications for regulators seeking to elevate the CISO role within organizations. By learning from the current CISO literature and the challenges associated with the CISO role, regulators can better understand the complexities faced by CISOs in today's rapidly evolving security landscape. This understanding can inform the development of more targeted and effective regulations that support the growth and success of CISOs. These could include defining clear accountability structures for security incidents, clarifying CISOs' position within the organizational hierarchy, and promoting board and C-suite executive involvement in cybersecurity governance and accountability.

## 8. Limitations and Future Research Directions

This study is not without limitations. First, research on the CISO role is still emerging, and there are not yet enough empirical studies available to conduct a robust meta-analysis. Meta-analyses are useful for the critical review and statistical evaluation of prior research (Paré et al. 2015). Although there is no consensus about the minimum number of studies required for a meta-analysis (Cram et al. 2019), more quantitative studies on the CISO role are needed. Currently, only seven studies in the existing CISO literature are quantitative or contain a quantitative component. More studies would allow for the examination and comparison of the effects of diverse variables across different research settings with an increased power and reduced bias (Cram et al. 2019).

Moreover, the majority of samples in the current academic literature on CISOs are from the US, where regulations significantly affect the elevation of the CISO role. A study by Vance et al. (2020), grounded in cultural psychology, shows how a nation's culture can impact security policy enforcements within organizations. Hence, more studies are needed to explore the CISO role various cultural settings to uncover how cultural differences and regulatory environment influence the perception of the CISO role, responsibilities, and interactions across different countries and cultures.

Lastly, the relatively narrow range of methodological approaches used in the academic and practitioner articles limits the types of insights that can be obtained. Methodologies such as longitudinal studies, ethnographic research, qualitative comparative analysis, and social network analysis could yield more nuanced insights into the CISO role over time, across different cultural contexts, and in relation to other organizational roles. Furthermore, as previously mentioned, the SEC's 2023 reporting requirements on cybersecurity provide insights into the CISO role in annual reports companies listed on US stock exchanges, including who the CISO reports to and the nature of the CISO's interaction with the board of directors. Analysis of financial reports, which has already been widely adopted in the literature on CIOs (e.g., Bendig et al. 2023; Jingyu et al. 2021), can provide valuable insights into cybersecurity governance practices, the characteristics of CISOs, and their impact on cybersecurity outcomes.

## 9. Conclusion

This study provides a structured narrative literature review of the CISO literature. We identified organizational and managerial challenges facing CISOs that represent important research gaps that should be addressed in future research. Additionally, we suggested theoretical lenses for future research directions that can tackle these challenges. Our study contributes to research and practice by providing an analysis and synthesis of the CISO literature and proposing a research agenda with potential theories. By pursuing this research agenda, scholars can better understand the role of CISOs in improving their retention, support, and overall effectiveness, leading to better cybersecurity outcomes for organizations.

## Funding

This work was supported by a fellowship from the Commonwealth Cyber Initiative of Virginia.

## Appendix A. Academic Literature on the CISO Role

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs' place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 1. | Anderson et al. 2022 | ICIS 2022 Proceedings | Competencies of Cybersecurity Leaders: A Review and Research Agenda | Qualitative content analysis to analyze literature search result | NA | Literature review on the required CISO role competencies | | X | X |
| 2. | Ashenden and Sasse 2013 | Computers & Security | CISOs and Organizational Culture: Their Own Worst Enemy? | Semi-structured interviews with 5 CISOs from UK-based global organizations. | Organizational discourse analysis model by Hardy et al. 2000. | Examines the role of CISOs in creating security awareness and building security culture within organizations | X | | X |
| 3. | Cano and Almanza 2023 | International Conference on Information Technology & Systems | The Information Security Function and the CISO in Colombia: 2010–2020 | Survey with 500 security professionals in Colombia | NA | Explores how CISO role, responsibilities, and place in the organizational chart changed between 2010 and 2020 | X | X | X |
| 4. | Cleveland and Cleveland 2018 | MWAIS 2018 Proceedings | Toward Cybersecurity Leadership Framework | Conceptual | Leadership theory | Explains different leadership styles required for different stages of NIST's cybersecurity framework | | X | |
| 5. | Da Silva 2022 | Computers & Security | Cyber security and the Leviathan | Semi-structured interviews with 15 CISOs and six senior organizational leaders | Hobbesian philosophy | Examines the CISO role in a commercial organization. They especially emphasize the CISOs' role as educators and advisors. | | | X |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs' place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 6. | Da Silva and Jensen 2022 | Proceedings of the on Human-Computer Interaction | "Cyber security is a dark art": The CISO as Soothsayer | Interpretive paradigm to analyze interview data with UK-based 21 CISOs and 6 organizational leaders | Identity work | Examines the CISO role in commercial organizations with a focus on nuances of the position and the CISO work identity | X | | X |
| 7. | Dawson et al. 2010 | Journal of Information Systems Technology and Planning | Examining the Role of The Chief Information Security Officer | Opinion | NA | Discusses CISO role, responsibilities, and skill sets | | X | X |
| 8. | Dhillon et al. 2021 | Journal of Strategic Information Systems | Information Systems Security Research Agenda: Exploring the Gap Between Research and Practice | Literature review on IS security research and Delphi study with 15 CISOs of US companies | NA | A systematic literature review of the cybersecurity research is conducted, and then the results are compared with the major security issues facing CISOs | | | X |
| 9. | Dor and Elovici 2016 | Computers & Security | A Model of The Information Security Investment Decision-Making Process | Grounded theory interview study with 23 cybersecurity experts and decision makers from nine companies | NA | Provides a framework for CISOs to make security investment decisions | | | X |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs’ place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 10. | Hielscher et al. 2023 | 32st USENIX Security Symposium | Employees Who Don’t Accept the Time Security Takes Are Not Aware Enough”: The CISO View of Human-Centered Security | Action research with 33 CISOs in organizations located in Switzerland | NA | Examines CISOs’ effort in providing human-centered security and challenges they face in doing so | | | X |
| 11. | Hooper and McKissack 2016 | Business Horizons | The Emerging Role of the CISO | 100 job postings for CISO positions that were available on three different websites eBizMBA, JobisJob, and Trade Me were analyzed | NA | Studies challenges facing organizations in relation to selecting a candidate CISO | X | | X |
| 12. | Johnson and Goetz 2007 | IEEE Security & Privacy | Embedding Information Security into The Organization | Field study and workshops with IT and security executives from more than 30 Fortune 500 companies | NA | Explores CISO reporting structures, responsibilities, and associated role challenges | X | | X |
| 13. | Kappers and Harrell 2020 | The Journal of Applied Business and Economics | From Degree to Chief Information Security Officer (CISO): A Framework for Consideration | A Delphi study and survey with 21 faculty member participants from a US institution | NA | Examines the gap between required CISO job skills and the content of academic studies | | X | X |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs' place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 14. | Karanja 2017 | Information and Computer Security | The Role of The Chief Information Security Officer in The Management of IT Security | Qualitative content analysis of 12 US firms that experienced security breaches between 2009 and 2015 | Agency theory | Examines CISO role reporting structures of firms experiencing a data security breach between 2009 and 2015 | X | | |
| 15. | Karanja and Rosso 2017 | Journal of International Technology and Information Management | The Chief Information Security Officer: An Exploratory Study | Event study methodology was applied to a dataset that shows firms that hired a CISO between 2010 and 2014, sourced from LexisNexis Academic | NA | Explores the trends of CISO role reporting structure over the period of 2010 and 2014 | X | | |
| 16. | Kayworth and Whitten 2010 | MIS Quarterly Executive | Effective Information Security Requires a Balance of Social and Technology Factors | Interview study with 21 cybersecurity executives from 11 organizations | NA | Examines how CISOs can balance business and security needs from a sociotechnical perspective | X | X | X |
| 17. | Loonam et al. 2020 | IEEE Transactions on Engineering Management | Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective | Grounded theory methodology; Interview with eight executives with CISO, CIO, and CTO titles in the UK and Ireland | NA | Explores roles of business leaders in supporting cybersecurity strategy | X | | X |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs' place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 18. | Lowry et al. 2022 | ICIS 2022 Proceedings | Taking a Seat at the Table: The Quest for CISO Legitimacy | Grounded theory qualitative field study with 35 participants, including CISOs, board directors, and consultants, in US companies | Legitimacy theory | Investigates how CISOs can gain legitimacy in the eyes of board of directors and C-suite executives | X | | |
| 19. | Maynard et al. 2018 | Pacific Asia Journal of the Association for Information System | Defining the Strategic Role of The Chief Information Security Officer | Systematic literature review of cybersecurity and strategic management disciplines | NA | Investigates attributes required for CISOs to become a strategist | | X | X |
| 20. | Monzelo and Nunes 2019 | CAPSI 2019 Proceedings | The Role of The Chief Information Security Officer (CISO) in Organizations | Interviews with four CISOs', three CIOs', two expert consultants, and one cybersecurity technician | NA | Explores CISO role, reporting structure, and responsibilities | X | | X |
| 21. | Moon et al. 2018 | International Journal of Information Management | The Impact of Relational Leadership and Social Alignment on Information Security System Effectiveness in Korean Governmental Organizations | Survey study with 102 CSOs from each department in the South Korean central government | Social capital theory | Examines how relational leadership of CISOs influences the social capital between CISOs and business executives | X | X | |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs’ place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 22. | Zwilling 2022 | Sustainability | Trends and Challenges Regarding Cyber Risk Mitigation by CISOs—A Systematic Literature and Experts’ Opinion Review Based on Text Analytics | Text mining method applied to (1) recent scientific literature, (2) security threat-related opinion news articles, and (3) OWASP’s reported list of vulnerabilities | NA | Investigates how current and emerging security threats impact the CISO's role and their effectiveness in addressing them based on their skills and expertise | | X | |
| 23. | Mulgund et al. 2023 | AMCIS 2023 Proceedings | A Qualitative Exploration of Stressors Influencing CISO Burnout | Interpretivist approach; Interview with 11 US CISOs | NA | Examines the determinants of CISO role stressors | | | X |
| 24. | Rosiek 2018 | Cyber Security: A Peer-Reviewed Journal | Chief Information Security Officer Best Practices For 2018: Proactive Cyber Security | Opinion | NA | Discusses CISOs’ evolving role and challenges facing them in securing their organizations | | | X |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs’ place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 25. | Shayo and Lin 2019 | Journal of Computer Science and Information Technology | An Exploration of The Evolving Reporting Organizational Structure for The Chief Information Security Officer CISO) Function | The case study method used to analyze 37 interviewees from open sources on the Internet, including O’Connor (2018a-g), Info Sec Institute (2010, 2012a-d, 2013, 2017a-d), and Cybereason (2017), as well as two additional interviews with CISOs | Complexity theory and interaction theory | Explores the evolving reporting structure for the CISO role and associated job skills | X | X | |
| 26. | Smit et al. 2021 | International Information Management Association, Conference Preceding 2021 | The Soft Skills Business Demands of the Chief Information Security Officer | Delphi study with 21 Dutch organizations that have a CISO position, and a quantitative content analysis of CISO job ads | NA | Investigates required soft skills for CISOs to function as an executive leader | | X | |
| 27. | Steinbart et al. 2018 | Accounting, Organizations & Society | The Influence of a Good Relationship Between the Internal Audit and Information Security Functions | Data were obtained from a web-based survey of IT auditors that were members of the IMTA section of the AICPA. | NA | Studies how CISOs’ reporting structure and their relationships with internal audit function influence security outcomes | X | | |
| 28. | Triplett 2022 | Journal of Cybersecurity and Privacy | Addressing Human Factors in Cybersecurity Leadership | Systematic literature review on human factor management | NA | Describes CISO’s challenges related to managing human factor | | | X |

| # | Author | Publication Outlet | Title | Method & Data Source | Theory/ Framework | Summary | Themes of Academic Literature | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | CISOs' place in the organizational hierarchy and reporting structure | Necessary Skills and training for CISOs | CISO roles and responsibilities |
| 29. | van Yperen Hagedoorn et al. 2021 | BLED 2021 Proceedings | Soft Skills of the Chief Information Security Officer | Delphi Study with 23 CISOs in Dutch organizations and a quantitative content analysis of CISO job ads published at eight different Dutch recruitment websites | NA | Examines the soft skills demands of Dutch CISOs | | X | |
| 30. | Whitten 2008 | The Journal of Computer Information Systems | The Chief Information Security Officer: An Analysis of The Skills Required for Success | Interviews with 7 CISOs and analysis of 33 CISO job listings posted by "Chief Security Officer Magazine" | NA | Investigates required skill sets for CISOs and CISO role and responsibilities | | X | X |

## Appendix B. Practitioner Literature on the CISO Role

| # | Author | Date | Organization | Title | Method & Data Source | Themes of Whitepapers | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | CISOs' Place in Organizational Hierarchy and Reporting Structure | Necessary Skills and Educational Background for the CISO Role | CISO Roles and Responsibilities |
| 1. | Aguas et al. | 2016 | Deloitte | The New CISO | Deloitte CISO Labs survey | x | x | x |
| 2. | Aiello and Thompson | 2020 | Heidrick & Struggles | North American Chief Information Security Officer (CISO) Compensation Survey | Survey study with 372 CISOs in North America | x | | x |
| 3. | Aiello et al. | 2021 | Heidrick & Struggle | Global Chief Information Security Officer (CISO) Survey | Survey study with 354 CISOs around the world | x | x | x |
| 4. | Aiello et al. | 2023 | Heidrick & Struggles | 2023 Global CISO Survey | Survey with 262 global CISOs | x | x | x |
| 5. | BT | 2021 | BT | CISOs Under the Spotlight | A survey with 4,016 consumers in eight countries and 715 executives | | x | x |
| 6. | Crawford | 2019 | Kaspersky | Cybersecurity Through the CISO's Eyes: Perspectives on a Role | Survey study with 305 cybersecurity executives in enterprise worldwide | | | x |
| 7. | ECSO | 2021 | The European Cybersecurity Organization | Chief Information Security Officers' (CISO) Challenges & Priorities | Survey study with 101 CISOs in Europe | x | x | x |
| 8. | Eichenwald et al. | 2021 | Korn Ferry | Meet the New CISOs | One-on-one interviews with 15 CISOs | x | x | |
| 9. | EY | 2020 | Ernst & Young | How Does Security Evolve from Bolted on to Built-In? | 22nd annual EY Global Information Security Survey with 1300 organizations | x | x | |

| # | Author | Date | Organization | Title | Method & Data Source | Themes of Whitepapers | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | CISOs' Place in Organizational Hierarchy and Reporting Structure | Necessary Skills and Educational Background for the CISO Role | CISO Roles and Responsibilities |
| 10. | F-Secure | 2021 | F-Secure | The CISOs' New Dawn | Interview with 28 CISOs in the US, UK, and Europe | x | x | x |
| 11. | Fortinet | 2019 | Fortinet | The CISO and Cybersecurity: A Report on Current Priorities and Challenges | Survey study with CISOs, CSOs, and VPs of IT security | x | | x |
| 12. | GAO-16-686 | 2016 | United States Government Accountability Office (GAO) | Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority | An interview and survey of 24 CISOs | | | x |
| 13. | Guenther | 2019 | Advanced cybersecurity center (ACSC) | Leveraging Board Governance for Cybersecurity: The CISO/CIO Perspective | Interview with 20 CISOs and CIOs, and an online survey with executives | | | x |
| 14. | Haworth | 2020 | Nominet Cybersecurity | The CISO Stress Report | Online surveys with C-suite executives and CISOs in the US and UK | | | |
| 15. | Kaspersky | 2018 | Kaspersky | What It Takes to Be a CISO: Success and Leadership in Corporate IT Security | Survey of 250 organizations from around the world with CISOs or their equivalent, and 11 expert interviews | x | x | x |
| 16. | KPMG | 2019 | KPMG | The Seven Ways of the Agile CISO | 2018 CIO survey by KPMG | x | x | x |
| 17. | McGraw et al. | 2017 | Synopsys | Four CISO Tribes and Where to Find Them | In-person interviews with 25 CISOs | x | x | x |

| # | Author | Date | Organization | Title | Method & Data Source | Themes of Whitepapers | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | CISOs' Place in Organizational Hierarchy and Reporting Structure | Necessary Skills and Educational Background for the CISO Role | CISO Roles and Responsibilities |
| 18. | Milica | 2021 | Proofpoint | 2021 Voice of the CISO Report | Survey study with1,400 CISOs from various industries in 14 countries. | | | |
| 19. | Milica | 2022 | Proofpoint | 2022 Voice of the CISO | A survey of 1400 CISOs from organizations of 200 employees or more from different industries in 14 countries, and interviews with 100 CISOs | x | | x |
| 20. | Oltsik | 2020 | Enterprise Strategy group (ESG) | The Life and Times of Cybersecurity Professionals 2020- A Cooperative Research Project by ESG And ISSA | Online Survey of security and IT professionals from the North America, Central/South America, Europe, Africa, Asia, and Australia | x | x | x |
| 21. | Olyaei | 2020 | Gartner | The Key Drivers for an Effective Security and Risk Leader | Survey study with 129 CISOs around the world | x | x | x |
| 22. | Phelps et al. | 2019 | Center for long term cybersecurity at UC Berkeley | Resilient Governance for Board of Directors | Interview study with 20 board of directors mainly but not only form US companies | x | x | x |
| 23. | Ponemon Institute and f5 | 2017 | Ponemon Institute | The Evolving Role of CISOs and Their Importance to the Business | Interview study with CISOs at 184 countries in the US, Germany, the United Kingdom, Brazil, Mexico, China, and India | x | x | x |
| 24. | Proofpoint | 2020 | Proofpoint | People-Centric Cybersecurity: A Study of IT Security Leaders in the UAE | A survey with 150 CSOs/CISOs across the United Arab Emirates | | | |
| 25. | PwC | 2020 | PwC | Out of the Shadows: CISOs in the Spotlight | Survey study with 45 companies in Luxembourg | x | x | x |

| # | Author | Date | Organization | Title | Method & Data Source | Themes of Whitepapers | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | CISOs' Place in Organizational Hierarchy and Reporting Structure | Necessary Skills and Educational Background for the CISO Role | CISO Roles and Responsibilities |
| 26. | PwC | 2021 | PwC | Global Digital Trust Insights Survey 2021 | Survey of 3249 executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-suite officers) around the world | | x | x |
| 27. | Rica | 2021 | KPMG | From Enforcer to Influencer | Interviews with CISOs | x | x | x |
| 28. | Salt Security | 2023 | Salt Security | State of the CISO | Survey with 300 global CISOs/CSOs | | | x |
| 29. | Salvi | 2019 | Infosys | Assuring Digital Trust | A survey of 867 executives from US, Europe, Australia, and New Zealand | x | x | x |

## 10. References

Aguas, T., Kark, K., and François, M. 2016. "The new CISO leading the strategic security organization," Deloitte Review. URL: https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf, accessed: May 7, 2024.

Aguilar, L. A. 2014. "Boards of directors, corporate governance and cyber-risks: Sharpening the focus," U.S. Securities and Exchange Commission. URL: https://www.sec.gov/news/speech/2014-spch061014laa, accessed: May 7, 2024.

Aiello, M., Randria, M., and Reventlow, C. 2021. "2021 Global Chief Information Security Officer (CISO) survey." Heidrick & Struggles. URL: https://www.heidrick.com/en/insights/technology-officers/2021-global-chief-information-security-officer-ciso-survey, accessed: May 7, 2024.

Aiello, M., Randria, M., and Reventlow, C. 2023. "2023 global CISO survey," Heidrick & Struggles. URL: https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2023-global-chief-information-security-officer-survey.pdf, accessed: May 7, 2024.

Aiello, M., and Schneidermeye, P. 2016. "Four mistakes to avoid when hiring your next Information Security Officer," in: *China Business Review.* URL: https://chinabusinessreview.com/four-mistakes-to-avoid-when-hiring-your-next-information-security-chief/, accessed: May 7, 2024.

Aiello, M., and Thompson, S. 2020. "North American Chief Information Security Officer (CISO) compensation survey," Heidrick & Struggles. URL: https://www.heidrick.com/en/insights/cybersecurity/2020_north_american_chief_information_security_officer_ciso_compensation_survey, accessed: May 7, 2024.

Alexander, A., and Cummings, J. 2016. "The rise of the Chief Information Security Officer," *People and strategy* (39:1), pp. 10-10.

Alter, S. 2008. "Defining information systems as work systems: Implications for the IS field," *European Journal of Information Systems* (17:5), pp. 448-469.

Alter, S. 2013. "Work system theory: Overview of core concepts, extensions, and challenges for the future," *Journal of the Association for Information Systems* (14:2), pp. 72-121.

Anderson, A. B., Ahmad, A., and Chang, S. 2022. "Competencies of cybersecurity leaders: A review and research agenda," in: *ICIS 2022 Proceedings. 9.*

Anderson, P. 1999. "Complexity theory and organization science," *Organization Science* (10:3), pp. 216-232.

Ashenden, D., and Sasse, A. 2013. "CISOs and organisational culture: Their own worst enemy?," *Computers & Security* (39), pp. 396-405.

Balozian, P., and Leidner, D. 2017. "Review of IS security policy compliance: Toward the building blocks of an IS asecurity theory," *Data Base for Advances in Information Systems* (48:3), pp. 11-43.

Barney, J. 1991. "Firm resources and sustained competitive advantage," *Journal of management* (17:1), pp. 99-120.

Beatty, R. C., Arnett, K. P., and Liu, C. 2005. "CIO/CTO job roles: An emerging organizational model," *Communications of the IIMA* (5:2), p. 1.

Bendig, D., Wagner, R., Piening, E., and Nils Foege, J. 2023. “Attention to digital innovation: Exploring the impact of a Chief Information Officer in the top management team,” *MIS Quarterly* (47:4), pp. 1487-1516.

Bitektine, A., and Haack, P. 2015. “The “macro” and the “micro” of legitimacy: Toward a multilevel theory of the legitimacy process,” *Academy of Management Review* (40:1), pp. 49-75.

BitSight. 2019. “The evolution of the CISO,” BitSight. URL: https://www.bitsight.com/resources/evolution-of-the-ciso, accessed: April 28, 2024.

Bodin, L. D., Gordon, L. A., and Loeb, M. P. 2005. “Evaluating information security investments using the analytic hierarchy process,” *Communications of the ACM* (48:2), pp. 78-83.

Brodbeck, P. W. 2002. “Complexity theory and organization procedure design,” *Business Process Management Journal* (8:4), pp. 377-402.

BT. 2021. “CISOs under the spotlight,” British Telecommunications. URL: https://www.globalservices.bt.com/en/insights/whitepapers/cisos-under-the-spotlight, accessed: May 7, 2024.

Cano, J. J., and Almanza, A. R. 2023. “The information security function and the CISO in Colombia: 2010–2020,” *International Conference on Information Technology & Systems*: Springer, pp. 95-108.

Carpenter, M. A., Geletkanycz, M. A., and Sanders, W. G. 2004. “Upper echelons research revisited: Antecedents, elements, and consequences of top management team composition,” *Journal of Management* (30:6), pp. 749-778.

Cleveland, S., and Cleveland, M. 2018. “Toward cybersecurity leadership framework,” in: *MWAIS 2018 Proceedings. 49.*

Cram, W. A., D’Arcy, J., and Proudfoot, J. G. 2019. “Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance,” *MIS Quarterly* (43:2), pp. 525-554.

Da Silva, J. 2022. “Cyber security and the Leviathan,” *Computers & Security* (116), p. 102674.

Da Silva, J., and Jensen, R. B. 2022. “"Cyber security is a dark art": The CISO as soothsayer,” *Proceedings of the ACM on Human-Computer Interaction* (6:CSCW2), pp. 1-31.

Dawson, M., Burrell, D. N., Rahim, E., and Brewster, S. 2010. “Examining the role of the Chief Information Security Officer (CISO) & Security plan,” *Journal of Information Systems Technology & Planning* (3:6).

Dhillon, G., Smith, K., and Dissanayaka, I. 2021. “Information systems security research agenda: Exploring the gap between research and practice,” *The Journal of Strategic Information Systems* (30:4), p. 101693.

DOJ. 2023. “Former Chief Security Officer of Uber sentenced to three years’ probation for covering up data breach involving millions of Uber user records.” from URL: https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data, accessed: May 7, 2024.

Dor, D., and Elovici, Y. 2016. “A model of the information security investment decision-making process,” *Computers & Security* (63), pp. 1-13.

Drinkwater, D. 2016. “These CISOs explain why they got fired.” CSO Online.URL: https://www.csoonline.com/article/555777/these-cisos-explain-why-they-got-fired.html#:~:text=Other%20sources%2C%20speaking%20to%20me,solutions%20to%20these%20same%20problems, accessed: May 7, 2024.

ECSO. 2021. “Chief Information Security Officers’ (CISO) challenges & priorities survey analysis report.” The European Cyber Security Organisation. URL: https://riskcue.id/ebook/ECS-Survey-Analysis-Report-Chief-Information-Security-Officers-CISO-Challenges-and-Priorities, accessed: May 7, 2024.

Eichenwald, M., Huang, K., and Mayville, B. 2021. “Meet the New CISO,” Korn Ferry Cybersecurity. URL: https://www.kornferry.com/insights/featured-topics/leadership/the-evolving-CISO-role-what-success-looks-like, accessed: May 7, 2024.

Eisenhardt, K. M. 1989. “Agency theory: An assessment and review,” *Academy of Management Review* (14:1), pp. 57-74.

EY. 2020. “How does security evolve from bolted on to built-in? Bridging the relationship gap,” Ernst & Young. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report.pdf, accessed: May 7, 2024.

F-Secure. 2021. “The CISOs’ new dawn,” F-Secure. URL: https://www.withsecure.com/en/expertise/campaigns/the-cisos-new-dawn, accessed: May 7, 2024.

Fama, E. F. 1980. “Agency problems and the theory of the firm,” *Journal of Political Economy* (88:2), pp. 288-307.

FBI. 2014. “A byte out of history $10 million hack, 1994-style.” from URL: https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack, accessed: May 7, 2024.

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), pp. 257-263.

Fortinet. 2019. “The CISO and cybersecurity: A report on current priorities and challenges,” Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-ciso-and-cybersecurity.pdf, accessed: May 7, 2024.

FTC. 2022. “Standards for safeguarding customer information,” in: *86 FR 70272*. Federal Trade Commission: pp. 71509-71511. URL: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314, accessed: May 7, 2024.

GAO. 2016. “Federal Chief Information Security Officers: Opportunities exist to improve roles and address challenges to authority,” The U.S. Government Accountability Office. URL: https://www.gao.gov/products/gao-16-686, accessed: May 7, 2024.

Gartner. 2020. “The key drivers for an effective security and risk leader,” Gartner. URL: https://assets-powerstores-com.s3.amazonaws.com/data/org/20033/media/doc/the_key_drivers_for_an_effective_security_and_risk_1599830720728015h2n-e76294009bde4bacaad9bda1702825da.pdf, accessed: May 7, 2024.

Guenther, W. 2019. “Leveraging board governance for cybersecurity: The CISO/CIO perspective,” Advanced Cyber Security Center. URL: https://static1.squarespace.com/static/61fbd5d6acd847546568c72b/t/622a305a330a1b1c688d2ed3/1646932061165/acsc_cyber_%2B_boards_report_full.pdf, accessed: May 7, 2024.

Haislip, J., Lim, J.-H., and Pinsker, R. 2021. “The impact of executives’ IT expertise on reported data security breaches,” *Information Systems Research* (32:2), pp. 318-334.

Hambrick, D. C. 2007. “Upper echelons theory: An update,” *The Academy of Management Review* (32:2), pp. 334-343.

Hambrick, D. C., and Mason, P. A. 1984. "Upper echelons: The organization as a reflection of Its top managers," *The Academy of Management Review* (9:2), pp. 193-206.

Hardy, C., Palmer, I., and Phillips, N. 2000. "Discourse as a strategic resource," *Human Relations* (53:9), pp. 1227-1248.

Haworth, R. 2019. "Trouble at the top: The boardroom battle for cyber supremacy," Nominet. URL: https://media.nominet.uk/wp-content/uploads/2019/06/03164309/Trouble_at_the_Top.pdf, accessed: May 7, 2024.

Haworth, R. 2020. "The CISO stress report," Nominet. URL: https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf, accessed: April 30, 2024.

Heider, F. 1982. *The psychology of interpersonal relations*. Psychology Press.

Hielscher, J., Menges, U., Parkin, S., Kluge, A., and Sasse, M. A. 2023. ""Employees who don't accept the time security takes are not aware enough": The CISO view of human-centred security," *32st USENIX Security Symposium (USENIX Security 23), Boston, MA*.

Hobbes, T. 1845. *The English works of Thomas Hobbes of Malmesbury*. John Bohn.

Hobbes, T., and Gale. 1839. *English works of Thomas Hobbes of Malmesbury, now first collected and edited / by William Molesworth*.

Hom, P. W., Lee, T. W., Shaw, J. D., and Hausknecht, J. P. 2017. "One hundred years of employee turnover theory and research," *Journal of applied psychology* (102:3), p. 530.

Hooper, V., and McKissack, J. 2016. "The emerging role of the CISO," *Business Horizons* (59:6), pp. 585-591.

Infosys. 2019. "Assuring digital trust," Infosys Knowledge Institute. URL: https://www.infosys.com/services/cyber-security/insights/assuring-digital-trust-cybersecurity.html, accessed: May 7, 2024.

Jingyu, L., Mengxiang, L., Xincheng, W., and Thatcher, J. B. 2021. "Strategic directions for AI: The role of CIOs and boards of directors," *MIS Quarterly* (45:3), pp. 1603-1643.

Johnson, M. E., and Goetz, E. 2007. "Embedding information security into the organization," *IEEE Security & Privacy* (5:3), pp. 16-24.

Johnson, V., Torres, R., Maurer, C., Guerra, K., Srivastava, S., and Mohit, H. 2023. "The 2022 SIM IT issues and trends study," *MIS Quarterly Executive* (22:1), p. 6.

Kappelman, L., Johnson, V., Torres, R., Maurer, C., and McLean, E. 2019. "A study of information systems issues, practices, and leadership in Europe," *European Journal of Information Systems* (28:1), pp. 26-42.

Kappers, W. M., and Harrell, M. N. 2020. "From degree to Chief Information Security Officer (CISO): A framework for consideration," *Journal of Applied Business and Economics* (22:11).

Karanja, E. 2017. "The role of the Chief Information Security Officer in the management of IT security," *Information & Computer Security* (25:3), pp. 300-329.

Karanja, E., and Rosso, M. A. 2017. "The Chief Information Security Officer: An exploratory study," *Journal of International Technology and Information Management* (26:2), pp. 23-47.

Kaspersky. 2018. "What It takes to be a CISO: Success and leadership in corporate IT security," Kaspersky Lab. URL: https://usa.kaspersky.com/blog/ciso-report/16480/, accessed: May 7, 2024.

Kaspersky. 2019. "Cybersecurity through the CISO's eyes: Perspectives on a role," Kaspersky. URL: https://go.kaspersky.com/rs/802-IJN-240/images/10752_Advisory_BW_Kaspersky_CISO_report.pdf, accessed: May 7, 2024.

Kayworth, T., and Whitten, D. 2010. "Effective information security requires a balance of social and technology factors," *MIS Quarterly Executive* (9:3), pp. 2012-2052.

Kelley, H. H. 1967. "Attribution theory in social psychology," *Nebraska symposium on motivation*: University of Nebraska Press.

Kouns, B. L., and Kouns, J. 2011. *The Chief Information Security Officer: Insights, tools and survival skills*. Ely: IT Governance.

KPMG. 2019. "The seven ways of the agile CISO," 2019 KPMG International Cooperative. URL: https://home.kpmg/ky/en/home/insights/2019/08/the-seven-ways-of-the-agile-ciso.html, accessed: May 7, 2024.

KPMG. 2021. "From enforcer to influencer: Shaping tomorrow's security team," KPMG. URL: https://home.kpmg/xx/en/home/insights/2021/07/cyber-trust-securing-the-future.html, accessed: April 29, 2024.

Lanz, J. 2017. "The Chief Information Security Officer: The new CFO of information security," *The CPA Journal* (87:6), pp. 52-57.

Loonam, J., Zwiegelaar, J., Kumar, V., and Booth, C. 2020. "Cyber-resiliency for digital enterprises: A strategic leadership perspective," *IEEE Transactions on Engineering Management* (69:6), pp. 3757-3770.

Lowry, M., Vance, A., and Vance, M. D. 2023. "Inexpert supervision: Field evidence on boards' oversight of cybersecurity," *Available at SSRN 4002794*).

Lowry, M. R., Sahin, Z., and Vance, A. 2022. "Taking a seat at the table: The quest for CISO legitimacy," in: *ICIS 2022 Proceedings.14.*

Malle, B. F. 2011. "Attribution theories: How people make sense of behavior," in *Theories in social psychology.,* D. Chadee (ed.). Hoboken, NJ: Wiley Blackwell, pp. 72-95.

March, J. G., and Simon, H. A. 1958. *Organizations*. New York:Wiley.

Markman, K. D., and Tetlock, P. E. 2000. "'I couldn't have known': Accountability, foreseeability and counterfactual denials of responsibility," *British Journal of Social Psychology* (39:3), pp. 313-325.

Markus, M. L. 1983. "Power, politics, and MIS implementation," *Communications of the ACM* (26:6), pp. 430-444.

Maynard, S., Onibere, M., and Ahmad, A. 2018. "Defining the strategic role of the Chief Information Security Officer," *Pacific Asia Journal of the Association for Information Systems* (10:3), p. 3.

McGraw, G., Migues, S., and Chess, B. 2017. "Four CISO tribes and where to find them," Synopsys. URL: https://www.garymcgraw.com/wp-content/uploads/2018/01/CISO-2017.pdf, accessed: May 9, 2024.

Milica, L. 2021. "Voice of the CISO report," Proofpoint. URL: https://library.cyentia.com/report/report_007469.html, accessed: May 7, 2024.

Milica, L. 2022. "2022 voice of the CISO," Proofpoint. URL: https://go.proofpoint.com/en-voice-of-the-ciso-2022.html, accessed: May 7, 2024.

Monzelo, P., and Nunes, S. 2019. "The role of the Chief Information Security Officer (CISO) in organizations," in: *CAPSI 2019 Proceedings. 36.*

Moon, Y. J., Choi, M., and Armstrong, D. J. 2018. “The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations,” *International Journal of Information Management* (40), pp. 54-66.

Morgan, S. 2024. “List of Fortune 500 Chief Information Security Officers,” in: *Cybercrime Magazine*. URL: https://cybersecurityventures.com/ciso-500/, accessed: April 29, 2024.

Mulgund, P., Higgins, K., Singh, R., Li, Y., and Chew, S. L. 2023. “A qualitative exploration of stressors influencing CISO burnout,” in: *AMCIS 2023 Proceedings. 4.*

Nahapiet, J., and Ghoshal, S. 1998. “Social capital, intellectual capital, and the organizational advantage,” *Academy of management review* (23:2), pp. 242-266.

Navisite. 2021. “The state of Cybersecurity leadership and readiness,” Navisite. URL: https://www.navisite.com/resources/state-of-cybersecurity-leadership-and-readiness-report/, accessed: May 7, 2024.

NCSC. 2023. “Cyber security toolkit for boards,” National Cyber Security Centre. URL: https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf, accessed: May 7, 2024.

Neville-Neil, G. V. 2019. “What is a Chief Security Officer good for?,” *Communications of the ACM* (62:10), pp. 26-27.

Northouse, P. G. 2018. *Introduction to leadership : Concepts and practice*, (Fourth edition. ed.). Los Angeles: SAGE.

NYDFS. 2023. “Cybersecurity requirements for financial services companies,” in: *Second Amendment to 23 NYCRR 500*. New York Department of Financial Services. URL: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf, accessed: May 7, 2024.

NYFDS. 2017. “New York Department of Financial Services. Cybersecurity requirements for financial services companies,” in: *23 NYCRR s 500.4(b)*. New York Department of Financial Services. URL: https://www.dfs.ny.gov/industry_guidance/cybersecurity, accessed: April 28, 2024.

Oracle. 2019. “The mission of the cloud-centric CISO,” Oracle. URL: https://www.oracle.com/a/ocom/docs/cloud/mission-of-the-cloud-centric-ciso-report.pdf, accessed: May 7, 2024.

Pare, G., Tate, M., Johnstone, D., and Kitsiou, S. 2016. “Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews,” *European Journal of Information Systems* (25:6), pp. 493-508.

Paré, G., Trudel, M.-C., Jaana, M., and Kitsiou, S. 2015. “Synthesizing information systems knowledge: A typology of literature reviews,” *Information & Management* (52:2), pp. 183-199.

Parker, D. B. 1981. *Computer security management*. Reston Publishing Company Reston, VA.

Petersen, R. 2006. “Safeguarding information assets in higher education: The role of the CSO,” *EDUCAUSE Review* (41:5), p. 72.

Pfeffer, J., and Salancik, G. R. 2003. *The external control of organizations: A resource dependence perspective*. Stanford University Press.

Phelphs, B., Cleaveland, A., and Weber, S. 2019. “Resilient governance for boards of directors,” UC Berkeley-Center for Long-Term Cybersecurity. URL: https://cltc.berkeley.edu/resilient-governance/, accessed: May 7, 2024.

Ponemon. 2017. "The evolving role of CISOs and their importance to the business," Ponemon Instittute. URL: https://www.ponemon.org/news-updates/blog/security/the-evolving-role-of-cisos-and-their-importance-to-the-business.html, accessed: May 7, 2024.

Proofpoint. 2020. "People-centric cybersecurity: A study of IT security leaders in the UAE," Proofpoint. URL: https://www.proofpoint.com/sites/default/files/2020-05/Proofpoint_UAE%20CISO%20REPORT_May%202020_FINAL.pdf, accessed: May 7, 2024.

PwC. 2020. "Out of the shadows: CISOs in the spotlight," PricewaterhouseCoopers. URL: https://www.pwc.lu/en/advisory/digital-tech-impact/cyber-security/2020-ciso-role-and-responsibilities-survey.html, accessed: May 7, 2024.

PwC. 2021. "Global digital trust insights survey 2021," PricewaterhouseCoopers. URL: https://www.pwc.com/kz/en/services/global-digital-trust-insights.html, accessed: May 7, 2024.

Rao, S., and Ramachandran, S. 2007. "Information security governance arrangements: The devil is in the details," in: *AMCIS 2007 Proceedings. 250.*

Room, S. 2023. "SolarWinds is a game changer - You cannot sugarcoat cybersecurity," Forbes. URL: https://www.forbes.com/sites/stewartroom/2023/11/01/solarwinds-is-a-game-changeryou-cannot-sugarcoat-cybersecurity/?sh=6f13b68362cb, accessed: May 7, 2024.

Rosiek, T. 2018. "Chief Information Security Officer best practices for 2018: Proactive cybersecurity," *Cyber Security: A Peer-Reviewed Journal* (1:4), pp. 361-367.

Salt. 2023. "State of the CISO," Salt Security. URL: https://content.salt.security/global-state-ciso-report-2023.html#:~:text=State%20of%20the%20CISO%202023&text=Nearly%20half%20of%20CISOs%20worldwide,control%20gaps%20in%20digital%20initiatives, accessed: May 7, 2024.

San Miguel, J. G., and Govindarajan, V. 1984. "The contingent relationship between the controller and internal audit functions in large organizations," *Accounting, Organizations and Society* (9:2), pp. 179-188.

Schein, E. H. 1999. *The corporate culture survival guide : Sense and nonsense about culture change*, (1st ed.). San Francisco, Calif.: Jossey-Bass.

Schein, E. H. 2010. *Organizational culture and leadership*, (Fourth edition ed.). San Francisco: Jossey-Bass.

SEC. 2023. "Cybersecurity risk management, strategy, governance, and incident disclosure," in: *17 CFR Parts 229, 232, 239, 240, and 249*. Securities and Exchange Commission. URL: https://www.sec.gov/news/press-release/2023-139, accessed: April 29, 2024.

Seyranian, V. 2009. "Contingency theories of leadership, encyclopedia of group processes & intergroup relations edited by John M. Levine and Michael A. Hogg." Thousand Oaks, California: SAGE,

Shayo, C., and Lin, F. 2019. "An exploration of the evolving reporting organizational structure for the Chief Information Security Officer (CISO) function," *Journal of Computer Science* (7:1), pp. 1-20.

Smit, R., van Yperen Hagedoorn, J. M. J., Versteeg, P., and Ravesteijn, P. 2021. "The soft skills business demands of the Chief Information Security Officer," *Journal of International Technology & Information Management* (30:4), pp. 41-61.

Snow, D. A., and Anderson, L. 1987. "Identity work among the homeless: The verbal construction and avowal of personal identities," *American Journal of Sociology* (92:6), pp. 1336-1371.

Somers, M. 2023. "5 enduring management ideas from MIT Sloan's Edgar Schein," MIT Sloan Management Review. URL: https://mitsloan.mit.edu/ideas-made-to-matter/5-enduring-management-ideas-mit-sloans-edgar-schein, accessed: May 10, 2024.

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. 2018. "The influence of a good relationship between the internal audit and information security functions on information security outcomes," *Accounting, Organizations and Society* (71), pp. 15-29.

Straub, D. W. 1988. "Organizational structuring of the computer security function," *Computers & Security* (7:2), pp. 185-195.

Sullivan, P. 2022. "Maintaining your compliance strategy during (and after) CISO turnover." ISACA. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/maintaining-your-compliance-strategy-during-and-after-ciso-turnover, accessed: May 7, 2024.

Templier, M., and Paré, G. 2015. "A framework for guiding and evaluating literature reviews," *Communications of the Association for Information Systems* (37:1), p. 6.

ThreatTrack. 2015. "No respect. Chief Information Security Officers misunderstood and underappreciated by their C-level peers," ThreatTrack Security. URL: https://www.ten-inc.com/presentations/ThreatTrack-The-Role-of-the-CISO.PDF, accessed: May 7, 2024.

Tost, L. P. 2011. "An integrative model of legitimacy judgments," *Academy of Management Review* (36:4), pp. 686-710.

Townsend, K. 2021. "CISO conversations: Steve Katz, the world's first CISO," Security Week. URL: https://www.securityweek.com/ciso-conversations-steve-katz-worlds-first-ciso/, accessed: February 8, 2024.

Triplett, W. J. 2022. "Addressing human factors in cybersecurity leadership," *Journal of Cybersecurity and Privacy* (2:3), pp. 573-586.

van Yperen Hagedoorn, J. M. J., Smit, R., Versteeg, P., and Ravesteijn, P. 2021. "Soft skills of the Chief Information Security Officer," in: *BLED 2021 Proceedings. 31.*

Vance, A., Siponen, M. T., and Straub, D. W. 2020. "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures," *Information & Management* (57:4), p. 103212.

Vijayan, J. 2017. "CISOs, board members have widely divergent views on cybersecurity," in: *Dark Reading*. URL: https://www.darkreading.com/operations/cisos-board-members-have-widely-divergent-views-on-cybersecurity, accessed: May 8, 2024.

Vincent, N. E., Higgs, J. L., and Pinsker, R. E. 2019. "Board and management-level factors affecting the maturity of IT risk management practices," *Journal of information systems* (33:3), pp. 117-135.

Webster, J., and Watson, R. T. 2002. "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly* (26:2), pp. xiii-xxiii.

Whitten, D. 2008. "The Chief Information Security Officer: An analysis of the skills required for success," *Journal of Computer Information Systems* (48:3), pp. 15-19.

Zwilling, M. 2022. "Trends and challenges regarding cyber risk mitigation by CISOs—A systematic literature and experts' opinion review based on text analytics," *Sustainability* (14:3), p. 1311.