Taking a Seat at the Table: The Quest for CISO Legitimacy

Short Paper

Anthony Vance
Virginia Tech
Pamplin Hall 880 W Campus Dr Suite 1007, Blacksburg, VA 24061
anthony@vance.name

Michelle Lowry
Virginia Tech
Pamplin Hall 880 W Campus Dr Suite 3007, Blacksburg, VA 24061
michellel@vt.edu

Zeynep Sahin
Virginia Tech
Pamplin Hall 880 W Campus Dr Suite 1007, Blacksburg, VA 24061
zeyneps@vt.edu

Abstract

The role of the chief information security officer (CISO) has emerged as critically important to organizations in managing cybersecurity risks. Unfortunately, many CISOs are limited by perceptions of boards and executive teams that the CISO is not a strategic partner. This study investigates CISOs' struggles for legitimacy in their ascendancy into the executive suite and in directly reporting to the board of directors. In a grounded theory interview study, we use legitimacy theory as a lens to develop a model of a virtuous cycle of legitimacy, wherein a CISO's legitimacy gains at the board level feed into successful bids for legitimacy within the executive suite, extending legitimacy theory to include legitimacy assessments within related hierarchal groups (i.e., the board and executive team). Given the growing importance of CISOs, we inform research and practice on how they can become full-fledged members of the executive team and legitimate partners of the board.

Keywords: CISO, board of directors, top management team, legitimacy theory, grounded theory, cybersecurity

"If you're not in the CEO staff meeting, then the 'C' [in CISO] in front of your name is for marketing. It's not real."

CISO, S&P 500 company

Introduction

Since the first chief information security officer (CISO) position was created at Citibank in 1994 in the wake of hackers stealing $10 million (Morgan 2021), the CISO role has emerged as critically important to organizations in managing cybersecurity risks (Steinbart et al. 2018). Today, approximately 75% of *Fortune 500* companies have a CISO (Morgan 2021). Moreover, existing and proposed regulations in the U.S. are elevating the importance of the CISO role. For example, a rule by the U.S. Federal Trade Commission effective January 2022 requires U.S. financial institutions to employ a CISO or equivalent role and that this individual must report at least annually to the institution's board of directors (FTC 2021). Similarly, the U.S. Securities and Exchange Commission has proposed rules that would require public companies traded

on U.S. exchanges to declare whether they have a CISO, the individual's expertise and to whom they report within the organization, and whether and how frequently the CISO reports to the board of directors. Similar rules are likely to be adopted around the world (SEC 2022).

However, despite the importance and the prevalence of this position, CISOs continue to struggle for support within their firms. For example, a global survey of 1,581 security executives and senior-level managers reported that 51% lack executive support, 53% claim that senior leadership did not understand their role, and 63% believe that their budget is insufficient. In addition, 64% reported being three or more reporting levels away from the CEO (LogRhythm 2021). Likewise, the onus is on CISOs to prove that they are qualified to be legitimate members of the C-suite, gain the trust of the board and executive team, and develop influence within the organization to overcome organizational politics, because "in the C-suite world, it is all about influence" (KPMG 2021, p.7). Given the critical role of CISOs for the security of their organizations, and the discrepancy between growing regulatory pressures to elevate the role of the CISO and the lack of support for and influence of CISOs in many organizations, there is a need for scholars and practitioners to better understand how CISOs can transition from mid-level managers to bona fide members of the C-suite.

We address this gap in this study by investigating the following research question:

> *RQ: What inhibits or facilitates CISO's legitimacy in the eyes of the board and C-suite executives?*

To answer this question, we conducted a grounded theory qualitative field study with CISOs, board directors, and consultants specializing in advising CISOs. To guide our investigation, we adopt the lens of legitimacy theory. Legitimacy is "the belief that authorities, institutions, and social arrangements are appropriate, proper and just" (Tyler 2006, p. 376). Legitimacy theory explains the process by which subjects (CISOs in the case of this study) can develop legitimacy within their aspirational peer group (here, the board and C-suite) and in so doing gain organizational influence (Bitektine and Haack 2015; Tost 2011).

Our preliminary findings indicate that although CISOs often lack legitimacy in the eyes of the board of directors and C-suite, CISOs can increase their legitimacy through a virtuous cycle of proactive engagement with the board and C-suite members. Furthermore, as CISOs gain legitimacy with the board, the board can influence the legitimacy perceptions of the C-suite, and vice versa. Importantly, our findings reveal how this virtuous legitimacy cycle leads to tangible security program outcomes, such as an increased security budget and the prioritization of security programs.

This ongoing research project is expected to make several contributions. First, whereas legitimacy theory has been used in management previously, little is known about the role of legitimacy at the executive level. This research contributes to legitimacy theory by providing an understanding of the legitimating process for would-be executives (here, CISOs) attempting to be included in, and more effective in working with, the C-suite. Second, in previous research such as Bitekine and Haack (2015), the targets of legitimacy assessments are passive objects of study. In contrast, in this study, the targets of legitimacy (CISOs) are subjects with agency who can take proactive measures to influence how they are assessed. Third, previous legitimacy research has examined the legitimating process within a single aspirational peer group. In contrast, we explain this process in the context of two hierarchical peer groups, in which one (the board of directors) oversees the other (the C-suite). We demonstrate that CISOs are evaluated in two interdependent legitimacy cycles for the board and C-suite groups, in which hierarchy plays an important role in the legitimating process. Finally, we identify specific proactive actions that CISOs can take to advocate for their legitimacy.

This paper proceeds as follows. First, we discuss our research method, then we summarize our findings in relation to our CISO legitimating model, and then we conclude by discussing the implications of this study for practice and developing policies.

Theoretical Lens of Legitimacy Theory

While the earliest guidance in grounded theory method presumes researchers have no theoretical lens or a priori background through which to interpret their data (Glaser and Strauss 1967), further explications of grounded theory presume researchers have exposure to the relevant literature and extant theories as

sensitizing concepts (Charmaz 2002; Matavire and Brown 2013). As we jointly collected and analyzed data in our interviews regarding the challenges CISOs faced in their ascendancy, we identified themes relating to power, influence, proactivity, and legitimacy (Magee and Galinsky 2008; Pfeffer 1981; Tyler 2006). Because these themes are described by legitimacy theory (Bitektine and Haack 2015; Tost 2011; Tyler 2006), we adopted it as a theoretical lens to guide our subsequent analysis. Legitimacy theory has been used by both organizational theory and social psychology researchers to explain how subjects are evaluated within a given social context. In the case of this study, the subject is the CISO and the social context is the board of directors and C-Suite.

We extend legitimacy theory to provide insight into the contextual factors and actions that enable and inhibit CISO legitimacy with the board and the C-suite. Bitektine and Haack (2015) proposed a multi-level organizational legitimacy model that both explains how legitimacy judgements facilitate institutional stability and also forms institutions in times of flux. In their model, legitimacy is conferred by individual evaluators, who both make personal assessments and also rely on external consensus legitimacy evaluations. In the context of institutions in flux, such as the ascendency of the CISO, less valence is ascribed to the opinions of others (Bitektine and Haack 2015), and thus the legitimacy of the CISO is based more on individual assessments. We extend their model to bids for executive legitimacy for CISOs, whose position is in flux. Within any given organization, the CISO's success in establishing legitimacy will vary according to how they reduce the barriers to support (Bitektine and Haack 2015), and induce positive updates to these individual assessments (Bitektine and Haack 2015), including building comprehensibility (Suchman 1995; Suddaby and Greenwood 2005).

We were reflexive in our analysis of the data, including shifting our thinking in the early part of the study to an understanding that most CISOs reside in a relatively low-legitimacy state. Rather than developing a descriptive model, we focused on a central challenge: the CISO legitimating process, and related actions and contingencies in CISOs' board and executive interactions.

Method

We conducted a multiple-case qualitative study to understand the challenges CISOs face in their ascendancy to the C-suite. A qualitative study is appropriate given the dynamic nature of the social processes that lead to legitimation. In doing so, we used grounded theory methodology, which is inductive, flexible, and iterative, allowing us to cyclically refine our methodology as we encountered and analyzed our data (Bryant and Charmaz 2007; Glaser and Strauss 1967). Our objective for using this method was to develop a substantive theory to understand the CISO ascendancy experience.[1] We follow previous research in the information systems field (Sarkar et al. 2020; Sarker and Sarker 2009) in adopting a less prescriptive version of grounded theory methodology, which features the key principles summarized below. Iterative data collection, analysis, and theoretical sampling are key to developing theoretical models that are grounded in the data, that is, the interviewees' reflections on their experiences with CISO ascendancy.

We interviewed 35 participants, comprising high-level cybersecurity executives, directors, and consultants, who we recruited through a theoretical, snowball sampling approach in which we asked participants for referrals to potential participants that could address the themes that surfaced. Furthermore, we tailored our questions in later interviews around our emergent theoretical model. At least two members of the research team with experience in conducting and publishing qualitative research participated in each of the interviews, which were conducted by phone or video call and lasted an average of 52 minutes. We audio-recorded and professionally transcribed all but four of these interviews, for which detailed notes were taken and compared for accuracy. A graduate research assistant then reviewed each transcript against the corresponding audio recording to ensure accuracy.

As part of our iterative coding process, at least two researchers initially coded a subset of interview transcripts, often immediately after an interview had been conducted, using an initial codebook and open coding. After coding each interview, each researcher wrote a short memo that included key insights gained from the interview, emergent themes, and proposed new codes. The research team then met after each

1 Grounded theory methodology defines substantive theories as those that are specific to situations, that is, persons and places, and thus can be considered middle-range theories (Lempert 2007).

initial coding and discussed new codes, concepts, emergent themes, and possible additional questioning of that specific interviewee as well as of future interviewees. These meetings promoted reflexivity amongst the research team. We also wrote overarching theme memos, including sketching process models, and eventually initiated selective coding to map our data to our emerging model, to refine the model and to direct further data collection according to theoretical sampling.[2]

Participant Type	Market Cap	Represented Industries
Executive (13)	Mid (5), Large (7)	Communication services Financial services Manufacturing Technology and services Wholesale trade
Director (12)	Mid (7), Large (4)	Construction Financial services Manufacturing Retail trade Technology and services Transportation Wholesale trade
Consultant (10)	n.a.	Various

Table 1. Summary of Interview Participants

Findings

Our model of the CISO legitimating process involves two interdependent, virtuous cycles, as depicted in Figure 1. As part of CISOs' ascendency to the C-suite, they manage both board and executive relationships. Over time, as the CISO iterates through these cycles of access and proactively engages the board and C-suite, the board and C-suite update their perceptions of the CISO's legitimacy, which in turn can lead to greater support for the CISO and security initiatives, and increased opportunities for access to the board and C-Suite. These cycles are hierarchical; since the board oversees and advises a corporation's management, the board's reassessments of the CISO's legitimacy influence the CISO's legitimation process with the C-suite.

Board Engagement (Access)

As second-tier executives, CISOs have a historical problem of access to the board, with one CISO describing their board reporting as their "15 minutes of fame" (Executive11). A consultant stated:

> *[T]here are so many risks in running an organization that it's hard for a C-suite or a board of directors to make enough time to have the conversation that needs to be had with the CISO. So it's a chicken-and-egg problem: you need the CISO to have access to the C-suite and the board so that they can educate the C-suite and the board on what they need to be worried about. But until they get that access, the board doesn't think about it, or the C-suite doesn't think about it, and often then the CISO is buried too far down in the organization to be able to make that happen. (Consultant10)*

As a partial resolution to this "chicken-and-egg" access problem, contemporary regulatory pressures (FTC 2021; SEC 2022), as well as developing norms emphasize CISO access to the board, initiating this key first step in the legitimacy cycle. Although some CISOs do not (yet) provide direct reports to the board, most boards have responded to SEC and other regulatory guidance to directly oversee cybersecurity risks, including receiving reports from the CISO, either directly or indirectly. Even when CISOs report up through

2 This selective coding is still in process at the time of this ICIS paper submission.

other executives such as the CIO, this access can serve as a foot in the door and provide opportunities to proactively engage with the board. Any access, even indirect access, opens the door to the CISO engaging with the board proactively.

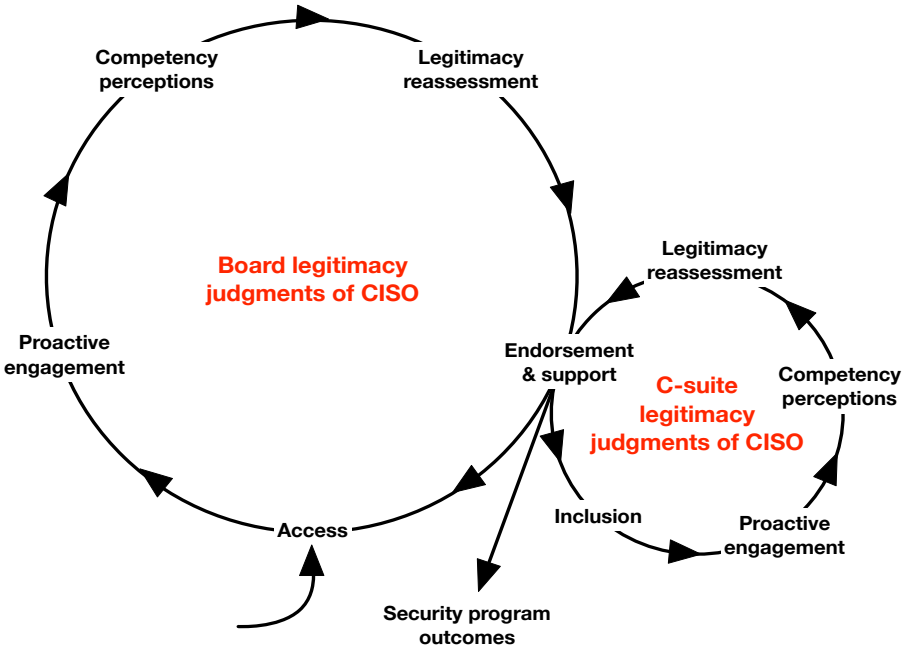

Figure 1. Process Model of CISO Legitimacy Judgments by the Board and C-Suite

Proactive Engagement with the Board

A CISO's effective, proactive engagement with the board is the main driver of the virtuous cycle of CISO legitimacy building. Effective engagement provides the board with insight for their reassessment of the CISO's competency and legitimacy. We categorize proactive engagement into three categories: relationship building, competency signaling, and political action.

Many proactive actions that facilitate understanding between the board and the CISO also develop the CISO's relationship with both the board as a whole and with individual directors. The CISO often plays a "coaching" role to the board, as they provide explicit and implicit education and guidance to the board on security matters (Director2, Director7). This is unique for an executive relationship with the board because most boards lack cybersecurity expertise (Lowry et al. 2021). For example, the board does not need to be coached on understanding financial statements; in contrast, they do need help understanding the fundamentals of security risks and their implications for the business (Executive1). One CISO explained that he provided explicit annual training sessions to his board to raise their "cyber IQ":

> *One year it was Security 101 — the anatomy of a [security] program, how it's built, how you evolved to the strategy, how you execute. [Then in year two] we did a tabletop demonstration, how we do our annual cyber security, executive tabletop exercise. We had one session on "how do you protect yourself from [cyber] criminals?". Every year you have that. (Executive6)*

Softer forms of coaching implicitly help the board understand cybersecurity, or as one CISO said, "condition them" to "level-set" (Executive4). One example is to proactively provide the board with information about high-profile security incidences: "Put something together and send it to the board before they reach out to you" (Consultant7). CISOs even provide guidance on how boards should provide oversight, for example,

when the board asked for a cybersecurity audit, a CISO said they "steered [the board] in the direction of a cybersecurity maturity audit that made the most sense. They knew it was important, but didn't know what they were asking for." (Executive5).

Another proactive CISO action that facilitates their legitimacy with the board is competency signaling. In other words, CISOs can be deliberate in demonstrating and/or communicating their understanding of their specific company's strategy and vision. By aligning security priorities with their business's strategy, CISO demonstrate their executive mindset to the board. For example, two CISOs commented as follows:

> *It ends up being a cost-benefit analysis and a business discussion […] that's a leveler, that we're all businessmen […] It's not we're either all businessmen now or we're all security now. It's that, yes, we're both. They've now become fused, and you could advance one at the same time you're advancing the other. (Executive7)*

> *[T]hat's what starts to build the credibility, the trust, the relationships, where it's like, "Okay, security's here to literally be a partner and enabler of the business." (Executive11)*

Political action is another signal to the board that the CISO is an effective executive; this strategy will be discussed in more detail below, as it is a critical feature in the executive legitimating process.

Board Competency Perceptions and Legitimacy Reassessment

Access enables proactive engagement, and proactive engagement influences the board's perception of the CISO's competency and provides relevant evidence for updating the board's assessment of the CISO's legitimacy. These updates then lead to board support and endorsement of the CISO's initiatives, which facilitate increased access to the board. Importantly, board support directly feeds into the CISOs legitimacy cycle within the executive suite.

Board Endorsement and Support

Participants described how board support facilitates the C-suite's assessment of CISO legitimacy. This is consistent with the individual evaluators relying heavily on consensus opinion in their legitimacy evaluations (Bitektine and Haack 2015; Gould 2002), especially when consensus is created by those in authority. One CISO explained how board support leads to executive support in this way: "You leverage [the board] and educate them in a way that they'll say [to] the CEO or the CFO, 'You've got a good guy there. You need to really support him. If he needs more head count, you need to give it to him. If he wants to advance this model, it resonates with us.'" (Executive7)

Inclusion in the C-suite

Board endorsement of CISO initiatives leads to increased CISO inclusion in the C-suite. For example, one of the CISO participants shared an experience where the C-suite decided to disregard the CISO's concern about the security around a product release – the C-suite decided to "accept the risk." (P32) The board sided with the CISO, and said:

> *'We don't care about your release schedule. Go fix the vulnerability.' It caused a huge rift with the head of product, because they're not interested in kind of serving 'non-customer needs.' And yet, between the CFO, the general council, it did absolutely elevate [my role], showing that, 'Look, I'm being responsible to the organization and it's not about me, it's about my view of supporting what's right for the organization.' […] other people all of a sudden recognized that I'm not in my own little technical bubble, worried about my own world. There is a larger lens that I can look through as a CISO and help the company's longer-term value. (Executive11)*

Proactive Executive Engagement

A CISO can influence legitimacy reassessments through similar forms of proactive engagement, as with board interactions discussed above. As with developing relationships with the board, educating the C-suite provides an opportunity for relationship building. Trust between the CISO and other executives gains high

salience because of endemic conflicting priorities within the C-suite. CISOs build trust by cultivating an "on-the-same-team" perspective with other executives. One concrete action mentioned by a consultant that builds trust is to help other executives be prepared with knowledge on breaches and hot security topics:

> *There are things that a CISO can do if there's an external breach event that pops up in the news, proactively going to the C-suite and saying, 'Look, this thing happened, we may have the same kind of event; here's how we would handle it if we had the same kind of event.' Or, 'It's not likely we would have this kind of event but you may get asked about it, so I'm going to pre-arm you with talking points around what you might say.' Those kinds of things. So, there's a lot of relationship building that goes into the CISO role, 'soft skills' that a CISO needs to do to build the relationship with the C-suite so that they are seen as a subject matter expert, so they are seen as a confidential advisor when the time comes. (Consultant10)*

The above quote not only emphasizes the role of trust but also illustrates how a CISO can signal that they are a resource and trusted ally of the other executives.

Political action is another key form of proactive action that can lead to increased CISO legitimacy. Participants indicated that although CISOs often do not have the background and natural inclination to see their responsibilities through a political lens, ascension to the C-suite makes effective political awareness and deal-making imperative. A consultant said:

> *[As a CISO] you can't just check out from internal politics when you are leading an organization. Now that doesn't mean that you have to play the same game as everybody else […] but you can't disengage from it. You have to figure out how to make it work for you, so that your organization gets the influence and the resources that they need to be successful […] A lot of first-time CISOs are fumbling through trying to figure how [and] what to do and, as a result, they don't often get the respect from their peers or from their leadership that they actually need to be successful. (Consultant7)*

Executive Competency Perceptions, Legitimacy Reassessment, and Endorsement and Support

A CISO's proactive engagement with the C-suite catalyzes updates to the C-suite's perceptions of the CISO's competency and legitimacy as a member of the executive team. Greater legitimacy leads to greater CISO influence, facilitating executive endorsement and support for security program initiatives. Executive support also feeds back into opportunities for more board access and opportunities to build legitimacy with the board.

Security Program Outcomes

The increased legitimacy of CISOs in the eyes of the board and C-suite executives leads to improved security outcomes, not only in terms of an increased security budget and the prioritization of security concerns, but also in cultural support for security initiatives.

Discussion

Similar to the evolution of other executive positions (e.g., Zorn (2004), for the historical evolution of the chief financial officer), the CISO executive position is in a liminal state of ascendancy. With limited inter-firm norms, CISOs have an opportunity to build their intra-firm legitimacy and to shape norms for their influence within their own organizations, and collectively increase their stature as legitimate C-suite executives across economies. We anticipate that this ongoing research will make the following contributions.

Anticipated Contributions to Theory

First, we provide an understanding of how the legitimacy process works at the executive level in the context of two hierarchical groups, in which one group (the board of directors) has oversight over the other (the C-

suite). We provide a novel account of two interdependent legitimacy cycles for these groups, in which the hierarchy of groups plays an important role in the legitimating process.

Second, we contribute to legitimacy theory for individuals in general, and emergent corporate leaders in particular. While legitimacy theory has been applied to management initiatives and to the role of gender in executive legitimacy, little is known about the mechanisms by which legitimacy is cultivated. Previous research on corporate leadership legitimacy has focused on the legitimacy judgments of subordinates, and their attendant adherence to policies based on those judgments (Tyler 2006; Tost 2011). Our process model focuses on a junior executive's potential for entering a virtuous cycle of legitimating with more established and legitimate corporate leaders.

Third, our hierarchical legitimating process model provides new insight into how individuals can proactively motivate for beneficial reassessments of their legitimacy. Bitekine and Haack's (2015) legitimacy model focuses on the actions of legitimacy evaluators, whereas our model takes into account the proactive actions of the executive whose legitimacy is in question (in our case, the CISO) and the role those actions play in the legitimating process.

Fourth, despite the cruciality of the CISO role for the security of organizations (Steinbart et al. 2018), little IS research has examined CISOs and how their effectiveness can be increased. This research helps to address this important research gap, opening the door for future IS research on this topic.

Anticipated Contributions to Practice

This study provides evidence on why CISO access to the board is critical to successful security programs. We also provide explanations of how CISOs can increase their legitimacy with the board and the C-suite. While access to the board is an important first step, CISOs can proactively use that access to improve the board's legitimacy assessments, which then facilitates a virtuous cycle of more board support and greater board access. Board support in turn signals the legitimacy of the CISO to the executive team, which fosters inclusion and increased interactions of the CISO with the C-suite. Furthermore, our model can extend to other emergent executives, especially those from technical domains in terms of which boards are playing "catch up."

Our findings have implications for the current comment period for cybersecurity oversight regulation from the SEC. We demonstrate how the board's interactions with the CISO can directly and indirectly mitigate corporate cybersecurity risks.

Future Research Steps

We have some further steps to take to complete this research project. We need to complete our selective coding, that is, mapping our data to our emerging model, to refine the model, and to direct further data collection according to theoretical sampling. We believe we are currently in the last stages of interviewing, including returning to early participants with follow-up questions motivated by our findings and our emergent model. We will achieve theoretical saturation when later interviews cease to add new insights into the developed themes. To facilitate theoretical saturation, and as a later form of theoretical sampling, we will perform theoretical group interviews, both to finalize saturation and to provide insight into conundrums and areas where our data are sparse (Morse 2010, p. 241).

Conclusion

We used a grounded theory approach to investigate the contemporary challenges CISOs face as they ascend into the boardroom and the C-suite, and we developed a hierarchical CISO legitimating process model. Although CISOs may initially be hired for window-dressing, the virtuous cycle of legitimating can enable CISOs to rise to the inner circle of the executive suite and association with the board to achieve more success in developing effective security programs.

References

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.

Bryant, A., and Charmaz, K. 2007. *The Sage Handbook of Grounded Theory*. Sage.
Charmaz, K. 2002. "Qualitative Interviewing and Grounded Theory Analysis," in *Handbook of Interview Research: Context and Method,* J.F. Gubrium and J.A. Holstein (eds.). Thousand Oaks, CA: Sage Publications, Inc., pp. 675-694.
FTC. 2021. "Standards for Safeguarding Customer Information," in: *86 FR 70272*. Federal Trade Commission.
Glaser, B. G., and Strauss, A. L. 1967. "Grounded Theory: Strategies for Qualitative Research," *Chicago, lL: Aldine Publishing Company*).
Gould, R. V. 2002. "The Origins of Status Hierarchies: A Formal Theory and Empirical Test," *American Journal of Sociology* (107:5), pp. 1143-1178.
KPMG. 2021. "From Enforcer to Influencer: Shaping Tomorrow's Security Team."
Lempert, L. B. 2007. "Asking Questions of the Data: Memo Writing in the Grounded Theory Tradition," in: *The SAGE Handbook fo Grounded Theory,* A.C. Bryant, Kathy (ed.). SAGE Publications Ltd, pp. 245-264.
LogRhythm. 2021. "Security and the C-Suite: Making Security Priorities Business Priorities."
Lowry, M., Vance, A., and Vance, M. D. 2021. "Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity," *Available at SSRN 4002794*).
Magee, J. C., and Galinsky, A. D. 2008. "Chapter 8: Social Hierarchy: The Self-Reinforcing Nature of Power and Status," *Academy of Management Annals* (2:1), pp. 351-398.
Matavire, R., and Brown, I. 2013. "Profiling Grounded Theory Approaches in Information Systems Research," *European journal of information systems* (22:1), pp. 119-129.
Morgan, S. 2021. "List of Fortune 500 Chief Information Security Officers." Cybercrime Magazine.
Morse, J. M. 2010. "Sampling in Grounded Theory," *The SAGE handbook of grounded theory*), pp. 229-244.
Pfeffer, J. 1981. *Power in Organizations*. Marshfield, MA: Pitman Publishing.
Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., and Wu, D. T. 2020. "The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context," *Information Systems Research* (31:4), pp. 1240-1259.
Sarker, S., and Sarker, S. 2009. "Exploring Agility in Distributed Information Systems Development Teams: An Interpretive Study in an Offshoring Context," *Information Systems Research* (20:3), pp. 440-461.
SEC. 2022. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," in: *17 CFR Parts 229, 232, 239, 240, and 249*. Securities and Exchange Commission.
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.
Suchman, M. C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *The Academy of Management Review* (20:3), pp. 571-610.
Suddaby, R., and Greenwood, R. 2005. "Rhetorical Strategies of Legitimacy," *Administrative Science Quarterly* (50:1), pp. 35-67.
Tost, L. P. 2011. "An Integrative Model of Legitimacy Judgments," *Academy of management review* (36:4), pp. 686-710.
Tyler, T. R. 2006. "Psychological Perspectives on Legitimacy and Legitimation," *Annual Review of Psychology* (57:1), pp. 375-400.
Zorn, D. M. 2004. "Here a Chief, There a Chief: The Rise of the Cfo in the American Firm," *American sociological review* (69:3), pp. 345-364.