

# **The Problem of CISO Turnover: Toward a Theory of CISO Turnover**

**Early stage paper**

**Zeynep Sahin**  
Virginia Tech  
zeyneps@vt.edu

**Anthony Vance**  
Virginia Tech  
anthony@vance.name

**Jason Bennett Thatcher**  
Temple University  
jason.thatcher@temple.edu

## **ABSTRACT**

Due to the increasing number of data breaches and regulations that have elevated the role of the Chief Information Security Officer (CISO), the CISO position has become critical to organizations. Unfortunately, organizations are experiencing a high rate of CISO turnover, which has negatively impacted organizations in a number of ways. Existing research on turnover has typically focused on non-executive IT staff, CEOs, or the top management team (TMT). However, the CISO role has unique characteristics that set it apart from CIOs and other C-suite executives. As a result, there is a need for research to better understand why CISOs leave their jobs. To understand the drivers of CISO turnover, we propose to conduct a mixed-methods study. First, we will conduct a field interview study with CISOs using the lens of upper echelon theory to better understand the factors that lead to turnover. Then, we will conduct a fuzzy-set qualitative comparative analysis (fsQCA) of qualitative interview data to identify configurations that influence CISO turnover and develop a middle-range theory based on upper echelon theory. This paper aims to contribute to IS research by developing a CISO turnover theory and determining configurations of factors that lead to CISO turnover intention using a set-theoretic approach.

## ***Keywords***

Chief information security officer, CISO, IT executive turnover, CISO turnover, upper echelon theory, fuzzy-set qualitative comparative analysis (fsQCA), mixed-methods.

## **INTRODUCTION**

Due to the high-profile nature of cybersecurity incidents and their negative impact on organizations, the CISO role has become critical to organizations' efforts to mitigate cybersecurity risks (Moon et al. 2018; Steinbart et al. 2018). Recognizing the destructive impact of data breaches on organizations, regulators have begun to propose rules to elevate the role of the CISO. For example, the Federal Trade Commission has issued a rule requiring financial institutions to employ an individual responsible for cybersecurity, typically the CISO, who reports to the board of directors at least annually (FTC 2022). The US Securities and Exchange Commission has proposed rules that require public companies to designate a CISO role, identify to whom the CISO reports and declare the CISO's expertise (SEC 2022). The New York State Department of Financial Services has updated its influential Cybersecurity Regulation to require financial institutions to ensure that CISOs "have adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain a cybersecurity program" (NYDFS 2022, p. 6).

Despite the CISO's increasingly important role in mitigating cybersecurity risk and driving regulatory compliance, organizations are experiencing an alarming rate of CISO turnover (Haworth 2020; Sullivan 2022). CISO turnover negatively impacts organizations in a number of ways. Because cybersecurity executives have extensive knowledge of their organizations' critical security systems and services, when they leave, (1) the organization loses the institutional and operational knowledge needed to avoid cybersecurity risks, which in turn opens the door to cyber

adversaries (Rosiek 2018), (2) cybersecurity initiatives are interrupted and cybersecurity strategies must be rebuilt (Johnson and Goetz 2007), (3) recruiting and retaining security executives is a growing concern due to the shortage of CISO talent and the increasing demand for CISO professionals (Rosiek 2018). According to Nominet's report on CISO stress, the average CISO tenure is 26 months (Haworth 2020).

Although articles by academics and practitioners have acknowledged that challenges to the CISO role can lead to turnover, little if any research has examined the drivers of CISO turnover. Existing IS research on IT executive turnover has examined the influence of IT failures and security breaches on CIO turnover (Banker and Feng 2019; Benaroch and Chernobai 2017; Li 2021) and on CEO/CFO turnover (Masli et al. 2016). However, little is known about the unique drivers of CISO turnover. This is because each type of executive has different responsibilities, span of control, and contributions to organizational outcomes (Hambrick 2007; Hambrick and Mason 1984), causing each executive to have different reasons to exit (Andrus et al., 2019).

CISOs have unique characteristics that set their experience apart from that of CIOs and other C-suite executives. Therefore, there is a need for research to better understand why CISOs leave their jobs. Some factors that distinguish CISO positions from other executive positions are (1) recent regulations that have put pressure on organizations to have a CISO with a reporting line to the board, (2) increasingly frequent and high-profile security incidents have captured the attention of boards and raised the profile of CISOs within organizations, (3) most CIOs and other C-suite executives have hierarchical power and are members of the top management team (TMT) (Karahanna and Watson 2006). In contrast, CISOs are typically subordinate to CIOs (Haislip et al. 2021) or positioned two or more levels below the 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). CISOs, on the other hand, while also holding the title of "chief," are seen primarily as managing downside risk, and there is no consensus on the strategic role of CISOs in organizational performance (Lowry et al. 2022). All of these factors set the experience of CISOs apart from that of CIOs and other C-suite executives. Given the critical role that CISOs play in their organizations, the characteristics that make this position unique, and the negative consequences of CISO turnover, there is a need for researchers and practitioners to better understand the determinants of CISOs' desire to leave their positions. Therefore, our study aims to address this need by examining the factors that cause CISOs to leave their jobs. Thus, our first research question is:

**RQ1: What organizational and personal factors lead to CISO turnover intention?**

Because turnover is a complex employee behavior, multiple combinations of factors may explain an individual's behavior (Liu et al. 2017). Thus, to better understand the relationship between organizational and personal factors and CISO turnover intention, we go beyond the linear paradigm of examining the unique contribution of each factor to the outcome and examine how combinations of these factors influence CISO turnover intention. This allows us to examine asymmetric relationships between the configurations of determinants that drive CISO turnover, and how different interactions of these factors influence CISO turnover intention. For example, while some configurations of factors may contribute to high levels of CISO turnover intention, another configuration of factors may lead to low levels of CISO turnover intention. Therefore, our second research question is:

**RQ2: What configurations of factors influence high and low levels of CISO turnover intention?**

To address these research questions, we will use upper echelon theory (Carpenter et al. 2004; Hambrick 2007; Hambrick and Mason 1984) as a theoretical lens because it explains how individual characteristics of executives influence their perceptions and decisions. We will use a mixed-methods design approach with two sequential, equally-weighted studies (Venkatesh et al. 2013; Venkatesh et al. 2016). In Study 1, because the factors leading to CISO turnover have not been previously studied, we will conduct a qualitative field study with CISOs to identify organizational and personal factors that lead to CISO turnover. Study 1 addresses our first research question. Following a developmental purpose (Venkatesh et al. 2016), Study 2 will build on the results of Study 1, in which we will apply a fsQCA (Mattke et al. 2022; Misangyi et al. 2017; YoungKi et al. 2020) to the identified factors to determine configurations of factors leading to CISO turnover, thus addressing our second research question.

We anticipate that this study will make several contributions to research and practice. First, our research contributes to IS research by identifying organizational and personal factors that lead to security executive turnover. Because CISOs are essential employees in securing their organizations, understanding and reducing their turnover can have a significant impact on organizational outcomes. Second, beyond identifying the factors, we aim to explain how configurations of factors influence CISO turnover intentions. Third, we contribute to theory by using a set-theoretic approach that allows us to identify complex interactions among factors that lead to CISO turnover in order to better explain CISO turnover. Finally, we expect that this study will provide practitioners with insights to better understand the factors that lead to CISO turnover and can help organizations develop strategies to reduce CISO turnover that negatively impacts them.

The rest of the paper unfolds as follows. First, we discuss related research on IT employee turnover. We then present our theoretical lens and methodological approach. Finally, we conclude the paper with the expected contributions to research and practice.

## **LITERATURE REVIEW**

In this section, we provide research on IT executive and nonexecutive-IT employee turnover.

### **Research on Executive and Nonexecutive-IT-Employee Turnover**

Given the powerful influence of executives on organizational outcomes and the high costs associated with executive turnover, the question of why high-level and low-level executives would want to leave their firms is an important phenomenon (Andrus et al. 2019). While studies of executive turnover in the management literature have focused on either CEO turnover or the group level in the TMT (Andrus et al. 2019), IS researchers have focused on the link between IT-related deficiencies and CEO/CFO turnover (Masli et al. 2016) or CIO turnover (Li 2021), and the influence of data security breaches on CIO/CTO turnover (Banker and Feng 2019; Benaroch and Chernobai 2017).

Nonexecutive IT employee turnover phenomena have been studied since the 1980s. Research on IT employee turnover shows that IT professionals may have unique characteristics that make their turnover process different from other occupations (Baroudi 1985; Bartol 1983; Igbaria et al. 1994; Igbaria and Siegel 1992; Mourmant et al. 2009; Niederman et al. 2007). Thus, IS researchers have examined a variety of organizational, environmental, and individual factors that lead IT workers to leave their jobs. The seminal studies show that organizational commitment, job satisfaction and its antecedents, role ambiguity and role conflict (Baroudi 1985); and professionalism and perceived rewards (Bartol 1983), are the leading predictors of IT employee turnover intentions.

Several studies use organizational commitment (Ahuja et al. 2007; Maier et al. 2015; Thatcher et al. 2002) and job satisfaction (Dinger et al. 2015; Joseph et al. 2007; Maier et al. 2015) to predict IT employee turnover intention.

IS research shows that job perceptions, such as work overload and work exhaustion, are particularly salient for IT employees (Ply et al. 2012). Thus, some IS researchers have focused on the influence of work exhaustion and its antecedents on voluntary turnover intentions. For example, Moore (2000) found that autonomy, role ambiguity, role conflict, and fairness of rewards are the antecedents of work exhaustion, which can lead to IT employee turnover. Building on Moore's (2000) model of IT employee turnover, several studies have empirically tested the antecedents and consequences of work exhaustion. The results show that work exhaustion is highly related to low organizational commitment and high turnover intention (Ahuja et al. 2007); and low job satisfaction and high depersonalization (Shih et al. 2013). In addition, recent studies on IT employee turnover have increased our understanding regarding the factors that can lead IT personnel to quit their jobs. For example, the influence of personality (Maier et al. 2015); the impact of psychological contract violations (Moquin et al. 2019), and the features of technology (Tomer et al. 2022).

## **THEORETICAL LENS**

We will use upper echelon theory (Carpenter et al. 2004; Hambrick 2007; Hambrick and Mason 1984) as a basis for interviewing CISOs to understand the unique organizational and personal factors that lead CISOs to turnover. Upper echelon theory suggests that idiosyncratic differences in the leadership characteristics of executives are linked to their cognitive bases and values, which influence their perceptions and, ultimately, their strategic decisions (Carpenter et al. 2004; Hambrick and Mason 1984). Thus, upper echelon theory posits that observable characteristics,

such as age, personality, tenure in the organization, education, and power in the organizational structure, reflect unique cognitive styles, beliefs, and values (Hambrick and Mason 1984) that can influence organizational outcomes, such as turnover (Carpenter et al. 2004). For example, a recent study explains how the presence of the CIO in the TMT and the characteristics of the board of directors, such as educational background and experience, influence organizations' strategy choices and outcomes with respect to AI implementations (Jingyu et al. 2021).

Recent updates to upper echelon theory have proposed two moderators-managerial discretion and executive job demands-that may influence the predictive power of the theory (Hambrick 2007). According to Hambrick (2007), discretion stems from environmental (e.g., industry type), organizational (e.g., TMT or board composition), or personal factors (e.g., executive personality). In addition, they note that the demands of the job on executives make the relationship between executive characteristics and organizational outcomes more salient because high job demands can lead to mental shortcuts; thus, executives' decisions reflect their past experiences and dispositions (Hambrick 2007).

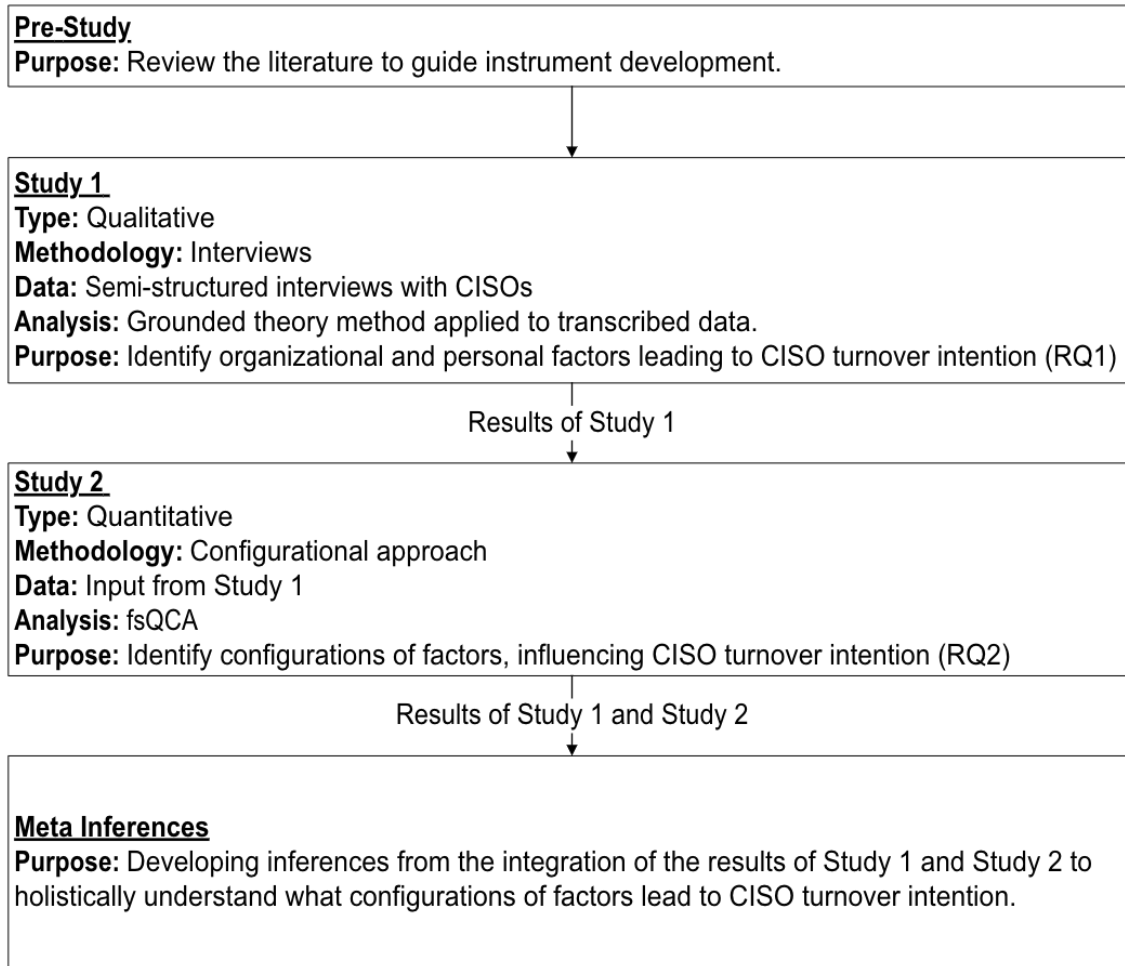
Prior studies of the CISO role have stated the following as job demands: lacking power, influence, credibility, and role identity within organizations (Ashenden and Sasse 2013; Karanja 2017; Karanja and Rosso 2017; Lowry et al. 2022; Maynard et al. 2018; Shayo and Lin 2019; Whitten 2008); increasing cybersecurity threats (Maynard et al. 2018; Neville-Neil 2019; Shayo and Lin 2019); lack of executive and board support (Johnson and Goetz 2007; Monzelo and Nunes 2019); limited budget for cybersecurity initiatives (Johnson and Goetz 2007; Monzelo and Nunes 2019); human resistance to change, and an underdeveloped organizational cybersecurity culture (Johnson and Goetz 2007; Monzelo and Nunes 2019; Triplett 2022); firing due to a security breach (Shayo and Lin 2019); lack of consensus among C-suite executives on the need for a CISO (Karanja 2017;



Karanja and Rosso 2017; Shayo and Lin 2019) and on the strategic role of CISOs (Maynard et al. 2018; Onibere et al. 2017); and balancing security and business needs (Kayworth and Whitten 2010; Moon et al. 2018; Shayo and Lin 2019).

## **RESEARCH DESIGN AND METHODOLOGY**

In this study, we will use a mixed-methods design, which includes qualitative and quantitative approaches (Tashakkori and Teddlie 1998). We will follow the guidelines provided by Venkatesh et al. (2013) and Venkatesh et al. (2016). According to these guidelines, the purpose of our study falls under the category of "developmental" because "questions for one strand emerge from the inferences of a previous strand (sequential mixed methods)" (Venkatesh et al. 2013, p. 26). In terms of phases or strands of research, our research design is categorized as "mixed-method multistrand" (Venkatesh et al. 2016, p. 443), where we identify constructs that lead to CISO turnover through a qualitative study and then configure them through a quantitative study (see Figure 1). We also follow a sequential sampling strategy and data analysis, as the results of the qualitative study are used in the quantitative study (Venkatesh et al. 2016). In terms of the priority of the methodological approach, our study falls under "equivalent-status designs" (Tashakkori and Teddlie 1998), where "both qualitative and quantitative approaches about equally to understand the phenomena of interest" (Venkatesh et al. 2016, p. 444). Lastly, in terms of our epistemological perspective, we adopt multiple paradigms. In line with the "dialectical paradigm stance" (Venkatesh et al. 2016, p. 442), we adopt an interpretive approach in the qualitative study and then a positivist approach in the quantitative study.



**Figure 1. Sequential Equivalent Status Mixed-Methods Design**

## Study 1 Factors Leading to CISO Turnover Intention

Study 1 will use a multi-case qualitative field study of approximately 20 CISOs from medium and large U.S. public companies to understand the organizational and personal factors that lead CISOs to leave their jobs. Study 1 thus answers our first research question, which asks about the organizational and personal factors that lead to CISO turnover. To do so, we will use grounded theory methodology to iteratively analyze the interview data (Bryant and Charmaz 2007; Charmaz 2014; Glaser and Strauss 1967) using NVivo version 12 software. To locate participants, we will use existing contacts from the researchers' relationships developed through interactions on campus,

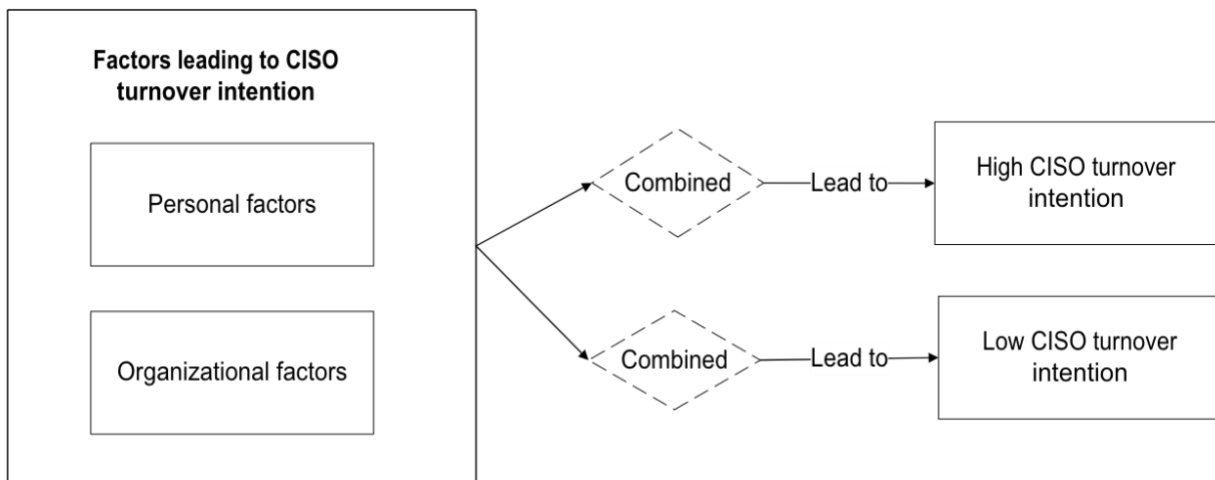
at events, or at practitioner conferences. We will also use a snowball sampling technique, asking participants for potential interviewees. Each semi-structured interview is expected to last approximately one hour. We plan to begin the interviews by asking about the participants' tenure at their current and previous employers, and then ask open-ended questions about why the participants left their organizations and the factors that influenced their decisions. We will then ask follow-up questions to get participants to elaborate on the factors that led or would lead them to leave their jobs.

With the participant's consent, we will record the interview using Zoom. We will use a professional third-party transcription service. After each interview, we will begin coding the anonymized and transcribed interview data. As part of the iterative coding process, each researcher will code the interview transcripts and write a brief memo reflecting key findings regarding factors leading to CISO turnover and new codes. The research team will then meet to discuss new codes, concepts, and potential questions for future interviews. We will then write our overarching theme memos and begin selective coding to identify factors that lead to CISO turnover. We will continue to interview CISOs until we reach theoretical saturation. To guide our coding process, we will use upper echelon theory to understand how organizational and personal characteristics of CISOs lead to CISO turnover.

## **Study 2 Configurations of Factors Leading to CISO Turnover Intention**

The factors identified in Study 1 will be used in Study 2 to address our second research question, which asks about configurations of factors that influence low and high levels of CISO turnover intention. Study 2 aims to identify configurations of factors that contribute to CISO turnover intention, which will allow us to construct a nomological network of personal and organizational factors that lead to CISO turnover. To do this, we will take a configurational approach and use the

fsQCA method (Misangyi et al. 2017; Ragin 2014; YoungKi et al. 2020) The fsQCA uses a set theory approach and allows us to determine how the interplay between the factors or sets of factors identified in Study 1 influence CISO turnover intention. Therefore, consistent with upper echelon theory, we will use fsQCA to examine how personal characteristics of CISOs and organizational factors combine into different configurations to increase (high turnover) or decrease (low turnover) CISO turnover intention. Figure 2 illustrates our research approach.



**Figure 2. Research Approach**

We will follow the neo-configurational approach (Misangyi et al. 2017), which allows us to test sufficient configurations of factors that lead to an outcome such as high or low turnover intention. We plan to use the fsQCA Version 3 software package in R and analyze our data in three steps to determine which configurations are associated with high or low turnover intention: (1) calibration of cases, (2) analysis of necessary factors for low and high turnover intention, and (3) analysis of sufficient configurations for our outcomes.

The first step is calibration, in which we will calibrate qualitative interview data into fuzzy sets following the recommendations of Basurto and Speer (2012) to determine the threshold for the

membership in sets (Misangyi et al. 2017). In other words, we will prepare qualitative interview data to be loaded into the fsQCA version 3.0 software package in R for analysis, and we will convert all construct values into fuzzy sets. To do this, we will develop membership anchor points, which are "the three main thresholds that structure a fuzzy set" (Basurto and Speer 2012, p.161). As suggested by Basurto and Speer (2012), we will determine the quantitative anchor points of fuzzy-set values for cases depending on the level of detail in the interview data. For example, fuzzy set value=1 indicates full membership or high state in a fuzzy set, and fuzzy set value=0 indicates non-membership or low state in a fuzzy set.

The second step is the analysis of necessary conditions for our dependent variable. Necessary condition is defined as "a condition that always exists when the outcome exists" (Matke et al. 2021a, p. 271). This analysis allows us to determine how and which combinations of factors can lead to the same dependent variable (Misangyi et al. 2017). In other words, this analysis allows us to know whether a particular set of factors is necessary for CISOs to develop high or low turnover intentions. In this study, a necessary factor for high CISO turnover intention is always present when a CISO has high turnover intention. For example, does a specific factor such as "lack of organizational support" always exist for CISOs to have high turnover intentions? The same logic applies to low CISO turnover intent. If a single factor exceeds the consistency threshold of 0.90 (Schneider and Wagemann 2012) and a coverage threshold of 0.60 (Ragin 2006), it means that this necessary condition exists. Therefore, in this study, we will use the proposed coverage threshold of 0.60 and the consistency threshold of 0.90. The consistency threshold is used to assess "the degree to which cases sharing a given condition or combination of conditions agree in exhibiting the outcome in question...the coverage threshold, on the other hand, assesses the degree to which a cause or causal combination accounts for instances of an outcome" Ragin (2006, p. 292). It is

also recommended to check whether the relevance of necessity (RoN) score is at least 0.60 to avoid inconsequential necessary conditions (Mattke et al. 2021b; Ragin 2006).

The third step is to analyze sufficient configurations for our dependent variables. This analysis allows us to determine whether a combination of factors is sufficient to lead to high or low levels of CISO turnover. For example, this analysis can determine whether different configurations of certain organizational or personal factors always contribute to high levels of CISO turnover despite all other factors. To do this, we create a truth table containing all possible configurations of factors. We will then apply three thresholds: a consistency threshold of 0.8, a frequency threshold of 3, and "a proportional reduction in inconsistency (PRI) threshold of 0.75" to identify sufficient configurations (Mattke et al. 2022, p. 221). Finally, we will apply Quine-McCluskey algorithm to simplify the sufficient configuration (Ragin 2008).

## **EXPECTED CONTRIBUTIONS AND FUTURE RESEARCH DIRECTIONS**

Our research will contribute to theory, research, and practice. First, our research will contribute to IS research by providing a better understanding of the CISO turnover problem and insights into how to reduce CISO turnover that negatively impacts organizations. Second, our study goes beyond the traditional correlation-based approach of examining the linear relationship between a dependent variable and various independent variables. This study conceptualizes and analyzes the causal complexity of various factors leading to CISO turnover intention. Third, this study contributes to theory by developing a theory that reflects configurations of different organizational and personal conditions that drive CISOs to leave their jobs. Since merely identifying key drivers is not enough to understand individual behavior (Liu et al. 2017), our study takes a configurational approach that can explain the complex interdependencies of factors that influence CISO turnover intention. Furthermore, providing a theoretical explanation for CISO turnover can have significant

implications for organizational outcomes, as CISOs are essential digital leaders in securing their organizations.

Given the shortage of CISO talent, the increasing demand for CISOs, and the negative consequences of high rates of CISO turnover that organizations face, this research may also have important implications for practitioners. We expect that this study will provide practitioners with insights to better understand the factors that lead to CISO turnover and can help organizations develop strategies to reduce CISO turnover by addressing specific combinations of the factors we identify.

Our study has several limitations. First, we focus only on CISOs of U.S.-based public companies, and thus cannot make any claims for CISOs of private companies or CISOs of other countries. The second limitation of our study is that we are testing intentions to divest rather than actual behavior to divest. This is a limitation of our study because intentions do not always lead to actual turnover behavior, although turnover intention is the strongest predictor of actual turnover. (Thatcher et al. 2002).

Because our study cannot capture actual turnover behavior, future research could examine actual CISO turnover behavior through longitudinal studies. In addition, future research can examine the consequences of CISO turnover. For example, future research can examine the influence of CISO turnover on CISOs' cultivation of legitimacy among corporate leaders, as "CISOs often lack legitimacy in the eyes of the board and the C-suite" (Lowry et al. 2022, p. 2). In this sense, frequent turnover and short tenure of CISOs may affect CISOs' relationship building with boards and C-suite teams (Kaspersky, 2018), which in turn negatively affects their legitimization process (Lowry et al. 2022). This is because legitimacy theory posits that individuals can earn legitimacy by gaining the trust of their aspirational peer groups through relationship building (Bitektine and

Haack 2015; Tost 2011). Thus, if a CISO has a short tenure, they can lose the opportunity to build relationships with organizational leaders (Kaspersky 2018). Lastly, future studies can examine whether the high rates of CISO turnover influence other organizational outcomes, such as security program effectiveness and CISOs' job performance, using upper echelon theory.

## REFERENCES

- Ahuja, M. K., Chudoba, K. M., Kacmar, C. J., McKnight, D. H., and George, J. F. 2007. "IT Road Warriors: Balancing Work-Family Conflict, Job Autonomy, and Work Overload to Mitigate Turnover Intentions," *MIS Quarterly* (31:1), pp. 1-17.
- Andrus, J. L., Withers, M. C., Courtright, S. H., and Boivie, S. 2019. "Go Your Own Way: Exploring the Causes of Top Executive Turnover," *Strategic Management Journal* (40:7), pp. 1151-1168.
- Ashenden, D., and Sasse, A. 2013. "CISOs and Organisational Culture: Their Own Worst Enemy?," *Computers & Security* (39), pp. 396-405.
- Banker, R. D., and Feng, C. 2019. "The Impact of Information Security Breach Incidents on CIO Turnover," *Journal of Information Systems* (33:3), pp. 309-329.
- Baroudi, J. J. 1985. "The Impact of Role Variables on IS Personnel Work Attitudes and Intentions," *MIS Quarterly* (9:4), pp. 341-356.
- Bartol, K. M. 1983. "Turnover Among DP Personnel: A Casual Analysis," *Communications of the ACM* (26:10), pp. 807-811.
- Basurto, X., and Speer, J. 2012. "Structuring the Calibration of Qualitative Data as Sets for Qualitative Comparative Analysis (QCA)," *Field Methods* (24:2), pp. 155-174.
- Benaroch, M., and Chernobai, A. 2017. "Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes " *MIS Quarterly* (41:3), pp. 729-A726.
- 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.
- 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.
- Charmaz, K. 2014. *Constructing Grounded Theory*, (Second edition. ed.). London ;: SAGE Publications.
- Dinger, M., Thatcher, J. B., Treadway, D., Stepina, L., and Breland, J. 2015. "Does Professionalism Matter in the IT Workforce? An Empirical Examination of IT Professionals," *Journal of the Association for Information Systems* (16:4), pp. 281-313.
- FTC. 2022. "Standards for Safeguarding Customer Information," in: 86 FR 70272. Federal Trade Commission: pp. 71509-71511. Available at: <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314>
- Glaser, B. G., and Strauss, A. L. 1967. *Grounded theory: Strategies for qualitative research*. Chicago, IL: Aldine Publishing Company.



- 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.
- Haworth, R. 2020. "The CISO Stress Report," Nominet.
- Igbaria, M., Meredith, G., and Smith, D. C. 1994. "Predictors of Intention of IS professionals to Stay with the Organization in South Africa," *Information & Management* (26:5), pp. 245-256.
- Igbaria, M., and Siegel, S. R. 1992. "The Reasons for Turnover of Information Systems Personnel," *Information & Management* (23:6), pp. 321-330.
- 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.
- Joseph, D., Ng, K.-Y., Koh, C., and Ang, S. 2007. "Turnover of Information Technology Professionals: A Narrative Review, Meta-Analytic Structural Equation Modeling, and Model Development," *MIS Quarterly* (31:3), pp. 547-577.
- Karahanna, E., and Watson, R. T. 2006. "Information Systems Leadership," *IEEE Transactions on Engineering and Management EM* (53:2), pp. 171-176.
- Karanja, E. 2017. "The Role of the Chief Information Security Officer in the Management of IT Security," *Information & Computer Security*.
- 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.
- 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.
- Li, W. 2021. "The Strategic Role of CIOs in IT Controls: IT Control Weaknesses and CIO Turnover," *Information Management* (58:6), p. 103429.
- Liu, Y., Mezei, J., Kostakos, V., and Li, H. 2017. "Applying Configurational Analysis to IS Behavioural Research: A Methodological Alternative for Modelling Combinatorial Complexities," *Information Systems Journal* (27:1), pp. 59-89.
- Lowry, M. R., Sahin, Z., and Vance, A. 2022. "Taking a Seat at the Table: The Quest for CISO Legitimacy," *ICIS 2022 Proceedings*.
- Maier, C., Laumer, S., Eckhardt, A., and Weitzel, T. 2015. "Who Really Quits? A Longitudinal Analysis of Voluntary Turnover Among IT Personnel," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* (46:4), pp. 26-47.
- Masli, A., Richardson, V. J., Watson, M. W., and Zmud, R. W. 2016. "Senior Executives' IT Management Responsibilities," *MIS Quarterly* (40:3), pp. 687-708.
- Mattke, J., Maier, C., Reis, L., and Weitzel, T. 2021a. "Bitcoin Investment: A Mixed Methods Study of Investment Motivations," *European Journal of Information Systems* (30:3), pp. 261-285.
- Mattke, J., Maier, C., Weitzel, T., E. Gerow, J., and B. Thatcher, J. 2022. "Qualitative Comparative Analysis (QCA) In Information Systems Research: Status Quo, Guidelines, and Future Directions," *Communications of the Association for Information Systems* (50), pp. 208-240.

- Mattke, J., Maier, C., Weitzel, T., and Thatcher, J. B. 2021b. "Qualitative Comparative Analysis in the Information Systems Discipline: A Literature Review and Methodological Recommendations," *Internet research* (31:5), pp. 1493-1517.
- 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.
- Misangyi, V. F., Greckhamer, T., Furnari, S., Fiss, P. C., Crilly, D., and Aguilera, R. 2017. "Embracing Causal Complexity: The Emergence of a Neo-Configurational Perspective," *Journal of Management* (43:1), pp. 255-282.
- Monzelo, P., and Nunes, S. 2019. "The Role of the Chief Information Security Officer (CISO) in Organizations," *CAPSI 2019 Proceedings*.
- 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.
- Moore, J. E. 2000. "One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals," *MIS Quarterly* (24:1), pp. 141-168.
- Moquin, R., K. Riemenschneider, C., and L. Wakefield, R. 2019. "Psychological Contract and Turnover Intention in the Information Technology Profession," *Information Systems Management* (36:2), pp. 111-125.
- Mourmant, G., Gallivan, M. J., and Kalika, M. 2009. "Another Road to IT Turnover: The Entrepreneurial Path," *European Journal of Information Systems* (18:5), pp. 498-521.
- Neville-Neil, G. V. 2019. "What is a Chief Security Officer Good for?," *Communications of the ACM* (62:10), pp. 26-27.
- Niederman, F., Sumner, M., and Maertz Jr, C. P. 2007. "Testing and Extending the Unfolding Model of Voluntary Turnover to IT Professionals," *Human resource management: Published in cooperation with the school of business administration, the university of michigan and in alliance with the society of human resources management* (46:3), pp. 331-347.
- NYDFS. 2022. "New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies," in: *Second Amendment to 23 NYCRR 500*. New York Department of Financial Services. Available at: [https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2\\_text\\_20221109\\_0.pdf](https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf)
- Onibere, M., Ahmad, A., and Maynard, S. 2017. "The Chief Information Security Officer and the Five Dimensions of a Strategist," *PACIS 2017 Proceedings*.
- Ply, J. K., Moore, J. E., Williams, C. K., and Thatcher, J. B. 2012. "IS Employee Attitudes and Perceptions at Varying Levels of Software Process Maturity," *MIS Quarterly* (36:2), pp. 601-624.
- Ragin, C. C. 2006. "Set Relations in Social Research: Evaluating Their Consistency and Coverage," *Political Analysis-ANN ARBOR THEN OXFORD-* (14:3), pp. 291-310.
- Ragin, C. C. 2008. "Redesigning Social Inquiry: Fuzzy Sets and Beyond." Chicago: University of Chicago Press,
- Ragin, C. C. 2014. "The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies." Berkeley, California: University of California Press,
- Rosiek, T. 2018. "Chief Information Security Officer Best Practices for 2018: Proactive Cyber Security," *Cyber Security: A Peer-Reviewed Journal* (1:4), pp. 361-367.
- Schneider, C. Q., and Wagemann, C. 2012. *Set-theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis*. Cambridge University Press.

- SEC. 2022. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," in: 7 *CFR Parts 229, 232, 239, 240, and 249*. Securities and Exchange Commission. Available at: <https://www.sec.gov/rules/proposed/2022/33-11038.pdf>
- 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.
- Shih, S. P., Jiang, J. J., Klein, G., and Wang, E. 2013. "Job Burnout of the Information Technology Worker: Work Exhaustion, Depersonalization, and Personal Accomplishment," *Information and Management* (50:7), pp. 582-589.
- 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.
- Sullivan, P. 2022. "Maintaining Your Compliance Strategy During (and After) CISO Turnover." ISACA. Available at: <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/maintaining-your-compliance-strategy-during-and-after-ciso-turnover>
- Tashakkori, A., and Teddlie, C. 1998. *Mixed Methodology: Combining Qualitative and Quantitative Approaches*. Thousand Oaks, Calif.: Sage.
- Thatcher, J. B., Stepina, L. P., and Boyle, R. J. 2002. "Turnover of Information Technology Workers: Examining Empirically the Influence of Attitudes, Job characteristics, and External Markets," *Journal of Management Information Systems* (19:3), pp. 231-261.
- Tomer, G., Mishra, S. K., and Qureshi, I. 2022. "Features of Technology and Its Linkages with Turnover Intention and Work Exhaustion Among IT Professionals: A Multi-Study Investigation," *International Journal of Information Management* (66), p. 102518.
- Tost, L. P. 2011. "An Integrative Model of Legitimacy Judgments," *Academy of Management Review* (36:4), pp. 686-710.
- Triplett, W. J. 2022. "Addressing Human Factors in Cybersecurity Leadership," *Journal of Cybersecurity and Privacy* (2:3), pp. 573-586.
- Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54.
- Venkatesh, V., Brown, S. A., and Sullivan, Y. W. 2016. "Guidelines for Conducting Mixed-Methods Research: An Extension and Illustration," *Journal of the Association for Information Systems* (17:7), pp. 435-495.
- 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.
- YoungKi, P., Fiss, P. C., and El Sawy, O. A. 2020. "Theorizing the Multiplicity of Digital Phenomena: The Ecology of Configurations, Causal Recipes, and Guidelines for Applying QCA," *MIS Quarterly* (44:4), pp. 1493-1520.