MIS Quarterly

RESEARCH ARTICLE

UNITED WE STAND, DIVIDED WE FALL: AN AUTOGENIC PERSPECTIVE ON EMPOWERING CYBERSECURITY IN ORGANIZATIONS[1]

Alexandra Durcikova
Division of MIS, Price College of Business, University of Oklahoma
Norman, OK U.S.A. {alex@ou.edu}

Shaila M. Miranda
Information Systems Department, Sam M. Walton College of Business, University of Arkansas
Fayetteville, AR U.S.A. {SMiranda@walton.uark.edu}

Matthew L. Jensen
Division of MIS, Price College of Business, University of Oklahoma
Norman, OK U.S.A. {mjensen@ou.edu}

Ryan T. Wright
McIntire School of Commerce, University of Virginia
Charlottesville, VA U.S.A. {rtw2n@virginia.edu}

Cybersecurity groups navigate complex, challenging environments in their mission to protect their organizations. They experience uncertainty from adaptive threats from external attackers and unpredictable stakeholders. Under such volatility, business groups operate best when they are psychologically empowered. Recognizing the potential for empowerment to reduce organizational risk, we sought to learn how cybersecurity groups come to be (dis)empowered and how this (dis)empowerment is sustained. Instead of the conventional view of the empowerment process as designed, we advance an emergent view of the empowerment process. We abductively surface this process from our case analyses of 15 U.S. organizations. We offer three insights: First, organizations with empowered cybersecurity groups enjoy an enhanced level of protection from breaches. Second, we highlight generative rules through which groups become empowered—via their bridging initiatives that co-opt stakeholders into security behaviors and stakeholder responsiveness to bridging, rather than unilaterally applied buffering initiatives. Third, we highlight reinforcing rules through which empowered states persist—via the group's ability to safeguard organizational information assets, thereby ensuring cybersecurity group viability, continued bridging, and motivated stakeholder responsiveness. For practitioners, our study underscores the interdependence between cybersecurity groups and their stakeholders in securing an organization and posits processes for empowering cybersecurity groups.

Keywords: Cybersecurity group, autogenesis, empowerment, bridging, buffering

[1] Likoebe Maruping was the accepting senior editor for this paper. John D'Arcy served as the associate editor. The Online Supplement is available at https://osf.io/kev3f/

Introduction

The *cybersecurity group* is the *organizational workgroup responsible for identifying, detecting, and responding to cybersecurity threats, and for recovering from cybersecurity breaches* (e.g., Yoo et al., 2020). They do so by crafting and implementing cybersecurity strategies and promoting security compliance behaviors in their organizations (Li et al., 2023). The size, location, and structure of cybersecurity groups vary across organizations: the groups are sometimes a distinct organizational unit overseen by a chief information security officer (CISO) who reports directly to the executive level; at other times, they are a subunit within the information technology (IT) unit, legal unit, or another business unit. Cybersecurity incidents threaten the welfare of organizations and their stakeholders via regulatory fines and sanctions, loss of intellectual property and proprietary data, and reputational damage. Cybersecurity groups therefore serve a critical role in organizational risk mitigation (Arsenault 2023). Global cybersecurity spending has consequently grown from $3.5 billion in 2004 (Ross 2016) to an estimated $188.3 billion in 2023 (Gartner 2022). However, cybersecurity groups are often thwarted by the very people they are charged with protecting. For example, organizational leaders often ignore, circumvent, or sideline the cybersecurity group during important organizational deliberations and actions (KPMG 2022; Lowry et al., 2022). Moreover, stakeholders balancing their primary work with cybersecurity policy compliance often resist cybersecurity initiatives (e.g., Karjalainen et al., 2019; Wright et al., 2023).

The adaptive, emergent threats cybersecurity groups face from external attackers, coupled with unpredictable stakeholder behaviors, create a dynamic work environment for them. Dynamism results in high operational uncertainty (Mitchell et al., 2011). Organizations respond best to such uncertainty when their business groups are *empowered* (Cordery et al., 2010; Faraj & Sambamurthy 2006). Workgroups enjoy a state of empowerment—termed psychological empowerment—when they experience a collective sense of *competence* and *autonomy*, and view their endeavors as *meaningful* and *impactful* (Kirkman & Rosen, 1999). In contrast, disempowered groups lack confidence in their collective competence, a sense of autonomy, and the feeling that their work is meaningful and impactful to their organizations.

The empowerment of cybersecurity groups is therefore critical to their ability to successfully mitigate organizational risks, yet we have little knowledge on this topic. We therefore sought to understand how cybersecurity group empowerment (or disempowerment) comes about, i.e., the process of empowerment. Studies of organizational empowerment processes have focused on organizational efforts to structurally empower workgroups through formal decentralization of authority (Maynard et al., 2012), yet such efforts often fall short (e.g., Biron and Bamberger 2010). This slippage between empowerment design processes and concomitant empowerment states has prompted researchers to look for emergent rather than designed empowerment processes, e.g., via processes of connecting and communicating (van den Berg et al., 2022). Synthesizing these perspectives, we define *empowerment as a duality of state and process—a transient, recursively-produced state in which a group experiences itself as collectively competent and autonomous and the emergent process through which that experience comes about.* This view of empowerment as an emergent process resonates with the autogenesis paradigm premise that "the process of organizing can best be modeled at the level of observed actions and interactions of individuals" (Drazin & Sandelands, 1992, p. 231). Within this paradigm, we addressed the following research questions: *What are the emergent processes through which cybersecurity groups come to be (dis)empowered to address threats to their organizations? How is this (dis)empowerment sustained?*

To address these research questions, we used a multiple case study method, incorporating interviews with cybersecurity leaders of 15 US organizations (from energy, higher education, financial, and government sectors); dialogues with additional informants from these organizations; and archival data on security breaches, litigation, and press coverage of the organizations. We used an abductive approach within the autogenesis paradigm to surface the emergent rules through which the groups came to be (dis)empowered and the behavior patterns producing them.

Our insights inform theory by challenging common ontological assumptions regarding cybersecurity groups and their role in protecting organizations. Unlike cybersecurity perspectives that emphasize the group's dominion over stakeholders, our findings underscore the importance of empowering the cybersecurity group and the cybersecurity group's reliance on stakeholders for that empowerment. Empowerment is initialized when cybersecurity leaders perceive stakeholder responsiveness to their co-optive, bridging initiatives; it is sustained by the cybersecurity group's tangible successes in securing their organization. In contrast, when cybersecurity groups limit their bridging or perceive a lack of stakeholder responsiveness to bridging, a spiral of disempowerment commences; the spiral is reinforced by ensuing failures and constraints by other business units. This emergent view of structuring the cybersecurity function departs from formal approaches to cybersecurity governance, underscoring the relational mechanisms essential for complex organizing. For practitioners, our research highlights the nature of the mutual dependency between cybersecurity groups and their stakeholders necessary for securing an organization. For researchers and practitioners, our work suggests the need for a paradigm shift—from viewing the cybersecurity function as compliance-seeking to viewing it as stakeholder-engaging. In other words, a united stand empowers the cybersecurity group, while divisiveness disempowers it.

Study Background

To set the context for our study of cybersecurity group empowerment, we briefly review the literatures with which our research engages: cybersecurity governance, perspectives on empowerment, and organizational perspectives on structural emergence.

Cybersecurity Governance

Cybersecurity groups confront persistent and adaptive external threats. In doing so, they must respond to incidents (D'Arcy and Basoglu 2022; Nikkhah and Grover 2022), learn from them (Mehrizi et al., 2022), and develop awareness of countermeasures to combat them (Li et al., 2023). When implementing countermeasures, they must then manage internal objectives that conflict with them (Karjalainen et al., 2019; Wright et al., 2023). They must balance risk reduction with innovation, caution with speed, and value production with value consumption (Schinagl et al., 2022). They must further contend with noncompliant and maladaptive stakeholder responses to countermeasures (Balozian et al., 2023) and their inability to deter personally motivated threats posed by insiders (Burns et al., 2023). In doing so, cybersecurity leaders and their organizations must consider how best to structure and govern the cybersecurity function. Though centralization of IT governance has been shown to be conducive to improved cybersecurity (Liu et al., 2020), knowledge sharing and inclusion in governance (Dhillon et al., 2020) and sharing of cybersecurity responsibilities (Yoo et al., 2020) have also been shown to improve organizational cybersecurity. Thus, prior research offers conflicting insights on cybersecurity governance.

Organizations faced with uncertainty perform optimally when their business groups are empowered (Cordery et al., 2010; Faraj and Sambamurthy 2006). Cybersecurity uncertainty accrues not only from the dynamic threats posed by attackers but also from the unpredictability of stakeholder behaviors. A viable governance alternative therefore is empowering organizations' cybersecurity groups, and the cybersecurity literature has begun to attend to their potential. For example, Yoo et al. (2020) considered cybersecurity groups' perceptions of their collective efficacy—one aspect of empowerment (Lee & Koh, 2001). They found the self-efficacy of individual cybersecurity group members and their internal knowledge sharing to positively impact beliefs in the self-efficacy of the collective and, subsequently, of cybersecurity outcomes (Yoo et al., 2020). Researchers have also examined the empowerment of stakeholders (Dhillon et al., 2020). But we lack a holistic understanding of how the cybersecurity group comes to be empowered.

Perspectives on Empowerment

There are two perspectives on empowerment within organizations. The first is the perspective on the *psychological empowerment* of the employee. Psychological empowerment is a state characterized by four cognitions: *competence*, *autonomy*, *meaningfulness*, and *impact* (Kirkman & Rosen, 1999; Lee & Koh, 2001). It entails individuals' subjective experience of competence and autonomy and their beliefs that their work is meaningful and valuable (Chen et al., 2007; Kirkman & Rosen, 1999). In this state, empowered individuals perceive future outcomes as contingent on their own actions and demonstrate proactive behaviors and resilience when facing failure (e.g., Rappaport, 1984). In contrast, disempowered individuals lack self-confidence and agency, experience a diminished sense of control, and an inability to effect meaningful change in their lives. They avoid situations requiring risk-taking or asserting themselves (Seibert et al., 2011). When individuals continually face disempowerment, they may enter a vicious cycle where their sense of agency, motivation, and well-being are negatively impacted, leading to a decline in their ability to effectively respond to the situations they encounter (Berti & Simpson, 2021).

The concept of psychological empowerment has been extended from the individual to the group level (Kirkman & Rosen, 1997; Kirkman & Rosen, 1999), recognizing a consistent homology across both levels (Seibert et al., 2011). At the group level, empowerment is conceptualized along the same dimensions as individual empowerment: *competence*, *autonomy*, *meaningfulness*, and *impact* (Seibert et al., 2011). As with individual empowerment, when a group feels empowered, its members believe in their collective capability to successfully accomplish their work tasks, that they have collective autonomy in how they approach those tasks, and that their work is intrinsically meaningful and valuable (Seibert et al., 2004).

The meaningfulness of cybersecurity work is well established due to the pervasiveness of cybersecurity threats and the severity of consequences to organizations. Likewise, successful cybersecurity work is necessarily impactful, enabling organizations to withstand prevailing and emergent threats. Meaningfulness and the impact of cybersecurity work are therefore likely to be relatively invariant across organizations. However, cybersecurity groups vary in competence based on the human and technological resources at their disposal and the autonomy they enjoy by virtue of their governance structure. In the literature, these two dimensions of the psychological empowerment concept intersect with other organizational behavior concepts. To clarify the meaning of these dimensions, Lee and Koh (2001) established their correspondence to associated concepts, noting that competence "is analogous to agency beliefs, personal mastery or *self-efficacy*" and autonomy

"addresses the *locus of causality*" (p. 686, italics added). We have previously discussed self-efficacy in the context of cybersecurity groups. The locus of causality refers to whether actors view themselves as the origin of their behaviors or as a pawn to external forces (Ryan & Connell, 1989). We therefore conceptualize the psychological empowerment of cybersecurity groups in terms of their self-efficacy and locus of causality.

The second perspective on empowerment in organizations is *structural empowerment*, i.e., through the design of organizational structures and work practices (Mills & Ungson, 2003), "away from top-down control systems toward high involvement practices where power, knowledge, information and rewards are shared with employees in the lower echelons" (Spreitzer, 2008, p. 55). The objective of structural empowerment is psychological empowerment (Conger & Kanungo, 1988). Yet research has repeatedly shown that the relationship between structural and psychological empowerment is imperfect (e.g., Biron & Bamberger, 2010; Mills & Ungson, 2003; Perkins & Zimmerman, 1995). A second view of structural empowerment therefore maintains that empowerment processes are ongoing, organic, and cannot simply be designed (Drydyk, 2013; Rowlands, 1995). In this view, the empowerment process is inherently relational (Conger & Kanungo, 1988), entails give and take between actors (Bachrach & Baratz, 1963), and an ability to negotiate influence (Rowlands, 1995). The process is ecologically situated, unfolding in contexts with disparate affordances for empowerment (Pratto, 2016).

Building on views of empowerment as a psychological state and organic process, we define *empowerment as a duality of state and process, i.e., as a transient, recursively produced state in which a cybersecurity group experiences itself as collectively competent and autonomous and the emergent process through which that experience comes about*. This is a structurationist view of empowerment, one in which empowerment is both structure that enables and constrains action and action itself (Giddens, 1984). Here, "structure" refers to the social beliefs and expectations created and sustained through action (Giddens, 1979). This structurationist view therefore highlights the constant renewal of the state of empowerment through ongoing enactments.

The autogenesis paradigm helps us unpack this empowerment duality, i.e., the interplay of action and structure in the (re)production of a state of empowerment (Giddens, 1984). Unlike design views of organizational structure, the autogenic paradigm—with its roots in structuration theory—conceptualizes structure as cognitive, emerging from interactions among entities and temporary in nature (Drazin et al., 2004). Through the process of organizing, these cognitive structures become shared and durable over time. In the following sections, we will provide an overview of the autogenic paradigm and the concept of structural interpenetration, which are relevant to understanding empowerment in this context.

Autogenesis: A Process Perspective on Structural Emergence

"Autogenesis is the idea that organization can be explained by observation and categorization of the interactions of independent actors whose behavior is governed by a system of recursively applied rules" (Drazin & Sandelands, 1992, p. 236). It is a social constructionist perspective that seeks out these rules that generate habituated (inter)action patterns. This perspective is well-suited to understanding how cybersecurity groups are organized for three reasons. First, it enables us to study how organizational units develop practices before they become taken-for-granted within and across organizations (Tolbert & Zucker, 1996), i.e., before isomorphism takes hold. Second, an autogenic perspective is relevant for "theorizing and modeling dynamic systems" (Drazin et al., 2004, p. 170), which is characteristic of cybersecurity administration where novel threats are the norm (Maddison, 2020). Third, the perspective spotlights the structuring role of the seemingly mundane as "individuals are typically unaware of the rules governing their actions" (Drazin & Sandelands, 1992, p. 238). Consequently, it allows us to recognize the collective influence of organizational actors, not limited to "key" decision-makers, in shaping *new* groups.

Drazin and Sandelands (1992) noted that autogenic organizing can be examined in terms of three types of structure. First, it can be examined in the *observed structures*, i.e., *the visible state organizational arrangements* such as centralization or division of labor. Second, organizing can be examined in the *elemental structure*, i.e., *the actions and interactions that constitute observed structures*. Third, organizing can be examined in terms of *deep structure*, i.e., *the tacit rules that govern actions and interactions.* In organizational and MIS studies, following Gersick (1991), deep structures have been viewed as organizations' core values, organizational arrangements, power distribution, technologies, and control systems (Silva & Hirschheim, 2007). In contrast to these perspectives, which do not distinguish between the visible organization and activity patterns and the invisible rules from which they emerge, the autogenic quest is for the core values and rules that produce recurrent (inter)action patterns and organizational states. They are the "relatively stable, largely implicit, and continually recurring processes and patterns that underlie and guide surface, observable events and actions" (Heracleous & Barrett, 2001, p. 758).

Because the autogenesis of an organizational group is not unconstrained, we also consider how structures *interpenetrate*, i.e., *reinforce or contradict each other* (Benson, 1977; Drazin et al., 2004; Giddens, 1979; Robey & Azevedo, 1994). Interpenetration at the structural level means agency is constrained by *multiple* structures. In other words, cybersecurity group and stakeholder agency is shaped by structures beyond the emergent cybersecurity group. When extant structures interpenetrate with the emergent cybersecurity group in a contradictory manner, they reduce its degrees of freedom and weaken the emergent structure (Giddens, 1979).

We consider three organizational structures that may interpenetrate with the emergent cybersecurity structure: IT, public relations (PR), and legal. The IT unit is responsible for developing and administering organization information resources (e.g., databases) and provides the technical infrastructure for cybersecurity (e.g., firewalls). PR units are involved in cybersecurity because breaches negatively affect organizational reputation and how the organization manages the crisis can shield it from further negative outcomes (Gwebu et al., 2018; Nikkhah & Grover, 2022). Finally, because security breaches expose organizations to lawsuits (Romanosky et al., 2014), their legal units play an active role in cybersecurity (Kahn & Brock, 2007). While interpenetration also implies that the cybersecurity structure reinforces or contradicts other organizational structures, since our interest is in the cybersecurity function, we focus solely on interpenetration implications for cybersecurity.

Methods

Given the nascent understanding of the cybersecurity group, we used an abductive, multiple case study method. We focused on medium- to large-sized organizations, which are commonly targeted by external attackers and more likely to have cybersecurity groups than small organizations. Industries represented included energy, higher education, government, and finance. In choosing case organizations, we strove for diversity, rather than representativeness, which is "difficult to defend" with small numbers and therefore a less relevant concern in case research (Stake, 1995, p. 5). Anonymized descriptions of the 15 organizations studied are in Table 1.

Figure 1 summarizes our case study activities following Yin (1994). Specifically, we annotated each task with its contribution to validity and reliability. At the design stage, using multiple cases increases the positivist case study rigor (Sarker et al., 2013), enhancing external validity and permitting insights into contrasting conditions via multiple replications (Yin, 1994). We tempered our positivist stance in two ways. We pursued a soft positivism that drew upon concepts that preexisted our study and permitted concepts to emerge from the data (Madill et al., 2000; Ravishankar et al., 2011). Our second qualification of the positivist stance derives from the autogenesis ontological assumption of a dynamic and emergent reality (Drazin et al., 2004). This means that despite the expected tendency for observed realities to reproduce themselves, the observed states of empirical cases are subject to change. It also means that the generative and reinforcing rules autogenic investigators seek may change through accidental variation of actions, exogenous shock, and/or as cognizant actors deliberately intervene (King, 2000). We therefore offer the identified states, activities, and rules of cybersecurity groups as tentative conjectures rather than definitive laws. In doing so, we also characterize our approach as post-positivist, i.e., as a point of departure for future work rather than as a theory to be confirmed (Silva, 2007). Design also entailed developing the interview protocol (see Appendix A), vetting it with two cybersecurity officers and a security consultant, and refining it based on their feedback. In addition to eliciting information about the organization of the cybersecurity units, units' overall approaches to cybersecurity, and the challenges they experienced, our interview protocol probed the units' spam and phishing email detection techniques. By focusing interviewee attention on these specific threats, we obtained insight into their sense of agency in combating cybersecurity threats and about their relationships with their stakeholders.

We interviewed 17 cybersecurity leaders from the 15 organizations—one each from thirteen organizations and two from two organizations. Twelve (of 17) informants were their organizations' highest-ranked cybersecurity staff (see Table 1); the remaining five were delegated by the highest-ranked cybersecurity staff and held responsibilities for cybersecurity management. Though guided by the protocol, we followed up on issues informants raised during interviews. Most interviews lasted one hour. Interview transcripts averaged ~20 single-spaced pages per organization (details in the Data Analysis Activities section of the Online Supplement[2]). Through the study, we iteratively dialogued with 34 secondary informants from the focal organizations, including CIOs, other IT and cybersecurity personnel, legal and PR leaders, and lead users, spending more than 20 hours in phone, video, and in-person conversations with them. We followed up on four of these interactions via email and communicated exclusively via email with one informant. The diverse data sources enabled data triangulation and enhanced our research's external validity (Stake, 1995). After analyzing the data from secondary informants, no need for reanalysis emerged due to the consistency between primary and secondary sources (see Table 3 in the Data Analysis Activities section and Table 1 in the Connecting Methods to Findings section in the Online Supplement). Nonetheless, the initial interviewees remained our primary informants as we believed they were in the best position to provide insights into how their groups came to be structured.[3] Finally, we undertook data source triangulation and thickened our understanding of the organizations by collecting archival data on their breaches, security- and privacy-related litigation, and exposure in news media.

[2] The Online Supplement is available at https://osf.io/kev3f/

[3] Our approach focusing on primary informants is similar to approaches taken in other inductive/abductive work (e.g., Deken et al., 2016; Hatch et al., 2015; Rafaeli & Sutton, 1991). The value of primary informants hinges on informant competence (e.g., Kumar et al., 1993) and our primary informants were in the best position to report on the subjective experience of empowerment within their organizations.

Table 1. Description of Cases

Industry	Case	Primary informant title	Additional informants	Breaches[a] (most recent)	Number of employees			News articles[b]	Security lawsuits[c]
					Total	Security	IT		
Energy	NRG1	Director of IT Security & Risk Management	2	0	5,500	17	350	1.31	2
	NRG2	Manager of Information Security	2	0	4,200	2	160	0.01	0
	NRG3	Information Security Manager	3	0	2,700	12	110	0.04	0
	NRG4	Manager of Digital Security	2	0	7,000	50	670	1.03	1
	NRG5	Director of Information Security	3	0	5,000	10	160	0.46	0
Higher education	HIED1	CISO and Executive Director for Customer Relations	1	1 (2007)	5,000	6	350	0.22	0
	HIED2	CIO	0	7 (2008)	2,400	10	140	1.51	1
	HIED3	Information Security Manager	3	0	1,500	2	80	0.25	2
	HIED4	CISO	7	10 (2017)	3,000	11	250	0.41	2
	HIED5	CIO	5	9 (2019)	4,900	10	200	0.39	0
	HIED6	CISO	2	5 (2013)	15,500	6	800	0.73	3
Govern-ment	GOV1	System Integration Manager	0	2 (2009)	1,200	50	550	5.09	10
	GOV2	Information Security Officer	1	8 (2013)	1,300	12	200	16.17	8
Defense contractor	GOV3	CIO	1	3 (2019)	230	1	2	9.37	4
Insurance	FNCL	VP of Software Solutions	3	2 (2015)	1,600	15	200	0.15	0

Note: [a]From Privacy Rights Clearinghouse plus 7 other sources. Please see the Online Supplement for details—https://osf.io/kev3f/, Data Collection Activities. [b]Number of articles per day between 2011 and 2015 (from ABIInform). [c]Number of security- or privacy-related lawsuits between 2011 and 2015 (from WestLaw)

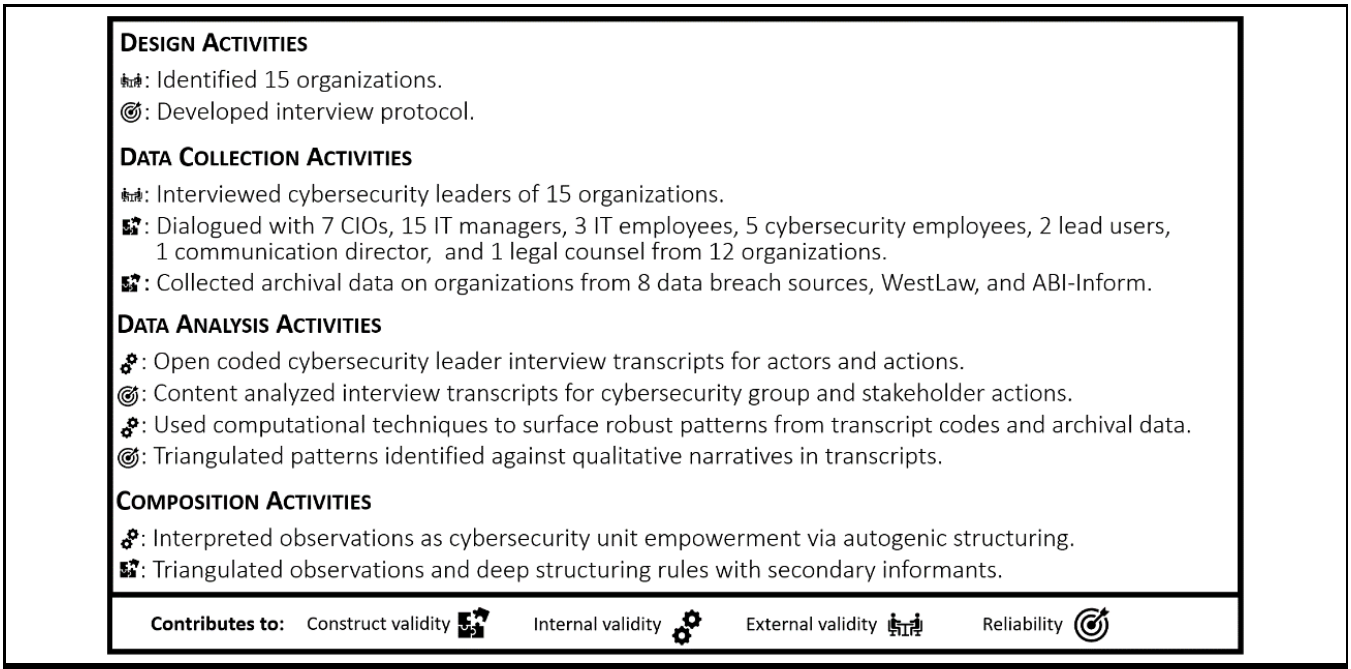


Figure 1. Study Overview

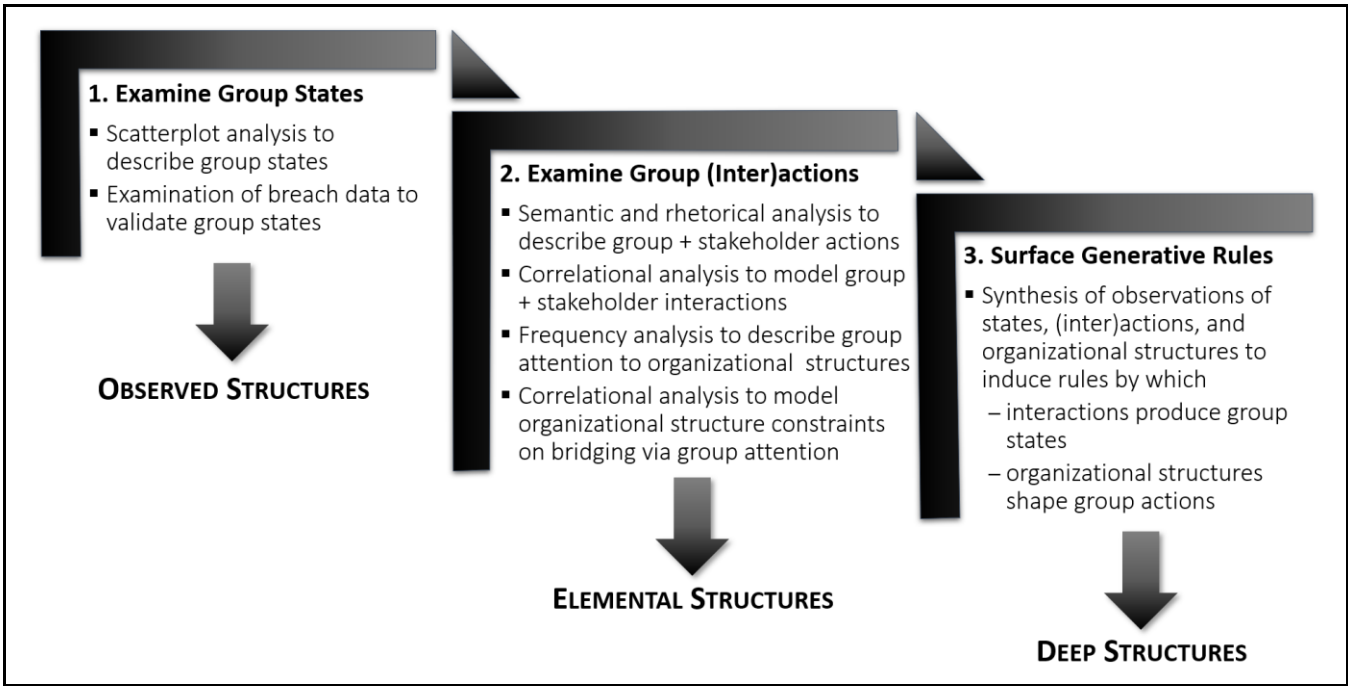


Figure 2. Interpreting Patterns to Surface Autogenic Structures

To kickstart our data analysis, two of the researchers met weekly, iteratively open-coding the interview transcripts and discussing their codes. Since these two researchers represented different epistemologies, this collaboration contributed to the validity of our insights through investigator triangulation (Stake, 1995). Through this coding process, we surfaced 28 concepts about problems faced by cybersecurity leaders, behaviors they initiated, and behaviors initiated by various organizational stakeholders. Via axial coding, we then focused on 11 core concepts, for which we compiled a codebook. See Appendix B for definitions of our core axial concepts and their relation to open codes. We iterated between the data from which we surfaced codes and existing literature to lexically frame and define each concept (Miranda et al., 2022). Our high-level concepts were: (1) whether the informant was addressing a security *problem* or a *solution*; (2) whether the actor was the *cybersecurity group*, *organizational stakeholder*, or an *outside agent*; (3) whether solutions enacted by the cybersecurity group represented *bridging* or *buffering*; and (4) whether organizational stakeholder actions represented *prioritizing*, *equivocating*, *avoiding*, or *thwarting*.

We then did a content analysis to ascertain the frequency with which the concepts occurred in interview transcripts. These frequency counts revealed cybersecurity leaders' emphasis on each concept. The coding unit was a sentence. We refined the codebook and trained two research assistants to use it to code interview transcripts. Interrater reliability, computed as Cohen's kappa, averaged 0.82. Coding disagreements were resolved via discussions among coders and researchers.

One author assumed responsibility for the computational analyses, pattern surfacing, and theorizing and developed memos to share with the research team. Again, the conceptual and methodological diversity of the research team contributed to theoretical and methodological triangulation (Stake, 1995). As our focus shifted to the deep structures associated with empowerment, we realized that these structures were implicit and often "outside of actors' intention or awareness" (Boutyline & Soter, 2021, p. 743). We therefore sought computational techniques enabling us to look beyond our informants' spoken words to underlying meanings. We iterated between high-level computational analyses to surface patterns and granular qualitative analyses of transcripts to interpret the patterns and retain sight of the specificities of each organization.

Finally, we zoomed in on the observed, elemental, and deep structures described by Drazin and Sandelands (1992), as summarized in Figure 2. To understand the observed structure, we considered the positioning of cybersecurity groups within their organizations, responsibility for cybersecurity tasks, and the number of security employees. We found that these conventional ways of thinking about structure, i.e., reporting relationships, division of labor, did not differentiate among our cases in an illuminating way. Instead, we inferred observed structure as the state of the cybersecurity groups from the totality of leader statements. We considered elemental structures represented in leader statements about their groups' and stakeholders' actions and inferred (inter)actions based on relative levels of cybersecurity and stakeholder actions.

Based on our conceptualization of structure as a cognitive trace induced by interactions, we assessed interpenetration of IT, legal, and PR structures with the cybersecurity group structure in the following manner. Since our case study commenced in 2015 and we wished to understand the role that extant organizational structures played in structuring the cybersecurity group, our assessments targeted those structures in place in 2015. For the IT structure, this was the level of IT staffing relative to organizations' total employees in 2015, a critical IT capability component (Bharadwaj, 2000). For legal and PR structures, we focused on events in the 5 years immediately preceding this period, i.e., 2011-2015 because temporally proximate events engender cognitive traces that interpenetrate in autogenesis (Drazin & Sandelands, 1992). Given the strong correlation between the number of lawsuits and the size of the legal department (Alvarado-Vargas & Zou, 2018), we assessed the strength of the legal structure as the proportion of organizations' total lawsuits between 2011 and 2015 that were security- or privacy-related, permitting us to control for "deep pocket" organizations' susceptibility to lawsuits. Because PR department size is positively associated with organizational concerns with their image (Markham, 1996), we assessed the PR structure strength as negative media coverage, i.e., the proportion of negative affect words in news articles about the organization between 2011 and 2015 (the 5 years immediately preceding this study).[4] Such coverage shapes organizational action because a negativity bias makes us more prone to act upon negative, rather than positive, events (Tversky & Kahneman, 1981). Considering only the proportion of negative words also precluded the contamination of findings by extraneous factors such as organization size and visibility. We then assessed interpenetration as (1) the relationship between the strength of these structures and cybersecurity leaders' attention to them and (2) how that attention consequently shaped cybersecurity group action.

We synthesized observations to surface generative and reinforcing rules, i.e., the deep structures, that give rise to extant states of cybersecurity groups and their stakeholder interactions. Throughout these endeavors, as groupings of cases emerged, we employed replication logic to confirm that cases within each emergent group behaved similarly in relation to the observed, elemental, and deep structures surfaced (Eisenhardt, 1989). To promote construct validity, research team members presented our findings to three different industry groups, which were supportive of the results and had positive feedback that did not oppose our findings (e.g., Yin, 1994). We thus ascertained the applicability of our findings to practitioners (Rosemann & Vessey, 2008).

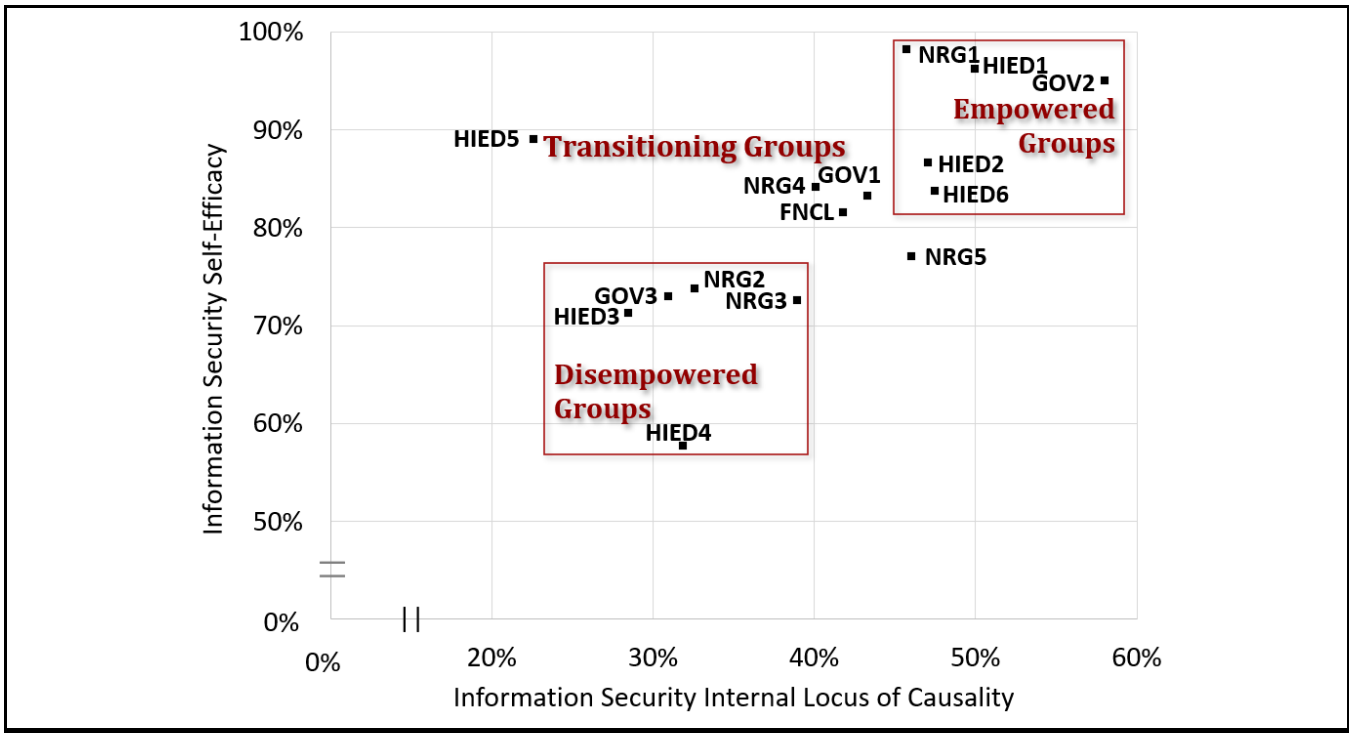


Figure 3. States of Cybersecurity Groups

[4] This was assessed using the SentimentR package, but scores correlated strongly with those produced by the Linguistic Inquiry and Word Count (LIWC) software (Tausczik & Pennebaker, 2010).

Findings

The autogenic perspective seeks to understand the state of an organization, or its observed structure based on its elemental structures, i.e., microlevel (inter)actions, to reveal the deep structures or rules that are enacted in those (inter)actions. Below, we abductively derive an autogenic model of how cybersecurity group and stakeholder actions, along with other organizational structures, engender an empowered cybersecurity group structure[5].

Observed Structure: Cybersecurity Group States

As noted earlier, conventional views of structure shed little light on how and why cybersecurity differed across the organizations studied. We therefore sought an alternate understanding of structure. Our coding of the actor (grammatical subject) in informants' statements about cybersecurity revealed their locus of causality; whether informants were describing a problem or solution revealed their self-efficacy—these two dimensions correlated with each other ($r = 0.58$).[6] Figure 3 (above) represents the sample organizations along these dimensions. (Note, locus of causality levels vary between 20% and 60%; self-efficacy between 50% and 100%.) Below, we describe each dimension and the resulting grouping of cybersecurity groups.

Locus of Causality

We define a *cybersecurity group's locus of causality* as its *subjective assessment of its ability to influence its behaviors* (Deci & Ryan, 1985). Drawing on existing research on the concept (e.g., Turban et al., 2007), we interpreted the proportion of interview statements in which the group was the subject or initiator of actions (relative to other agents such as users, management, and external actors) as groups' locus of causality. We interpreted a higher proportion of statements in which the cybersecurity group was the subject as revealing greater agency for cybersecurity and reflecting a higher *internal locus of causality.*[7] Such leaders believed that their own actions determined desired or undesired outcomes, as illustrated in the following interview excerpts:

> *We do awareness campaigns and phishing campaigns to try to educate people all the way through things that are more on the technical side. We maintain firewalls to obtain email security gateways. We do response, and we also do risk assessment, so we can try to assess the current posture of our environment.* (NRG4)

> *… awareness is our number one thing that we're doing through different campaigns...The work guys, the field guys generally have weekly huddles, and as a part of those weekly huddles, now we're trying to interject some reminders about cybersecurity.* (NRG5)

When agents other than the cybersecurity group were more often the subject of informants' statements, we interpreted the statements as revealing lower agency—i.e., a lower internal locus of causality for the group. This is reflected in the following interview excerpts:

> *They [senior management] let me hire one [other security person], finally.* (NRG2)

> *HR has a nasty habit here of not removing adjuncts, so we have adjuncts that haven't taught in three years, but they'll actually still be a current employee.* (HIED3)

Self-Efficacy

A *cybersecurity group's self-efficacy* is *its belief in its collective ability to perform a task* (Judge & Bono, 2001). Collective self-efficacy influences the goals of the collective, the efforts they invest, and their persistence in the face of failure (Bandura, 1986, p. 449). It has been found to enhance workgroup information security effectiveness (Yoo et al., 2020). We interpreted the proportion of statements in which the group was the subject of a statement describing solutions rather than problems as reflecting cybersecurity group self-efficacy. The following interview excerpts capture high cybersecurity group self-efficacy:

> *We have a training group… We offer some online training through things like a [intranet] setting where computer-based training is available... In the last two years, we have rolled out the Securing the Human online training environment. We first sourced about 1,200 seats to go out to our high-risk areas.* (HIED1)

> *We also have quarterly meetings with technology liaisons, individuals who take messages back to their group ... We perform regular phishing exercises and can track who clicks on a link.* (GOV2)

In contrast, the following excerpts capture low cybersecurity self-efficacy, i.e., a lack of confidence in the group's capability to secure their organization:

[5] See the Online Supplement (Table 1 in Connecting Methods to Findings) for a detailed mapping of our methods to our findings.

[6] Bounds on this correlation, obtained via a jackknifing approach of excluding each observation in turn, were 0.50 to 0.81.

[7] Note: We speak only of a higher versus lower internal locus of causality, not an internal versus external locus of causality.

I think this organization is most vulnerable to a mistake made by an employee. And by that, I mean classifying data the wrong way and storing it in a public location or inadvertently emailing the incorrect data to the wrong party. (GOV3)

Until the [HIED3] has a really costly major breach, we're not…they're not going to dedicate staff to it… For the majority of the time, we were doing this with one FTE, our sister institution was doing it with four FTE. (HIED3)

Empowered vs. Disempowered Cybersecurity Groups

Given the recognized impact and meaningfulness of the cybersecurity function, we characterize cybersecurity empowerment in terms of self-efficacy and locus of causality. Figure 3 depicts a set of organizations at the upper right with a high internal locus of causality and high self-efficacy (above the median values for both dimensions). We characterize the state of cybersecurity groups in these organizations as *empowered*. Cybersecurity leaders of these organizations believed cybersecurity was important to their stakeholders and that their groups were up to the challenge of securing their organizations. They expressed optimism, viewed their future as dependent on their behavior, and showed resiliency, as evident in these quotes:

My perspective … is that [cybersecurity] is a valued partner with the business … The ... atmosphere is … very much for information security… We do phishing tests, … we look at … user groups that are higher risk or susceptible to phishing attacks. (NRG1)

We take every opportunity we can to personally get in front of as many groups. (HIED1)

The President and first VP realized the importance of security and they will send out emails to all staff making them aware of things that they need to be cognizant of. (GOV2)

[Cybersecurity] is a … highly valued role in our organization, so we spend a lot of time on it… [Cybersecurity is] also one of the few areas where I can make budget requests and typically I get funded. (HIED2)

We've implemented some new governance structures in the past year where we reached out to each of the unit heads, with a unit broadly being a vice president or dean-level individual …, where the unit head was reminded that they're ultimately responsible for their area … and that they had to designate an individual to be their point person for implementing security within the unit. (HIED6)

Toward the bottom left of Figure 3 is a set of organizations with low internal locus of causality and low self-efficacy (below the median for both dimensions). We characterize these cybersecurity groups as *disempowered*. These groups had poor top management support or were inadequately resourced for cybersecurity. They expressed pessimism and low expectations that their behaviors would impact outcomes. Others (GOV3 and NRG3) shared the cybersecurity mandate with other organizational groups. Their sense of constraint is evident in these quotes:

Security and electronic assets and electronic information was not really considered to be a high priority. (NRG2)

I don't know the true statistics [percent of people that fall for mock phishing attacks] … that's put out by [headquarters]. I haven't had that shared with me yet. (GOV3)

You would think … higher ed would be able to learn from their peers [about the importance of cybersecurity], but I've just given up any hope of that happening. A year ago, we purchased [cloud storage] services through the Internet2 agreement, and that's completely email driven. They…blanketed everybody with emails … Enter your account information [including] your social security number. It was legit. We're our own worst enemy. It's … harder to tell people what to watch for. This is why we're so vulnerable. (HIED3)

The policy statements all end with the same general language of, failure to follow company policy may result in disciplinary action up to and including termination, but that's just kind of a vague, standard punishment threat that we put on all policy statements. We don't really have any benefits or punishments that are specifically designed for security. (NRG3)

Leadership do care about security, but with the challenges of being higher education and keeping information freely available, that can be difficult and hostile amongst colleges ... As far as training resources and learning resource, we don't have any out there right now; it's on our roadmap to create this training program. I don't even think the employee handbook really covers all the computer security policy. (HIED4)

Transitioning Cybersecurity Groups

From Figure 3, we notice that two groups—HIED5 and NRG5—exhibit scores above the median for one of the dimensions (internal locus of causality, self-efficacy) but below the median on the other. The HIED5 leader understood that everyone, regardless of expertise, needed to be involved for cybersecurity to be successful. This recognition reduced the observed level of locus of causality. However, the leader also evinced high self-efficacy in defending the organization from threats, as apparent in the following excerpt:

> *We've got a multi-million-dollar investment that the institution has made through the CIO to provide everyone with these tools. You have an ISP [information security policy] that will require people to use them. You have an information security office that will be part of the education and training efforts… We will also be working with deans, vice chancellors, through the various committees, whether it's HR committees, graduate student committees, student assembly, and throughout the employee environment to let them know that this is coming, that it's critical to the institution to have, and it will require their time and attention.* (HIED5)

NRG5's leader reported having authority to enact security strategies but felt the organization lacked salient know-how. Thus, the locus of causality was high, but self-efficacy was low. Initiatives implemented (e.g., training, ISPs) were unsuccessful. Despite the recently added CISO position and independent cybersecurity group, the work required seemed overwhelming, and the organization lacked mechanisms to set cybersecurity priorities.

> *We're in the process of building everything from a … security operations center to outlining what strategies we will use around technology, as well as ensuring that we are from a process and procedure perspective meeting the expectations of our board as well as others from a governmental perspective. And security was an element of that, but in the last five months the combined focus that the government has as well as other external factors, we have made a determination to go ahead and segment off a security organization.* (NRG5)

The three organizations—NRG4, GOV1, and FNCL1—had some top management support and cybersecurity resources and capabilities but experienced some obstacles, reducing the locus of causality and/or self-efficacy levels. Consider the following excerpts:

> *Most people feel as though it's the [cybersecurity group's] job to do security. [Responsibility] is not pervasive enough in the organization: those that do have an understanding play some part [in cybersecurity], they probably are more minor role … Yeah, and their [compliance on policies is] not great … but if you just look at the general usage sort of policies, they're not followed and enforced very well.* (NRG4)

> *My fear is that we don't know what we don't know right now and we're also trying to move … and I'm not against it, but we're trying to move aggressively for political reasons to cloud-based solutions in the commercial side of the world.* (GOV1)

> *Security sometimes goes overboard in a lot of people's minds and it just becomes hard to do the job. And so, there is some resistance from that perspective… Mostly it's just griping about it, but we still comply. Until we can change it, we have to comply.* (FNCL1)

From this analysis, we observe: *Based on leader perception of their groups' self-efficacy and control, groups evince empowered, transitioning, or disempowered states.*

Cybersecurity Group States and the Incidence of Security Breaches

To validate our categorization of groups and thicken our understanding of empowerment, we triangulated interviewee data with data on the number of security breaches experienced by groups. Figure 4 depicts the number of security breaches experienced by study organizations between 2005 and 2019. Collectively, the 15 organizations experienced a total of 47 breaches. Three of the five empowered, transitioning, and disempowered group organizations had been breached. Organizations with empowered groups had the most breaches, averaging over four breaches per organization, while those with transitioning or disempowered groups had fewer than three.

Organizations with empowered groups were last breached in 2013 though, the year of the landmark Adobe and Target breaches (Cimpanu, 2019). These events were noted by several interviewees, one of whom said, "The dismissal of the Target CEO really drove home [the need for cybersecurity] to the executive level" (NRG2). In contrast, breaches of organizations with transitioning and disempowered groups continued, despite a 35% average annual decrease in breaches of financial and insurance services organizations, a 64% decrease in breaches of higher education institutions, and a 75% decrease of government and military breaches, according to the Privacy Rights Clearinghouse (our most comprehensive data breach source). Thus, we observe: *Organizations with empowered groups are less likely to experience security breaches.*

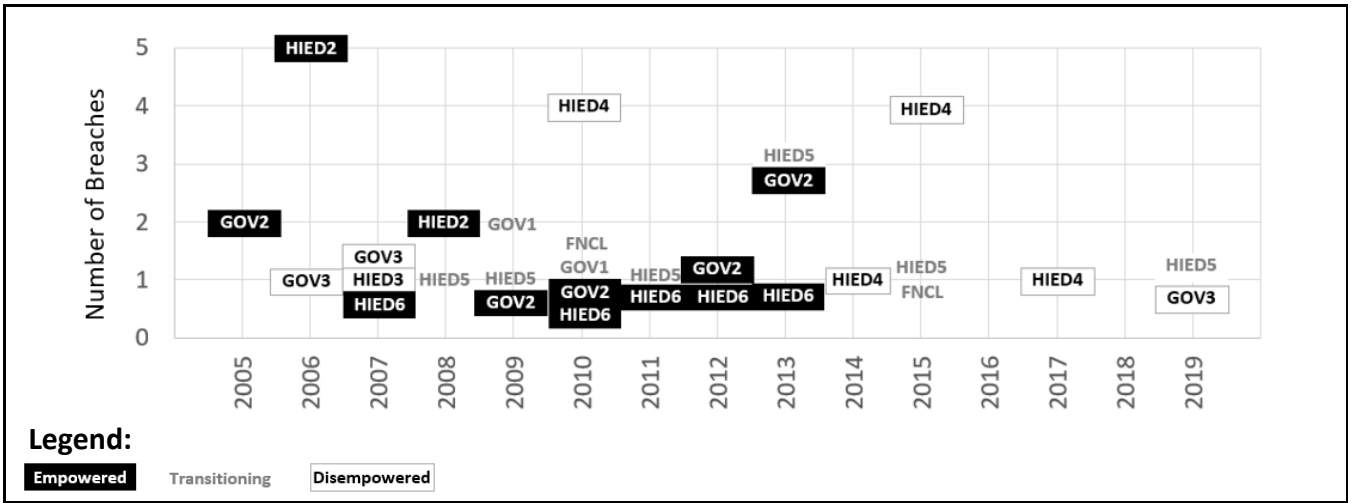


Figure 4. Timeline of Organizations' Cybersecurity Breaches

Elemental Structure: Group and Stakeholder Actions and Interactions

The rules circumscribing the state of cybersecurity groups "originate from the habituation of action and interaction" (Drazin & Sandelands, 1992, p. 238). These habituated (inter)action patterns constitute elemental structures. We look at cybersecurity group actions, then those of stakeholders. We next infer interactions from the patterning of these actions.

Cybersecurity Group Actions

Through initial coding, we surfaced two broad categories of cybersecurity group actions narrated by cybersecurity leaders. We lexically framed these categories of actions as the organizational risk mitigation actions of buffering and bridging (Thompson, 1967). Bode et al. (2011, p. 834) defined buffering as "attempts to gain stability by establishing safeguards that protect a firm from disturbances" and bridging as "attempts to manage uncertainty through engaging in 'boundary-spanning' and 'boundary-shifting' actions." Below, we describe the two types of actions as related to cybersecurity and the relative prevalence of the actions.

Unpacking Cybersecurity Bridging and Buffering Actions

We define *cybersecurity buffering* as *cybersecurity groups' efforts to protect their organizations by erecting virtual walls*. Quotes below illustrate buffering:

> *It took an intervention at the firewall to stop this [phishing attack].* (GOV1)

> *We're going to be deploying [a cloud security] appliance… [The email software] does have some limited capability where people can block individual senders [and has] high-level phishing detection.* (HIED6)

We define *cybersecurity bridging* as *cybersecurity group efforts to co-opt stakeholders into desirable cybersecurity behaviors*, as illustrated in the following excerpts:

> *We're training … to … pull together … good hygiene through a cyber perspective … And that goes into the safety culture, which is actually pretty good, because we do have a good mechanism to display statistics and to communicate the message out.* (NRG5)

> *We try to push things out through the campus IT leaders.* (HIED4)

Because bridging and buffering have not previously been contrasted in a cybersecurity context, we subjected leader statements coded as representing these two actions to semantic and rhetorical analysis. First, we identified words correlating strongly with "security" in statements describing each action. Based on these correlations, we plotted the semantic networks around "security" for bridging and buffering.[8] These semantic networks, in the foreground of Figure 5, depict fewer nodes, smaller nodes, and thinner lines for bridging (Figure 5a) than

[8] To do so, we identified terms correlating with "security" at $r = 0.25$ or higher (capturing the top 10 percentiles of correlations for the entire document-term matrix). Reasoning that meanings for groups in transition would be unsettled, and therefore mask visible patterning, we constructed the networks based only on the ten organizations with empowered or disempowered groups.

for buffering (Figure 5b). Thus, we see fewer terms consistently used with "security" when describing bridging, terms appearing less frequently in leader statements, and terms correlating weaker with "security" when describing bridging than buffering. From the number and strength of term associations across bridging and buffering statements, we infer greater consistency in how informants viewed security via buffering than bridging, i.e., greater shared understanding of buffering than bridging.

Second, to understand how leaders justified these two actions, we followed Abrahamson and Eisenman (2008), coding the rhetoric underlying statements as *rational*, i.e., argued based on efficiency maximization of an initiative, or *normative*, i.e., argued based on normality or emotional appeal.[9]

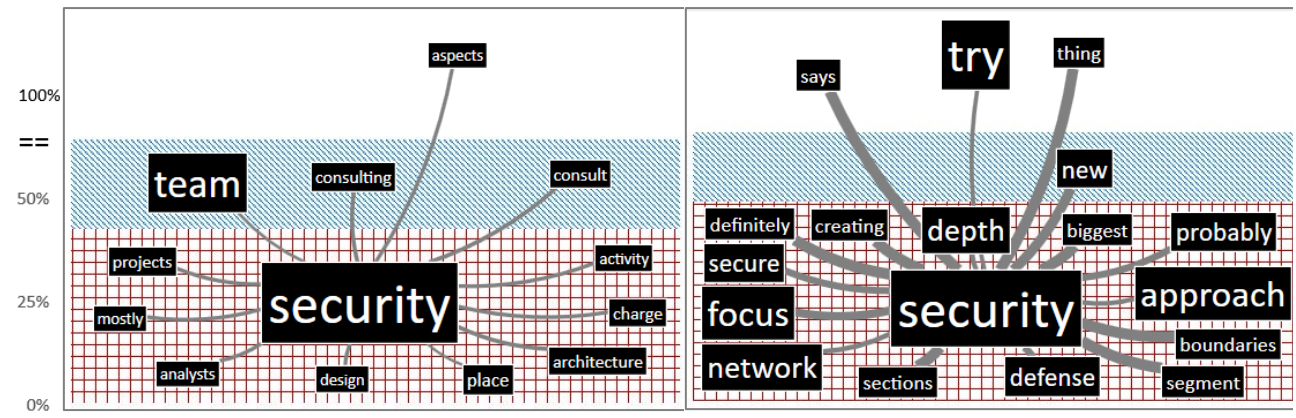
This analysis, depicted in the background of Figure 5, revealed the incidence of rational rhetoric was higher in statements concerning buffering (Figure 5b) than bridging (Figure 5a).[10] Thus, Figure 5 shows that cybersecurity leaders employ more rational justification for buffering than bridging. This may be because knowledge about means and ends pertaining to buffering initiatives is more widely diffused, as evident in leaders' focus on terms such as "approach," "boundaries," "network," and "defense." Thus, based on both semantic and rhetorical analyses, we observe *greater shared understanding around buffering than around bridging actions.*

The Prevalence of Cybersecurity Bridging (vs. Buffering)

Until about a decade ago "perimeter defense" initiatives focusing on "building 'bigger walls'" were the presumptive cybersecurity approach (Armerding, 2013; Radack, 2009). With the onset of social engineering attacks though, cybersecurity threats became more complex and dynamic; experts realized that buffering alone was inadequate (Jensen et al., 2017; Weinert et al., 2019) and that security capabilities needed to be embedded throughout an organization (Doan, 2019). This awareness saw a growth of what we term bridging, as reflected in the statements below:

> *We're starting to … change our paradigm a little bit, understanding that the old, … castle-and-moat approach to protecting IT isn't really going to work going forward.* (NRG2)

> *Any time your whole strategy is built around making static defenses when you're facing the well-financed and mobile adversary, the static defenses always fail eventually.* (HIED6)



A: BRIDGING **B: BUFFERING**

Legend: Size of nodes proportional to the relative density of terms in strategy discourse. Thickness of lines proportional to the strength of correlation between terms (r ranging from 0.25 to 0.88)

Normative rhetoric proportion *Rational rhetoric proportion* *Non-rhetorical language proportion*

Figure 5. Types of Group Strategies

[9] To assess these, one author identified 2,503 terms leaders used to describe their cybersecurity initiatives, following Abrahamson and Eisenman's method (2008) of first sorting the terms as no rhetoric or rational/normative rhetoric (1,583 or 63% of the terms), and then categorizing rhetorical terms as rational or normative. This yielded 1,169 rational terms, appearing an average of four times each in the transcripts, and 414 normative terms appearing an average of six times. A second author coded terms occurring 10 or more times in interviews. Pre-/post-reconciliation Cohen's kappas of 0.67/0.69 for whether a term was rhetorical or non-rhetorical and 0.83/0.87 for whether the term was rational or normative exceeded those reported by Abrahamson and Eisenman (2008).

[10] These patterns were consistent for each of the 10 empowered and disempowered organizations.

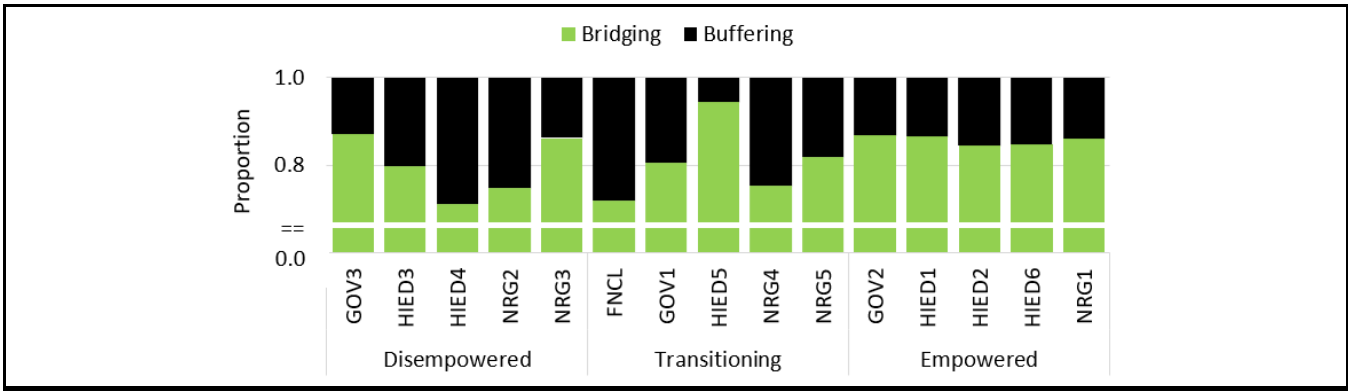


Figure 6. Group Action Orientations across Types

Thus, while buffering initiatives represent a minimum requirement for securing organizations (NIST, 2018), bridging initiatives have become an essential, higher-order activity. In our analyses below, we therefore focus on bridging. The proportion of each leader's statements about bridging (vs. buffering) actions is depicted in Figure 6.

Given the importance of bridging, it is unsurprising to observe that it dominated leader statements, representing at least 70% of statements describing their groups' actions. Statements by leaders of empowered groups did not differ systematically from those of disempowered and transitioning groups in their average attention to bridging in their statements. Figure 6 reveals that three disempowered and transitioning groups—GOV3, NRG3, and HIED5—evinced higher bridging levels than at least one empowered group. However, this does not necessarily reflect greater outreach by these groups. Rather, for disempowered groups, it reflects organizational limits imposed on these groups' buffering. Specifically, the GOV3 leader indicated that his role was limited to response only:

> *Once there has been [a] security incident, I'm responsible for the recovery … [Setting up hardware, software, policies, configurations] is handled by [headquarters].* (GOV3)

Similarly, most NRG3 buffering initiatives were handled by their IT group:

> *Network operations … configure the firewalls and those types of devices, and we're moving … responsibilities of monitoring those alerts to information security… Infrastructure still actually performs all of the patching, the security log configuration on the devices.* (NRG3)

The incoming leader of the transitioning HIED5 group did evince a very strong bridging orientation though, as seen in the following statements:

> *You simply can't throw a bunch of money into an intrusion detection system or firewall and think that you're done for the day ... In terms of the governance structure, it is everyone's responsibility. Every user of information technology, devices, and the network system on campus has a role to play in supporting information security.* (HIED5)

Thus, we observe: *While some disempowered and transitioning groups evinced higher bridging levels, bridging by empowered groups was uniformly high*.[11]

Organizational Stakeholder Actions

Stakeholders attend to cybersecurity demands along with other demands imposed by their roles (Karjalainen et al., 2019). Cybersecurity leaders recognized this tension:

> *Security is the opposite of convenience.* (NRG3)

> *We have to balance [exposure via offsite networks] against all the people that want to use technology from anywhere.* (NRG4)

Through qualitative analyses (detailed in Appendix B) of leader statements of stakeholder behaviors, we surfaced four cybersecurity approaches pursued by organizational stakeholders from top management to lower-level employees: *security prioritizing*, *hedging*, *avoiding*, and *thwarting*. Below, we describe the actions and discuss their relative prevalence.

[11] The coefficient of variation (σ/μ), a standardized dispersion measure, was 6.95 times higher for disempowered than empowered groups and 8.49 times higher for transitioning than empowered groups. Bounds on this ratio, obtained via a jackknifing approach, were 5.56 to 8.03 for empowered vs disempowered and 4.72 to 9.82 for empowered vs. transitioning groups.

Unpacking Organizational Stakeholder Security Actions

Security prioritizing is defined as stakeholders' *proactive support of cybersecurity initiatives*. This action is illustrated in the following interview excerpts:

> *Our biggest advocacy group is our executives … They're very behind the efforts that we have to make sure that the people understand.* (NRG1)

> *Our campus has been very receptive to … the need for security…we [cybersecurity and top management] spend a lot of time talking about how … we have to change.* (HIED2)

Security hedging is defined as stakeholders' *qualified support of cybersecurity initiatives*, reflecting their trade-offs between security and other job demands, as illustrated below:

> *We have a quarterly check and annual review [of compliance]. Those are pretty good, but ... the general usage sort of policies, they're not followed and enforced very well.* (NRG4)

> *I think that the very nature of higher ed as being open and accessible and in a place where a lot of people do a lot of experimentation and discovery kinds of things, it makes us more vulnerable because we don't … lock things down as much as some places do*. (HIED2)

Security avoiding is defined as stakeholder *evasion of cybersecurity initiatives*, as seen below:

> *We tried … putting articles or sending out emails, but it doesn't generate a lot of feedback. I'm not even sure that people are reading them.* (GOV2)

> *Most … ignore those [zero-day threat] notifications.* (GOV3)

Security thwarting is defined as stakeholders' *outright circumvention of cybersecurity initiatives*, as illustrated below:

> *Our executives and regular employees are out on social media just like everybody else is. They all give up too much information.* (NRG2)

> *Users … are ok with you doing whatever you need to do, provided it doesn't slow down or prevent them from doing what they [want]. That's [where] we've gotten … pushback.* (HIED1)

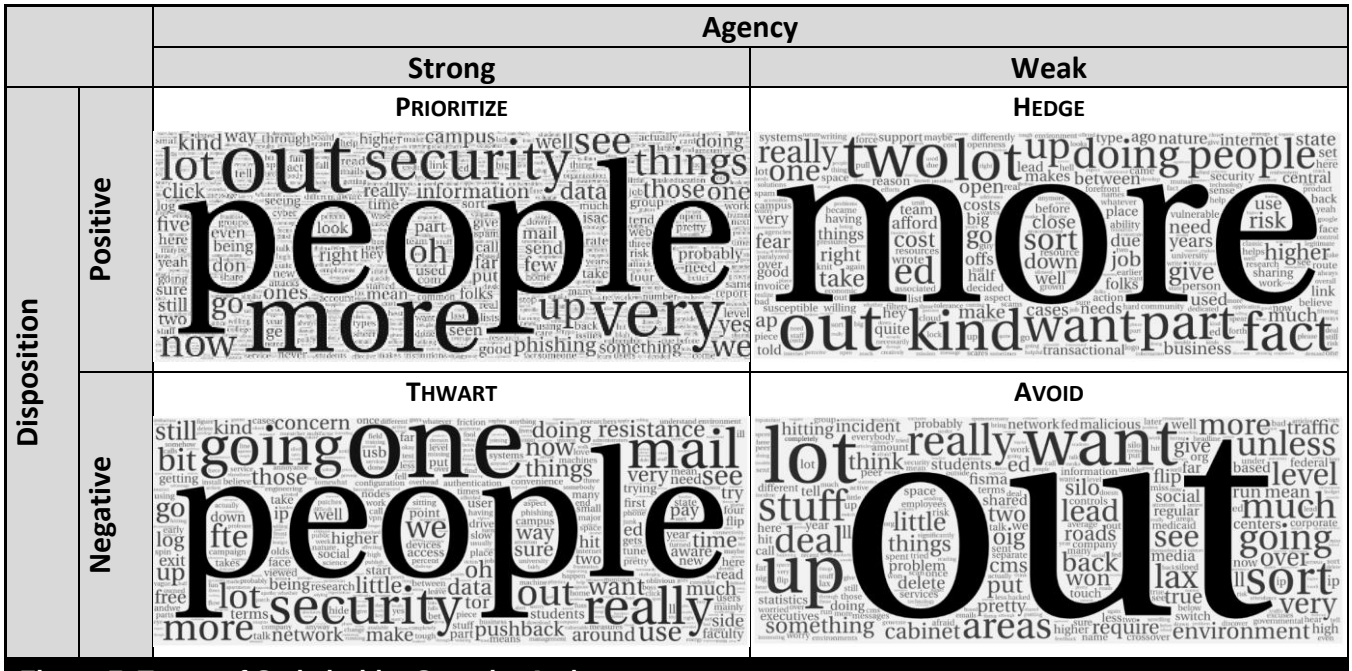


Figure 7. Types of Stakeholder Security Actions

We considered the semantics of leader descriptions of stakeholder actions via term frequency analysis of statements pertaining to each action, depicted as word clouds in Figure 7. First, noting more positive sentiment expressed[12] for the top than bottom types of action, we view prioritize and hedge as *positive* actions and thwart and avoid as *negative* actions. Second, given the prominence of "people" and "security" in security prioritizing (first and second most frequent terms, respectively) and thwarting (first and fifth most frequent terms, respectively) actions, we view these as reflecting *strong agency*, i.e., *as emphasizing the role of people as agents of security*; given the limited appearance of these two terms in security hedging and avoiding actions, we view these as reflecting *weak agency*, i.e., *not emphasizing people as agents of security*. Specifically, strong agency actions reflect the active role played by people in responding to security initiatives, while weak agency reflects a passive response or inaction by organizational stakeholders. Thus, we observe *two strong agency stakeholder actions—a positive, prioritizing action and a negative, thwarting action—and two weak agency actions—a positive, hedging response and a negative, avoiding action.*

The Prevalence of Security Prioritizing, Hedging, Avoiding, and Thwarting

Proportions of leader statements about the four types of stakeholder actions are depicted in Figure 8. We note that the dominant action orientations were the strong agency actions—prioritizing and thwarting, accounting for an average of 65% and 25% of leader statements about stakeholder actions. For all groups except NRG3, prioritizing was the dominant stakeholder orientation, accounting for over 50% of leader statements about stakeholder actions. Thwarting accounted for 54% of leader statements about NRG3 stakeholder actions and prioritizing only 46%. For all other disempowered groups, thwarting was the secondary stakeholder orientation. Thus, we observe that while stakeholders of some empowered and transitioning groups favored thwarting more than hedging or avoiding, *the stakeholders of disempowered groups consistently favored thwarting over hedging and avoiding, and even prioritizing.*

Latent Interactions: Relating Group and Stakeholder Actions across States

Because of its necessity and difficulty, we again focus on bridging. Figure 9 summarizes cybersecurity group bridging and organizational stakeholder prioritizing, hedging, avoiding, and thwarting for different states of cybersecurity groups.[13] The scatterplots depict how each of the four stakeholder actions correspond with group bridging for each study organization, as well as the resulting patterning of the group and stakeholder actions across study organizations. From this patterning, we infer stakeholder reactions to group bridging, i.e., group-stakeholder interactions.

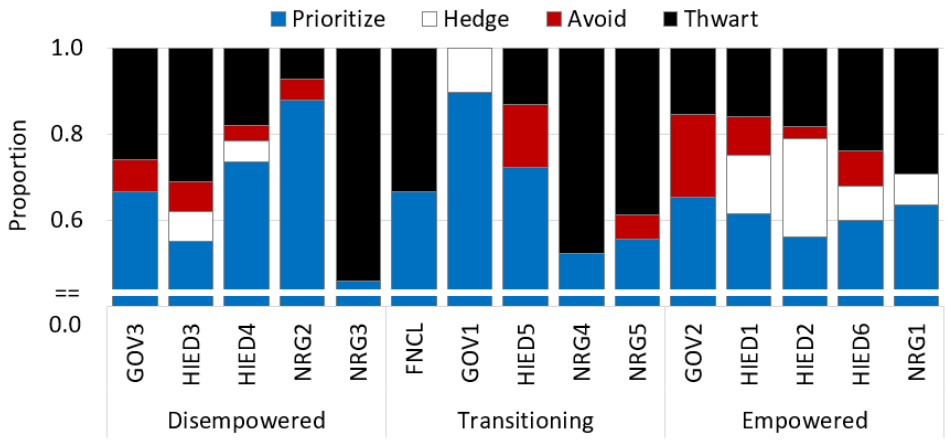


Figure 8. Stakeholder Action Orientations across Group Types

[12] Because informants used negation extensively, sentiment was assessed via the SentimentR package, which correctly accounts for negation (Naldi, 2019). Scores were 0.10 for prioritizing, 0.03 for hedging, 0.01 for avoiding, and -0.03 for thwarting.

[13] See Data Analysis Activities in the Online Supplement for a description of how proportions for bridging and stakeholder actions were calculated. Given the small samples used to draw inference, we assessed the robustness of relationships in Figure 9 via a jackknifing approach, i.e., correlations were deemed robust when the sign did not change with the exclusion of any data point.

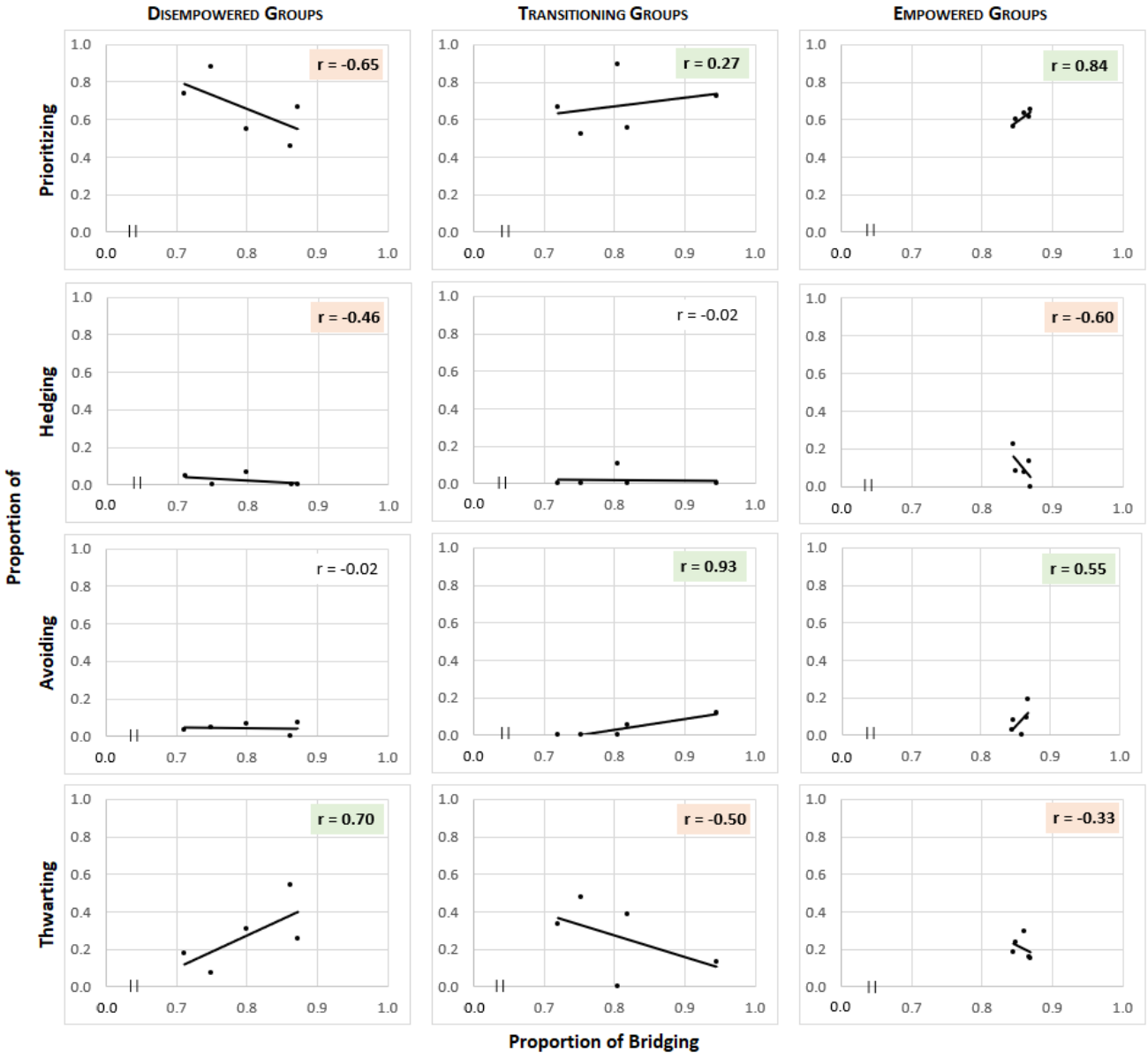


Figure 9. Organizational Stakeholder Actions Relative to Groups' Bridging

From Figure 9, we see that bridging was associated with lower stakeholder prioritizing for organizations with disempowered groups. Yet bridging was associated with higher prioritizing for those with empowered groups. We see this in these descriptions of stakeholder behaviors:

> *We have … shared ownership of phishing and other elements of our … user-layer security.* (NRG1)

> *When employees get a suspicious email, they tend to call … and they put in a ticket.* (GOV2)

Second, from Figure 9, we note that bridging was associated with lower stakeholder hedging for organizations with disempowered *and* empowered cybersecurity groups. Third, from Figure 9, we note that bridging is associated with greater stakeholder avoidance for organizations with transitioning and empowered cybersecurity groups. This reveals avoidance as the fallback strategy for transitioning and empowered groups when wholehearted behavioral adjustment is undesirable. Consider, for example, the following stakeholder behavior descriptions:

> *And every once in a while, they don't tell us and we discover later that some spammer has now sent out 30,000 messages under their name… So, we're more worried about those who are unwilling to call us because they're afraid they'll get into trouble.* (HIED2)

> *Tech liaison groups have regular meetings, and they are close to business staff... but it's hit/miss because of attendance.* (GOV2)

Fourth, from Figure 9 we note that bridging was associated with higher stakeholder security thwarting for organizations with disempowered, but not transitioning, groups and lower thwarting for empowered groups. This finding reveals thwarting as the fallback for stakeholders in disempowered organizations when confronted with undesired behavioral requirements, as illustrated below:

> *We see … pushback … [when] we ask people to identify potential phishing campaigns and report those… The other thing is… we're asking members to help us with the phishing [by not using] their company email address for personal uses, which [elicits] another convenience pushback.* (NRG3)

> *We did a social engineering campaign around USB drive, and we had a little bit more resistance because it was more in their face.* (NRG1)

From this, we observe: *Empowered group stakeholders respond to bridging initiatives with strong positive and weak negative agency, but disempowered group stakeholders respond with strong negative agency and transitioning group stakeholders with weak negative agency.*

Interpenetration of Cybersecurity Groups with Organizational Structures

Earlier, we noted the salience of IT, legal, and PR structures to cybersecurity and the consequent possibility for cybersecurity group structuring to interpenetrate with these structures. Sample leader statements illustrate the salience of these structures from the perspective of leadership of cybersecurity groups as well as that of IT, legal, and PR units (Table 2).

Table 2. Illustrating the Salience of Other Organizational Structures

Structure	Quotes from cybersecurity leaders	Quotes from IT, legal, and PR leaders
IT	I also report to a director of IT infrastructure and operations (NRG2). We report to the CIO, but not through the IT group. Our CIO is responsible for information technology but also has other roles in terms of corporate strategy and security (GOV1).	We've got communications channels and Slack or phone or whoever. But [when there was suspicious activity in a user's account,] it was immediately a communication with the security team. (HIED4) Just within last week [IT has] been approached by our security office asking us to implement an outbound spam filter policy. We started that a couple of months ago, but they kind of forgot about it (HIED3)
Legal	When it starts to move into a criminal environment, [where] something needs to be litigated, we'll work with [the] legal [group] (HIED4) The Office of General Counsel is a very important partner in [cybersecurity]. (HIED5) Corporate compliance and corporate legal uses [the corporate learning system] to deliver compliance and legal messages to people every year (NRG2).	As far as our level of collaboration directly with the IT folks and with the security governance folks, I would give us very high marks because we all work very closely together (FNCL1). The Office of General Counsel is a very important partner in [cybersecurity]. (HIED5)
PR	Cyberattacks became big headline news in 2013 when the *New York Times* went public with their own attack (HIED5). We absolutely get support from places we don't expect it, like the news media. Same time we're pushing to quit using personal email, then here comes all the Hillary stuff (NRG3).	If you have a security breach of data (financial or health) being prompt and direct and setting up an apparatus to answer questions from the influenced people is really important. You don't want to leave an impression with the stakeholders that we are not protecting their information. Working with the IT security people is very important (HIED5).

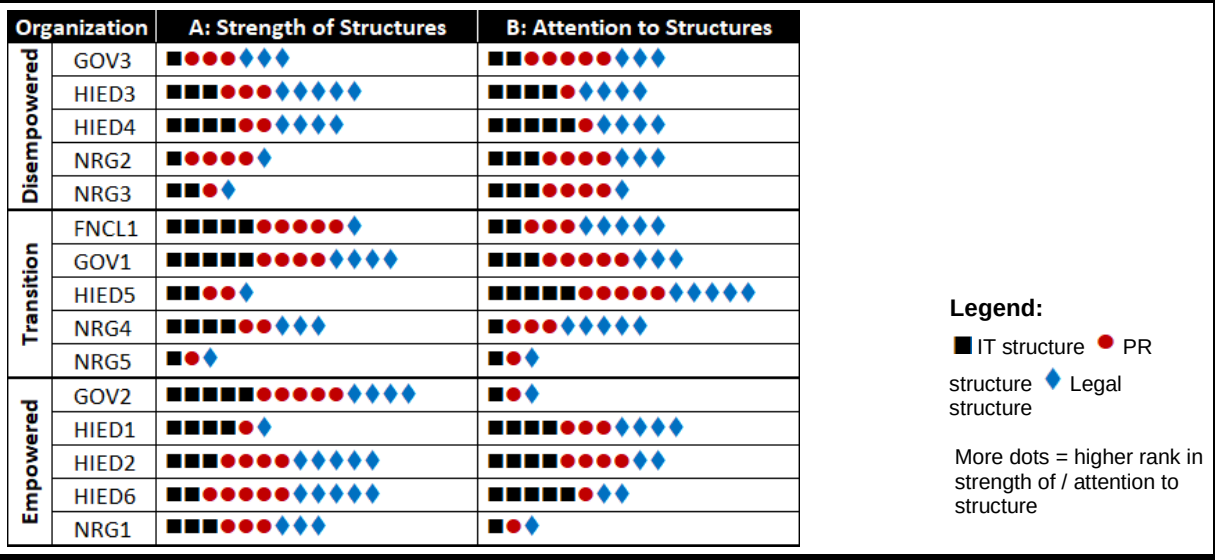


Figure 10. Strength of and Attention to Extant Structures

Table 3. Interpenetration with Extant Structures and Bridging

Extant Structure	Disempowered	Transitioning	Empowered
A: Attention to Structure Relative to Structural Salience			
IT structure	↗	--	↘
Legal structure	↗	↘	--
PR structure	↗	--	↘
B: Bridging Relative to Attention			
IT structure	↘	--	--
Legal structure	↘	--	--
PR structure	↗	--	--

Figure 10a quantifies the salience of the three structures (in terms of IT employees relative to all organizational employees, security lawsuits relative to total lawsuits, and negative news coverage) across sampled organizations. To enhance the comparability of structures across organizations, we represent the ranked strength of organizations' structures relative to the other organizations (more dots = higher strength rank). From Figure 10a, we note no systematic difference in the salience of structures across empowered, transitioning, and disempowered groups. To understand leader attention to extant structures more systematically, we quantified proportions of statements pertaining to each structure, e.g., containing "IT" or "systems" along with "staff," "team," "employee," "hire," "intern," "director," "group," or "position" for IT structure; "law," "legal," or "litig*" for legal; and "news," "media," or "press" for PR structure. For comparability of organizations' attention to the structures, we again represent their rank in Figure 10b. Here, we see no systematic difference between empowered and disempowered leader attention either. Thus, from Figure 10, we observe *no systematic differences in the strength of or leader attention to extant structures across empowered, transitioning, and disempowered groups.*

Next, we considered the extent to which these structures interpenetrated with the emergent cybersecurity structure. We interpreted existing structures as interpenetrating with cybersecurity if there was a robust positive relationship between the strength of a structure and leaders' attention to it. We depict these relationships in Table 3a.[14] Leader attention to all three structures correlated robustly and positively with the strength of structures for disempowered groups but *diminished* with the strength of the legal structure among organizations with transitioning groups and with increasing salience of IT and PR structures for those with

[14] See Data Analysis Activities in the Online Supplement for correlation coefficients and jackknifed bounds (obtained by excluding each observation in turn).

empowered groups. We therefore conclude that the IT, PR, and legal structures interpenetrated consistently with the emergent cybersecurity structure for disempowered, but not for transitioning and empowered, cybersecurity groups.

From Figure 10, we see the disempowered HIED4 had the strongest IT structure, with 8.33 IT staff members per 100 employees (Table 1). As illustrated in the quotes below, HIED4 leadership discussed several elements of the IT structure, including leadership, organization, staffing, and processes:

> *We report to the CIO… we have a vacant position right now of an IT director who reports directly to the CIO… Not all colleges report to central IT. Some of the colleges have their own IT staff, who are essentially in charge of security for their college.*
>
> *New IT staff start in onboarding programs.*
>
> *All the colleges have their own IT department… Central IT has about 230, 250 full-time to support [HIED4]. Central IT really only has about half of the IT resources at [HIED4]. The rest are supporting individual colleges…or other entities … We essentially act as an ISP for[them] and then that school or entity has their own IT staff … There's a lot of history with respect to how central IT is viewed on campus... And so central IT and the security team has sort of been paralyzed to not take an action in fear of the one-offs that may be out there that may have a legitimate use for that technology or that part of the internet on campus … We try to push things out through the campus IT leaders or, you know, work with the strategists in central IT who work with the external colleges to either put word out on things that might be happening or things to look for, be aware of.*

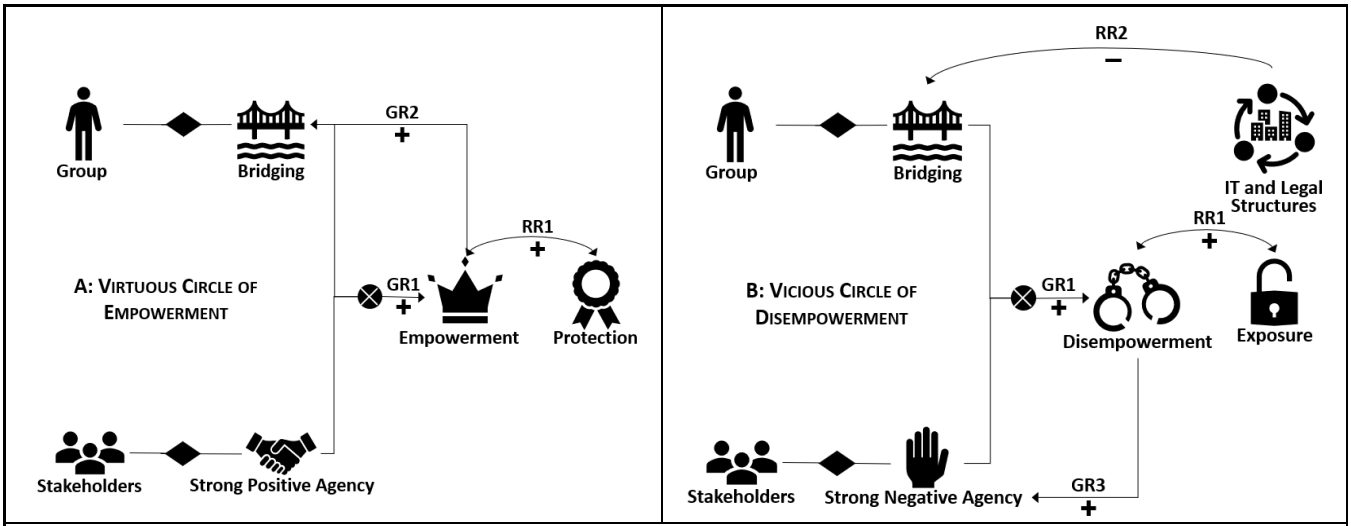
From Figure 10, we see that the disempowered NRG2 had the strongest PR structure. Though there were few news articles about NRG2 (Table 1), the tone of these articles was strongly negative. The resulting PR structure gave the cybersecurity leader hope of leveraging media coverage of breaches toward strengthening the cybersecurity structure, as illustrated in this quote:

> *We've seen [concern about security threats] through all the latest publicity with pretty major breaches ... In the last year with Home Depot and JP Morgan and Target and just this last week the US Department of State and etc., etc., etc., … it's in the media all the time now ... I think the dismissal of the Target CEO really drove it home to the executive level. When [board members] got to read about that and see that on the news and in the media, I think it really hit home at that point in time. I think it also kind of drove it home for the board members, seeing that they have some level of liability involved as being a board member. And I think it kind of drove them or started to drive them to realize, hey, I need to get educated … I wouldn't think [that we are more vulnerable to specific type of an attack]. I mean, our executives and regular employees are out on social media just like everybody else is. They all give up too much information, just like every other company does.*

From Figure 10, we see the disempowered HIED3 had the strongest legal structure: two of their four lawsuits concerned security. The following illustrates their legal structure attention:

> *I characterize a lot of [the cybersecurity group work] as very much like legal counsel ... Professors just never delete a grade book, which is illegal … where the standard practice was to put social security numbers in the grade book.*

Table 3b depicts the relationship between leader attention to IT, PR, and legal structures and bridging by the cybersecurity group. Of particular interest is the relationship for disempowered groups, for which we noted an interpenetration between these structures and their emergent group structure. Here, we see consistent patterning of groups' bridging relative to attention to extant structures among disempowered groups, with lower bridging by groups more attentive to IT and legal structures, but heightened bridging by groups more attentive to PR. GOV3, with the weakest IT structure, used the most bridging (Figure 6), while HIED4, with the strongest IT structure, used the least bridging (Figure 6). The imperviousness of leaders of transitioning and empowered groups to the strength of their IT, PR, and legal structures precludes these structures from circumscribing their bridging efforts. Because IT and legal structures circumscribe the consciousness of disempowered groups in a way that is unparalleled with other types of groups and this consciousness then relates to bridging levels, we observe: *IT and legal structures interpenetrate systematically with disempowered groups, encumbering bridging.*



Observation		Generative and Reinforcing Rules
1. Groups evince empowered, transitioning, or disempowered states. 2. Empowered organizations are less likely to experience security breaches.	→	RR1. Empowerment (disempowerment) cycles recur because they do (not) protect the organization.
3. There is greater shared understanding of buffering than bridging. 4. Bridging by empowered groups is uniformly high.	→	GR2. IF groups are empowered THEN they enact consistently high levels of bridging.
5. There are two strong – positive prioritizing and negative thwarting – and two weak agency stakeholder actions – positive hedging and negative avoiding. 6. Stakeholders of disempowered groups consistently favor thwarting over hedging and avoiding, and even prioritizing.	→	GR3. IF groups are disempowered THEN stakeholders consistently fall back on, or even favor, strong negative agency.
7. Empowered group stakeholders respond to bridging initiatives with strong positive and weak negative agency, but disempowered and transitioning group stakeholders respond with strong and weak negative agency respectively.	→	GR1. IF groups bridge AND stakeholder strong agency is positive THEN groups are empowered; ELSEIF groups bridge AND stakeholder strong agency is negative THEN groups are disempowered.
8. There are no systematic differences in strength of or leader attention to extant structures across different types of groups. 9. IT and legal structures interpenetrate systematically with disempowered groups, encumbering bridging.	→	RR2. Interpenetration with IT and legal structures encumbers bridging by impeded groups, fostering the cycle of disempowerment.

Figure 11. Circles of Empowerment and Disempowerment

Deep Structure: Tacit Rules for the Process of Empowerment

In the autogenic perspective, deep structures are those tacit, invisible rules that produce the visible states and (inter)action patterns. Above, we described alternate cybersecurity group states, actions of and interactions between cybersecurity groups and organizational stakeholders, and cybersecurity leader attention to other organizational structures. We now recapitulate the nine observations culled from our analyses to derive three generative and two reinforcing rules that explain how the observed states and group/stakeholder (inter)actions emerge.

Figure 11a depicts the virtuous circle of empowerment that is generated through a confluence of group bridging and stakeholders' strong positive agency (security prioritizing). This circle is reinforced as empowerment increases protection from cybersecurity attacks. Subsequent increased bridging activities and strong positive agency reinforce the cybersecurity group's co-optative bridging overtures and stakeholder reciprocation via prioritizing. Through this virtuous circle of empowerment, the cybersecurity group and stakeholders jointly enact people-centric security practices such as "consulting" and "team" (see Figure 5a) that practitioners have touted as effective in securing organizations. In this way, empowering (inter)actions in elemental structures persist and the observed structure of an empowered cybersecurity group is reproduced.

In contrast, the vicious circle of disempowerment (Figure 11b) is produced via a confluence of group bridging action and stakeholder strong negative agency (security thwarting). This circle is reinforced as disempowerment increases exposure to cyberattacks. In this vicious circle of disempowerment,

stakeholders increasingly fall back on, or even favor, strong negative agency as earlier efforts to prioritize cybersecurity seemed unsuccessful. This strong negative agency precludes people-centric cybersecurity practices, permitting only buffering initiatives that focus on "boundaries" and "segmenting" (see Figure 5b). Further, established IT and legal structures impinge on the emergent cybersecurity structure, commandeering leader attention and constraining potentially empowering bridging activities. In this way, impeding (inter)actions in elemental structures persist and the observed structure of a disempowered cybersecurity group is reproduced.

The Generative Rules

We characterize *generative rules* as *those internal to the cybersecurity structure that produce and reproduce its states of empowerment or disempowerment*. These rules underlie the patterning of the cybersecurity group and the stakeholder (inter)actions.

Generative Rule 1: Empowerment is Produced via Group Co-opting of Stakeholders

Our focal generative rule is that if groups successfully co-opt stakeholders on cybersecurity, groups are empowered; if they do not, groups are left disempowered. This is based on our seventh observation, i.e., while stakeholders of empowered groups met group bridging with strong positive (prioritizing) and weak negative (avoiding) agency, those of disempowered groups did the reverse—responding with strong negative (thwarting) and weak positive (hedging) agency. Below, we illustrate positive feedback of empowered group stakeholder strong positive responses to bridging:

> *I would say our organization [cybersecurity] is fairly highly thought of … It's been one of our institution's differentiators probably for the last five to seven years as far as what we do compared to other universities. It's sort of become the spine of our academic and business functions at the university.* (HEID1)

In contrast, stakeholder opposition to cybersecurity bridging *and* buffering contributes to group self-perception of low control and efficacy, as visible in the following narrative:

> *IT security [in the colleges] is very politically driven … We try our best to reach out to colleges … [but] a college decided to purchase a network storage appliance from a small vendor… and they're able to put their documents on their computer, which may contain student records.* (HIED4)

Underlying the interactions between cybersecurity groups and organizational stakeholders therefore is the generative rule that produces empowered or disempowered cybersecurity groups. Specifically, the enactment of a rule in which stakeholders respond to the co-optative overtures underlying cybersecurity bridging by thwarting security produces a disempowered cybersecurity group. In contrast, the enactment of a rule in which organizational stakeholders respond positively to co-optative overtures produces an empowered cybersecurity group. Alternatively put, *the core capability apparent in empowered organizations and missing from disempowered organizations is the co-opting of stakeholders.*

Generative Rule 2: Empowered Groups Consistently Enact Bridging

Our third observation was of greater shared understanding around buffering than bridging, revealing the latter to be a more difficult set of cybersecurity enactments. Our fourth observation was that empowered groups undertook consistently high levels of bridging, despite its apparent intractableness. Empowered groups therefore consistently enact this higher-order security approach that invites stakeholder cooperation and is essential to securing organizations (Doan, 2019). The following quote illustrates this generative rule:

> *Yeah, we heavily partner and utilize our marketing and communications group to try to help us craft messages and, you know, look at the communication strategies to help us land the message [about the importance of cybersecurity].* (NRG1)

Generative Rule 3: Disempowered Group Stakeholders Favor/Fall Back on Strong Negative Agency

Our fifth observation described positive and negative and strong and weak agency stakeholder actions. Our sixth observation was that stakeholders of disempowered cybersecurity groups consistently favored strong negative agency over weak agency actions and, in one case, even over strong positive agency. Disempowered groups therefore consistently favor or fall back on the cooperation-stymieing action. This generative rule is also supported by the following narrative:

> *When we try to put security measures in on the research campus, there's been a lot of resistance, because [research faculty] consider [cybersecurity policies] something going against friction-free connectivity… It is mind-boggling. [We] are more concerned about [researcher] data than [researchers] are*. (HIED4)

The Reinforcing Rules

While generative rules produce the (inter)actions through which the cybersecurity state initially emerges, reinforcing rules reproduce those observed and elemental structures. *Reinforcing rules* are therefore *established structures that reproduce structures of empowered or disempowered states via the recurrent (inter)action patterns of cybersecurity groups and stakeholders*.

Reinforcing Rule 1: Empowerment Cycles Recur Because They Are Protective

Primary reinforcement of an emergent structure accrues from outcomes associated with the structure (Drazin & Sandelands, 1992). Our first observation distinguished among states of cybersecurity groups based on the levels of self-efficacy for, and control of, cybersecurity revealed in leader narratives. The dimensions of self-efficacy and experienced locus of causality that define a group as empowered are themselves desired group states. This is because high self-efficacy and an internal locus of causality are associated with lower anxiety and greater well-being and with setting and achieving challenging goals (Karademas, 2006). Our second observation was that while organizations with empowered groups experienced no breaches after the landmark Target and Adobe cases, some with disempowered and transitioning groups did. Therefore, an empowered cybersecurity state confers on organizations the wherewithal to withstand security threats, reinforcing the state of empowerment. By the same logic, disempowered groups experiencing exposure will experience lower self-efficacy and an internal locus of causality, diminishing their sense of well-being. This builds on the finding by Li et al (2023) which provided evidence that a narrow scope of security strategies delivers poor security outcomes. In this way, positive outcomes promote a virtuous empowerment circle, while negative outcomes promote a vicious disempowered circle. Consider, for example, the experiences narrated by the leader of the empowered GOV2 organization, which had not suffered a breach since 2013, and then those of the leader of the disempowered HIED4, which had been breached as recently as 2017:

> *We also have quarterly meetings with technology liaisons, individuals who take messages back to their department. They are seen as experts in their department … we perform regular phishing exercises and can track who clicks on a link. The manager and employee will get a message explaining what they clicked at and what to look for… If they fail again- they will be assigned to another module. If they continue to fail exercises, they get to sit down with me and their officer. I know organizations where they publicly shame people, but we don't do that. The one-on-one meetings are useful because it helps me to understand why people clicked on a link. It helps us revise our training materials.* (GOV2)

> *We try our best to reach out to colleges … We see attacks on a … poorly written web application … that exposes usernames and passwords ... We found out about the server compromise from web communications. Somebody tweeted out to [HIED4] that, hey, we just put a bunch of your databases up online. We didn't know about it … that's how the university found out about it.* (HIED4)

Reinforcing Rule 2: Disempowered Cycles Recur through Structural Interpenetration

Our eighth observation was of no systematic differences in leader attention to IT, legal, and PR structures across empowered, transitioning, and disempowered groups. This suggests that the structures surrounding the three different types of groups were not inherently different. Yet, our ninth observation was that disempowered group attention to IT and legal structures encumbered bridging. The significance of this observation is that though organizations with disempowered groups did not consistently have stronger or weaker IT and legal structures, disempowered cybersecurity leaders in organizations with stronger IT and legal structures were more attentive to those structures. This suggests structural constraint on the already-disempowered groups. This constraint manifests itself further in lower bridging relative to IT and legal structures, indicating that bridging is obstructed in organizations with strong IT and legal structures and disempowered cybersecurity structures. Thus, the interpenetration of the disempowered cybersecurity group with IT and legal structures promotes the vicious disempowering circle by reducing cooperation-inviting bridging enactments, as seen below:

> *When it starts to move into a criminal environment [or] something needs to be litigated, we'll work with the legal team and make a decision as to what our next step is … [Cybersecurity] detected somebody was on the network viewing pornographic material using university assets. And [cybersecurity] went down the road to find it, blocking the person, and it turned out it was a professor who was doing some "research" and the dean and [legal] said they had a legitimate need to be on there doing it. That really tainted the approach that the security team was going to take … they said, well, if that's okay, then pretty much everything else is going to be okay, right?* (HIED4)

Discussion

Beginning with the understanding that a state of group empowerment is a transient, precarious one, the focal questions of our study were how cybersecurity groups come to be empowered and how empowerment is maintained. We answered these questions by surfacing the generative rules through which states of group (dis)empowerment occur and the reinforcing rules through which those states are maintained. In doing so, we theorized the empowerment process in terms of virtuous (vicious) circles of (dis)empowerment. Below, we describe how insights derived from our research augment understandings of cybersecurity, empowerment, and autogenesis. We then consider the practical implications of our work and offer suggestions for future research.

Contributions to the Cybersecurity Literature

Though much of the research on cybersecurity has focused on garnering stakeholder compliance, governance of the cybersecurity group has recently begun to command scholarly attention (Liu et al., 2020; Yoo et al., 2020). We join this fledgling conversation on governance for cybersecurity by first drawing attention to the extreme uncertainties that cybersecurity groups face and their concomitant need for empowerment. In contrast to conventional governance discourse that considers structure in terms of formally centralized, decentralized, or federated models (Sambamurthy & Zmud, 1999), we describe the emergent structuring of cybersecurity groups. In doing so, we advance the understanding of what Gregory et al. (2018) term "relational mechanisms" necessary for complex organizing. Beyond the specific relational practices of advice seeking and reciprocal participation that Gregory et al. (2018) noted, we highlight the criticality of the *experience* of empowerment enjoyed by cybersecurity leadership to cybersecurity outcomes.

We found the cybersecurity group's experience of empowerment is initiated and sustained when the groups enact bridging initiatives and perceive stakeholder responsiveness to these initiatives. We thus shift the focus off of taken-for-granted, control-oriented buffering initiatives to the less understood, relational bridging initiatives essential to cybersecurity success. By flagging the lack of consensus in meaning around bridging, we also call attention to a problem: effective ongoing implementation of bridging requires a better understanding of what it entails than is currently evident. Further, we highlight that how stakeholders respond is salient to the empowerment experienced by cybersecurity groups. This too shifts the cybersecurity discourse from focusing on the consequences of cybersecurity agency for stakeholder compliance to the consequences of stakeholder compliance for cybersecurity agency.

However, research has highlighted stakeholder trade-offs in navigating cybersecurity policy alongside their day-to-day work (Karjalainen et al., 2019; Wright et al., 2023). While policy violations certainly carry risk, we show that occasional negative weak agency stakeholder responses, i.e., avoidance, need not compromise an organization's ongoing cybersecurity when stakeholders mainly prioritize cybersecurity. Rather than focus on individual acts of compliance, our work suggests the need for a portfolio view of compliance in assessing the security viability of an organization. This insight complements Karjalainen et al.'s (2019) and Wright et al.'s (2023) findings on the balancing act stakeholders play in navigating their daily work alongside cybersecurity compliance by noting how those tensions might be alleviated—i.e., by permitting the occasional weak agency noncompliance response.

Contribution to the Empowerment Literature

Empowerment scholars have struggled to understand the intricate relationship between structural and psychological empowerment (e.g., Biron & Bamberger, 2010; Mills & Ungson, 2003; Perkins & Zimmerman, 1995). In this paper, we define empowerment as a *duality of state and emergent process*. In doing so, we undertake three moves significant to the empowerment literature. First, we shift our view of structural empowerment from a designed to an emergent process. In doing so, we join the strategy literature that views strategic processes as often emergent rather than designed (e.g., Mintzberg & Waters, 1985; Mirabeau & Maguire, 2014). This perspective emphasizes that empowerment processes are necessarily ongoing and cannot be a one-time organizational design initiative. Second, by recognizing the emergent nature of structural empowerment, we foreground the micro(inter)actions through which a state of empowerment—or disempowerment—occurs. These micro (inter)actions emphasize the importance of lateral, not just vertical, relationships in structural empowerment. Third, through its recursive emergence, we highlight the precarious nature of the state of empowerment. Through our autogenic analysis, we thus shed light on why organizations' structural empowerment initiatives may not always be associated with the psychological empowerment and performance consequences they aim to bring.

Contributions to the Autogenesis Literature

Since its initial exposition (Drazin & Sandelands, 1992), empirical investigations based on the autogenic perspective have been scant. This is despite the extensive stream of research tracing the emergence of structure from (inter)actions (e.g., Soderstrom & Weber, 2020). The challenge posed by the autogenic perspective involves surfacing the tacit rules that characterize the deep structures privileged by the perspective. As noted by Drazin and Sandelands (1992), these tacit rules are not themselves observable and can only be inferred. Yet, without understanding these tacit rules, managerial efforts at intervention can engender unintended structures and behaviors (King, 2000). Our first contribution to the autogenesis literature, therefore, is our empirical investigation of autogenesis. The relative novelty of the cybersecurity function provided a unique opportunity for us to apply an autogenic perspective to investigating organizing. Our multiple case study approach permitted us to contrast observations across a range of organizations to infer the tacit rules that otherwise are intractable to organizational studies.

Our second contribution is our distinction between generative and reinforcing rules. Our concept of reinforcing rules formalizes Drazin and Sandelands's (1992, p. 237) position that (inter)action patterns "may be reinforced" by their consequences. Here, we clarify that generative rules are instantiated in the initial emergence of a structure, while reinforcing rules promote recurrent (inter)action patterns, preserving the status quo in observed states.

Our third contribution is in demonstrating the relevance of computational techniques as complements to traditional qualitative analyses in autogenic research. Quantifying self- and other-referential statements made by cybersecurity leaders permitted us to surface an alternate social fact about cybersecurity groups, i.e., their relative empowerment. We found this to be related to cybersecurity and stakeholder (inter)actions in a more revelatory fashion than conventional views of structure as reporting relationships. Quantifying behavior patterns by security professionals and their stakeholders enabled us to surface elemental structures while quantifying the strength of and leaders' attention to other organizational structures permitted us to assess the interpenetration of these structures with the cybersecurity structure. Yet triangulating these observations with details embedded in leader narratives enabled us to infer the deep structures of tacit rules giving rise to the observed and elemental structures.

Implications For Practice

Practitioners have begun to prioritize involvement between organizational stakeholders on cybersecurity (EY, 2020; KPMG, 2022). Our results endorse this direction. We further argue that cybersecurity must move from compliance-seeking to involvement-seeking to provide protection and value to the organization. Thus, we join with others to promote people-centric security, which is a "mode of security [that] emphasizes individual accountability and trust." (Blum, 2020, p. 232). Our emphasis on bridging and empowerment is a departure from reliance on sovereign power and associated enactments of buffering favored by cybersecurity groups (D'Arcy & Herath, 2011). Moving from a compliance- to an involvement-seeking strategy does not mean abandoning buffering (e.g., access control) and ISPs. Nor does it entail a laissez-faire approach to cybersecurity governance. Instead, organizations need to design for empowerment, as such design can scaffold beneficial emergent structures (Clement & Puranam, 2018). Cybersecurity groups should initiate and sustain, the corporate center should encourage and facilitate, and business units should reciprocate involvement overtures.

Second, our findings show that every cybersecurity group, even empowered groups, should expect some noncompliance when enacting bridging. This is inevitable as stakeholders navigate cybersecurity demands in conjunction with their regular work demands. Therefore, cybersecurity groups enacting bridging should engage through involvement with stakeholders, communicating openness to negotiation. After all, our findings show that cybersecurity is possible even in the presence of occasional stakeholder noncompliance—as long as the noncompliance is in the form of avoidance rather than outright thwarting. Realistic expectations of stakeholder responses likely will yield healthier engagements and more realistic trade-offs in ISPs.

Third, there is little understanding of how to successfully engage in bridging initiatives. Secondary informants underscored the prevalence of stringent frameworks and standards (i.e., NIST), which almost exclusively focus on buffering techniques and tools (Disparte & Furlow, 2017; KPMG, 2022). These informants also highlighted mixed views by cybersecurity leadership regarding the use of bridging techniques. Thus, more work remains regarding how cybersecurity groups can successfully implement bridging initiatives. But our findings suggest that improved security outcomes await organizations in which cybersecurity groups implement bridging. We further observe an unmet need to develop and extend frameworks around bridging to facilitate assimilation into organizational best practices.

Finally, we find that organizations with disempowered cybersecurity groups have a pathway to escape the vicious circle of disempowerment. This entails: (1) the corporate center and cybersecurity group together elevate the group's locus of causality and self-efficacy, (2) the cybersecurity group increasing its bridging efforts, (3) stakeholders suspending short-term judgment of the cybersecurity group for past breaches, and (4) protection of the cybersecurity group from pressures toward buffering emanating from the IT and legal departments. Escaping the vicious circle of disempowerment is likely to require a sustained effort and could be undermined by antagonistic or unilateral actions from the corporate center, cybersecurity group, or other business units.

Limitations

There are several limitations of this work that should be considered along with its implications. First, a critical limitation of our work is that it entails mainly synchronic analysis. From a process perspective, reciprocal typifications like we have described here unfold over time. Second, though we interviewed and triangulated findings from numerous stakeholders in IT, legal, and PR business units, we infer structures, structuring processes, and stakeholder responses largely from the interviews with cybersecurity leaders. Consequently, the four organization responses (i.e., prioritizing, hedging, avoiding, thwarting) are not meant to be comprehensive but rather provide a foundation on which future research can build. Third, we only evaluate four industry segments in which cybersecurity is critical and yet suffers constant attacks. This may surface a certain set of activities that are less generalizable to a larger, more heterogeneous set of organizations. Fourth, our investigation of organizational structures other than the cybersecurity group was solely through archival sources. While this permitted us to assess the extent to which the strength of IT, legal, and PR structures impinged on the autogenic empowerment of cybersecurity groups, it precludes nuanced observations of how organizational differences in IT, legal, and PR structures enhanced or weakened interpenetration with the cybersecurity group.

Future Research Directions

This research invites and offers theoretical scaffolding for variance-, process-, and systems-based research. We discuss three of the most promising. The first concerns how bridging by the cybersecurity group can be performed more effectively. Since bridging is vital to cybersecurity but is not well understood, future research areas of inquiry include understanding: (1) involvement techniques that make bridging overtures more successful, inviting organizational groups and individual stakeholders to shoulder more responsibility for cybersecurity; (2) effects of bridging initiatives in co-opting long-term stakeholder compliance; and (3) how bridging reinforces empowerment over time. A second direction concerns the prevalence of strong versus weak negative agency, i.e., thwarting versus avoidance. Future research should investigate the organizational conditions that permit weak, but reduce the strong, negative agency that undermines collaborative cybersecurity initiatives. The third direction addresses how business units interpenetrate with the cybersecurity group. How much agency the corporate center grants to individual units around cybersecurity is a delicate balance. Understanding how to achieve and maintain this balance would shed light on the interpenetration of business units. In addition to IT, legal, and PR, other business units regularly interface with the cybersecurity group (e.g., operations), and may also play a role in organizing cybersecurity. Further, as supply chains become more integrated, structures outside organizational boundaries (e.g., powerful vendors, suppliers, customers) may also interpenetrate with the emergent cybersecurity group. Examining the nature and consequences of these relationships in structuring cybersecurity is crucial.

Conclusion

Via an autogenic, organic view of empowerment, we highlighted the seminal role of the relationship between cybersecurity groups and their stakeholders in effecting this empowerment and protecting informational assets. While a compliance-seeking approach to cybersecurity remains relevant, further understanding of this involvement perspective is crucial. In a nutshell, it takes a united stand for the cybersecurity group to become and remain empowered.

Acknowledgments

We are grateful to the senior editor, Likoebe Maruping, the associate editor, John D'Arcy, and the three reviewers for their constructive engagement throughout the review process. We would also like to thank Suprateek Sarker and workshop participants at the University of Georgia's MIS Department and the Stevens Institute of Technology's Information Systems Department for their valuable comments on the paper. This project was funded by the National Science Foundation (Grant 1421580).

References

Abrahamson, E., & Eisenman, M. (2008). Employee-management techniques: transient fads or trending fashions? *Administrative Science Quarterly*, *53*(4), 719-744. https://doi.org/10.2189/asqu.53.4.719

Alvarado-Vargas, M. J., & Zou, Q. (2018). Getting rid of a heavy shield: downsizing the in-house legal department? *American Journal of Business*, *33*(1/2), 2-17. https://doi.org/10.1108/AJB-08-2017-0022

Armerding, T. (2013). *Long live perimeter security*. Security. https://www.csoonline.com/article/2134133/long-live-perimeter-security.html

Arsenault, B. (2023). Your biggest cybersecurity risks could be inside your organization. *Harvard Business Review*. https://hbr.org/2023/03/your-biggest-cybersecurity-risks-could-be-inside-your-organization

Bachrach, P., & Baratz, M. S. (1963). Decisions and nondecisions: An analytical framework. *American Political Science Review*, *57*(3), 632-642. https://doi.org/10.2307/1952568

Balozian, P., Burns, A., & Leidner, D. E. (2023). An adversarial dance: Toward an understanding of insiders' responses to organizational information security measures. *Journal of the Association for Information Systems*, *24*(1), 161-221. https://doi.org/10.17705/1jais.00798

Bandura, A. (1986). *Social foundations of thought and action*. Prentice Hall.

Benson, J. K. (1977). Organizations: A dialectical view. *Administrative Science Quarterly*, *22*(1), 1-21. https://doi.org/10.2307/2391741

Berti, M., & Simpson, A. V. (2021). The dark side of organizational paradoxes: The dynamics of disempowerment. *Academy of Management Review*, *46*(2), 252-274. https://doi.org/10.5465/amr.2017.0208

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly*, *24*(1), 169-196. https://doi.org/10.2307/3250983

Biron, M., & Bamberger, P. (2010). The impact of structural empowerment on individual well-being and performance: Taking agent preferences, self-efficacy and operational constraints into account. *Human Relations*, *63*(2), 163-191. https://doi.org/10.1177/0018726709337039

Blum, D. (2020). *Rational cybersecurity for business: the security leaders' guide to business alignment.* Springer.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. *Academy of Management Journal*, *54*(4), 833-856. https://doi.org/10.5465/amj.2011.64870145

Boutyline, A., & Soter, L. K. (2021). Cultural schemas: What they are, how to find them, and what to do once you've caught one. *American Sociological Review*, *86*(4), 728-758. https://doi.org/10.1177/00031224211024525

Burns, A., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse. *Information Systems Research*, *34*(1), 342-362. https://doi.org/10.1287/isre.2022.1133

Chen, G., Kirkman, B. L., Kanfer, R., Allen, D., & Rosen, B. (2007). A multilevel study of leadership, empowerment, and performance in teams. *Journal of Applied Psychology*, *92*(2), 331. https://doi.org/10.1037/0021-9010.92.2.331

Cimpanu, C. (2019). *A decade of hacking: The most notable cyber-security events of the 2010s.* ZDNet. https://www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s/

Clement, J., & Puranam, P. (2018). Searching for structure: Formal organization design as a guide to network evolution. *Management Science*, *64*(8), 3879-3895. https://doi.org/10.1287/mnsc.2017.2807

Conger, J. A., & Kanungo, R. N. (1988). The empowerment process: Integrating theory and practice. *Academy of Management Review*, *13*(3), 471-482. https://doi.org/10.2307/258093

Cordery, J. L., Morrison, D., Wright, B. M., & Wall, T. D. (2010). The impact of autonomy and task uncertainty on team performance: A longitudinal field study. *Journal of Organizational Behavior*, *31*(2-3), 240-258. https://doi.org/10.1002/job.657

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, *23*(3), 779-805. https://doi.org/10.17705/1jais.00740

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658. https://doi.org/10.1057/ejis.2011.23

Deci, E. L., and Ryan, R. M. . (1985). *Intrinsic motivation and self-determination in human behavior*. Plenum Press. https://doi.org/10.1007/978-1-4899-2271-7

Deken, F., Carlile, P. R., Berends, H., & Lauche, K. (2016). Generating novelty through interdependent routines: A process model of routine work. *Organization Science*, *27*(3), 659-677. https://doi.org/10.1287/orsc.2016.1051

Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, *21*(1), 152-174. https://doi.org/10.17705/1jais.00595

Disparte, D., & Furlow, C. (2017). The best cybersecurity investment you can make is better training. *Harvard Business Review*. https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

Doan, M. (2019). Companies Need to Rethink What Cybersecurity Leadership Is. *Harvard Business Review*. https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is

Drazin, R., Glynn, M. A., & Kazanjian, R. K. (2004). Dynamics of structural change. In M. S. Poole & A. H. Van de Ven (Eds.), *Handbook of organizational change and innovation* (pp. 161-189). Oxford University Press.

Drazin, R., & Sandelands, L. (1992). Autogenesis: A perspective on the process of organizing. *Organization Science*, *3*(2), 230-249. https://doi.org/10.1287/orsc.3.2.230

Drydyk, J. (2013). Empowerment, agency, and power. *Journal of Global Ethics*, *9*(3), 249-262. https://doi.org/10.1080/17449626.2013.818374

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532-550.

EY. (2020). How does security evolve from bolted on to built-in? EY's 22nd Global Information Security Survey 2020. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report.pdf

Faraj, S., & Sambamurthy, V. (2006). Leadership of information systems development projects. *IEEE Transactions on Engineering Management*, *53*(2), 238-249. https://doi.org/10.1109/TEM.2006.872245

Gartner. (2022). *Gartner identifies three factors influencing growth in security spending*. https://www.gartner.com/en/newsroom/press-

releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i

Gersick, C. J. (1991). Revolutionary change theories: A multilevel exploration of the punctuated equilibrium paradigm. *Academy of Management Review*, *16*(1), 10-36. https://doi.org/10.2307/258605

Giddens, A. (1979). *Central problems in social theory: Action, structure, and contradiction in social analysis*. University of California Press. https://doi.org/10.1007/978-1-349-16161-4

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. Polity Press.

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT consumerization and the transformation of IT governance. *MIS Quarterly*, *42*(4), 1225-1253. https://doi.org/10.25300/MISQ/2018/13703

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714. https://doi.org/10.1080/07421222.2018.1451962

Hatch, M. J., Schultz, M., & Skov, A.-M. (2015). Organizational identity and culture in the context of managed change: Transformation in the Carlsberg Group, 2009-2013. *Academy of Management Discoveries*, *1*(1), 58-90. https://doi.org/10.5465/amd.2013.0020

Heracleous, L., & Barrett, M. (2001). Organizational change as discourse: Communicative actions and deep structures in the context of information technology implementation. *Academy of Management Journal*, *44*(4), 755-778. https://doi.org/10.2307/3069414

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

Judge, T. A., & Bono, J. E. (2001). Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis. *Journal of Applied Psychology*, *86*(1), 80-92. https://doi.org/10.1037/0021-9010.86.1.80

Kahn, R. A., & Brock, B. T. (2007). When information security became a lawyer's thang. *Business Law Today*. https://businesslawtoday.org/2017/09/when-information-security-became-a-lawyers-thang/

Karademas, E. C. (2006). Self-efficacy, social support and well-being: The mediating role of optimism.. *Personality and Individual Differences*, *40*(6), 1281-1290. https://doi.org/10.1016/j.paid.2005.10.019

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: a dialectical process perspective. *Information Systems Research*, *30*(2), 687-704. https://doi.org/10.1287/isre.2018.0827

King, A. (2000). Organizational response to environmental regulation: punctuated change or autogenesis? *Business Strategy and the Environment*, *9*(4), 224-238. https://doi.org/10.1002/1099-0836(200007/08)9:4%3C224::AID-BSE249%3E3.0.CO;2-X

Kirkman, B. L., & Rosen, B. (1997). A model of work team empowerment. *Research in Organizational Change and Development*, *10*(1), 131-167. https://doi.org/10.2307/256874

Kirkman, B. L., & Rosen, B. (1999). Beyond self-management: antecedents and consequences of team empowerment. *Academy of Management Journal*, *42*(1), 58-74.

KPMG. (2022). *Cyber trust insights 2022*. https://kpmg.com/us/en/articles/2022/cyber-trust-insights-2022.html

Kumar, N., Stern, L. W., & Anderson, J. C. (1993). Conducting interorganizational research using key informants. *Academy of Management Journal*, *36*(6), 1633-1651. https://doi.org/10.2307/256824

Lee, M., and Koh, J. (2001). Is empowerment really a new concept? *International Journal of Human Resource Management*, *12*(4), 684-695. https://doi.org/10.1080/713769649

Li, W. W., Leung, A. C. M., & Yue, W. T. (2023). Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. *MIS Quarterly*, *47*(1), 317-342. https://doi.org/10.25300/MISQ/2022/15713

Liu, C.-W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787. https://doi.org/10.1080/07421222.2020.1790190

Lowry, M. R., Sahin, Z., & Vance, A. (2022). Taking a seat at the table: The quest for CISO legitimacy. *Proceedings of the International Conference on Information Systems*.

Maddison, J. (2020). Rapid change is the new normal. *Security Week*. https://www.securityweek.com/rapid-change-new-normal

Madill, A., Jordan, A., & Shirley, C. (2000). Objectivity and reliability in qualitative analysis: Realist, contextualist and radical constructionist epistemologies. *British Journal of Psychology*, *91*(1), 1-20. https://doi.org/10.1348/000712600161646

Markham, S. (1996). Company/product image studies and other considerations of Fortune 500 public relations departments. *Journal of Promotion Management*, *3*(1-2), 15-30. https://doi.org/10.1300/J057v03n01_02

Maynard, M. T., Gilson, L. L., & Mathieu, J. E. (2012). Empowerment—fad or fab? A multilevel review of the past two decades of research. *Journal of Management*, *38*(4), 1231-1281. https://doi.org/10.1177/0149206312438773

Mehrizi, M. H. R., Nicolini, D., & Mòdol, J. R. (2022). How do organizations learn from information systems incidents? A synthesis of the past, present, and future. *MIS Quarterly*, *46*(1), 531-590. https://doi.org/10.25300/MISQ/2022/14305

Mills, P. K., & Ungson, G. R. (2003). Reassessing the limits of structural empowerment: Organizational constitution and trust as controls. *Academy of Management Review*, *28*(1), 143-153. https://doi.org/10.2307/30040694

Mintzberg, H., & Waters, J. A. (1985). Of strategies, deliberate and emergent. *Strategic Management Journal*, *6*(3), 257-272. https://doi.org/10.1002/smj.4250060306

Mirabeau, L., & Maguire, S. (2014). From autonomous strategic behavior to emergent strategy. *Strategic Management Journal*, *35*(8), 1202-1229. https://doi.org/10.1002/smj.2149

Miranda, S., Berente, N., Seidel, S., Safadi, H., & Burton-Jones, A. (2022). Editor's comments—Computationally intensive theory construction: A primer for authors and reviewers. *Management Information Systems Quarterly*, *46*(2), iii-xviii.

Mitchell, J. R., Shepherd, D. A., & Sharfman, M. P. (2011). Erratic strategic decisions: When and why managers are inconsistent in strategic decision making. *Strategic Management Journal*, *32*(7), 683-704.

Naldi, M. (2019). *A review of sentiment computation methods with R packages*. arXiv. https://arxiv.org/abs/1901.08319

Nikkhah, H. R., & Grover, V. (2022). An empirical investigation of company response to data breaches. *MIS Quarterly*, *46*(4), 2163-2196.

NIST. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST REPORT 800-37 R.1).

Perkins, D. D., & Zimmerman, M. A. (1995). Empowerment theory, research, and application. *American Journal of Community Psychology*, *23*(5), 569-579. https://doi.org/10.1007/BF02506982

Pratto, F. (2016). On power and empowerment. *British Journal of Social Psychology*, *55*(1), 1-20. https://doi.org/10.1111/bjso.12135

Radack, S. (2009). Protecting information systems with firewalls: Revised guidelines on firewall technologies and policies. *Computer Security Resource Center*. https://csrc.nist.gov/publications/detail/itl-bulletin/2009/10/protecting-information-systems-with-firewalls-revised-guideline/final

Rafaeli, A., & Sutton, R. I. (1991). Emotional contrast strategies as means of social influence: Lessons from criminal interrogators and bill collectors. *Academy of Management Journal*, *34*(4), 749-775. https://doi.org/10.2307/256388

Rappaport, J. (1984). Studies in empowerment: Introduction to the issue. *Prevention in human services*, *3*(2-3), 1-7. https://doi.org/10.1300/J293v03n02_02

Ravishankar, M., Pan, S. L., & Leidner, D. E. (2011). Examining the strategic alignment and implementation success of a KMS: A subculture-based multilevel analysis. *Information Systems Research*, *22*(1), 39-59. https://doi.org/10.1287/isre.1080.0214

Robey, D., & Azevedo, A. (1994). Cultural analysis of the organizational consequences of information technology. *Accounting, Management and Information Technologies*, *4*(1), 23-37. https://doi.org/10.1016/0959-8022(94)90011-6

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74-104. https://doi.org/10.1111/jels.12035

Rosemann, M., & Vessey, I. (2008). Toward improving the relevance of information systems research to practice: the role of applicability checks. *MIS Quarterly*, *32*(1), 1-22. https://doi.org/10.2307/25148826

Ross, A. (2016, April 25, 2016). Want job security? Try online security. *Wired*. https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross

Rowlands, J. (1995). Empowerment examined. *Development in Practice*, *5*(2), 101-107. https://doi.org/10.1080/0961452951000157074

Ryan, R. M., and Connell, J. P. (1989). Perceived locus of causality and internalization: examining reasons for acting in two domains. *Journal of Personality and Social Psychology*, *57*(5), 749. https://doi.org/10.1037/0022-3514.57.5.749

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, *23*(2), 261-290. https://doi.org/10.2307/249754

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Guest editorial: qualitative studies in information systems: a critical review and some guiding principles. *MIS Quarterly*, *37*(4), iii-xviii.

Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers & Security*, *122*, Article 102903. https://doi.org/10.1016/j.cose.2022.102903

Seibert, S. E., Silver, S. R., & Randolph, W. A. (2004). Taking empowerment to the next level: A multiple-level model of empowerment, performance, and satisfaction. *Academy of Management Journal*, *47*(3), 332-349. https://doi.org/10.2307/20159585

Seibert, S. E., Wang, G., & Courtright, S. H. (2011). Antecedents and consequences of psychological and team empowerment in organizations: A meta-analytic review. *Journal of Applied Psychology*, *96*(5), 981. https://doi.org/10.1037/a0022676

Silva, L. (2007). Post-positivist review of technology acceptance model. *Journal of the Association for Information Systems*, *8*(4), 255-266. https://doi.org/10.17705/1jais.00121

Silva, L., & Hirschheim, R. (2007). Fighting against windmills: Strategic information systems and organizational deep structures. *MIS Quarterly*, *31*(2), 327-354.

Soderstrom, S. B., & Weber, K. (2020). Organizational structure from interaction: Evidence from corporate sustainability efforts. *Administrative Science Quarterly*, *65*(1), 226-271. https://doi.org/10.1177/0001839219836670

Spreitzer, G. M. (2008). Taking stock: A review of more than twenty years of research on empowerment at work. In C. Cooper & J. Barling (Eds.), *Handbook of organizational behavior* (Vol. 1, pp. 54-72). https://doi.org/10.4135/9781849200448.n4

Stake, R. E. (1995). *The art of case study research*. SAGE.

Tausczik, Y. R., & Pennebaker, J. W. (2010). The pychological meaning of words: LIWC and computerized text analysis methods. *Journal of Language and Social Psychology*, *29*(1), 24-54.

Thompson, J. D. (1967). *Organizations in action: Social science bases of administrative theory*. Transaction Publishers. https://doi.org/10.4324/9781315125930

Tolbert, P. S., & Zucker, L. G. (1996). The institutionalization of institutional theory. In S. Clegg, C. Hardy, & W. Nord (Eds.), *Handbook of organization studies* (pp. 169-184). SAGE. https://doi.org/10.4135/9781446218556.n6

Turban, D. B., Tan, H. H., Brown, K. G., and Sheldon, K. M. (2007). Antecedents and outcomes of perceived locus of causality: An application of self-determination theory. *Journal of Applied Social Psychology*, *37*(10), 2376-2404. https://doi.org/10.1111/j.1559-1816.2007.00263.x

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453. https://doi.org/10.1126/science.7455683

van den Berg, J., Alblas, A., Blanc, P. L., & Romme, A. G. L. (2022). How structural empowerment boosts organizational resilience: A case study in the Dutch home care industry. *Organization Studies*, *43*(9), 1425-1451. https://doi.org/10.1177/01708406211030659

Weinert, A., Mayfield, P., Costica, Y., O'Donovan, S., Gulati, G., Radhakrishnan, D., Tor, Y., & Esibov, A. (2019). Traditional perimeter-based network defense is obsolete—transform to a zero trust model *Security*. https://www.microsoft.com/security/blog/2019/10/23/perimeter-based-network-defense-transform-zero-trust-model/

Wright, R. T., Johnson, S. L., & Kitchens, B. (2023). Phishing susceptibility in context: A multilevel information processing perspective on deception detection. *MIS Quarterly*, *47*(2), 803-832. https://doi.org/10.25300/MISQ/2022/16625

Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). SAGE.

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, *44*(2), 907-931. https://doi.org/10.25300/MISQ/2020/15477

About the Authors

Alexandra Durcikova is Mertes Presidential Professor and Professor of MIS at the University of Oklahoma. She serves as the Division Director for MIS. Dr. Durcikova's research interests include knowledge management, information security, and the adoption of information systems. Her work focuses on how knowledge is created, shared, and utilized in organizations, as well as the human factors in information security practices. She has published numerous peer-reviewed articles in top journals, such as *MIS Quarterly, Information Systems Research, Journal of the Association for Information Systems, and Journal of Management Information Systems*, contributing valuable insights into the successful implementation and utilization of information technologies. Dr. Durcikova's interdisciplinary approach bridges the gap between theory and practice in the field of information systems. ORC-ID: 0000-0002-6705-202X

Shaila M. Miranda is a professor, M. D. Matthews Endowed Chair, and chair of the Information Systems Department at the Sam M. Walton College of Business. She has a doctorate in information systems (with a minor in computer science) from the University of Georgia and an M.A. in sociology from Columbia University. Her research focuses on the constitutive nature of discourse and on emergent social structures in the arenas of digital activism and digital innovation. She employs a combination of qualitative and computational abductive techniques in her research. Shaila's research has appeared in journals such as the *MIS Quarterly*, *Information Systems Research*, and *Journal of Management Information Systems*, and she has published a book on social analytics. She serves as a senior editor for *MIS Quarterly*, previously has served as senior editor for *Information Systems Research* and is a Fellow of the AIS. ORC-ID: 0000-0003-4910-8074

Matthew L. Jensen is the W.P. Wood Professor of Management Information Systems and a co-director of the Center for Applied Social Research at the University of Oklahoma. Professor Jensen's interests include cybersecurity and privacy, computer-aided decision-making, and human-computer interaction. He leads interdisciplinary teams investigating how people filter and evaluate information they find online. Professor Jensen has published over 100 scholarly works in leading academic and practitioner outlets. Jensen has also been the primary investigator or co-primary investigator on research projects totaling more than $10 million sponsored by several federal agencies and private companies. ORC-ID: 0000-0001-8711-1827

Ryan Wright is the senior associate dean of Faculty and Research in the McIntire School of Commerce at the University of Virginia. Professor Wright's research interests include cybersecurity, privacy, and the diffusion of innovations. He has over 80 publications in outlets such as *MIS Quarterly*, *Information Systems Research*, *Journal of the Association for Information Systems*, *and Journal of Management Information Systems*. He has also garnered funding from the National Science Foundation, the state of Massachusetts, and the state of Virginia. His research has been featured in the *Harvard Business Review*, *The Washington Post*, *Forbes*, *Seattle Post-Intelligencer*, *The Australian*, *USA Today*, *Fast Company*, *Psychology Today*, and many other outlets. He has presented his research for several practitioner groups, including TEDx, the Salesforce Foundation, and the Association for Finance and Technology. ORC-ID: 0000-0002-9719-415X

Appendix A

Table A1. Structured Interview Protocol

Interviewee Background

1. What industry is your organization in? What is your current title/position? How long have you been at this organization/ in your present position?
2. What administrative group do you belong to (e.g., marketing, IT, finance)?
3. What is your highest degree? What is your specialty? How long have you been specializing in this?
4. What is your perspective on information security in general and at your organization? Are some groups more responsible than others?

Organizational Perspective

5. How many people are employed in your company? How many people are responsible for supporting IT? How many people are responsible for the security of IT?
6. Tell me about the overall security atmosphere at your organization? How does your organization support employees to be more secure? Is it working—why or why not?
7. Whose job is IT security at your organization?
8. What resources are available to employees learning and understanding what the appropriate behavior is when it comes to information security?
9. How frequently do you train employees? Have you had training that focused on phishing email detection? Why or why not?
10. What rewards or punishments are employed to support the secure behavior of employees? Do you believe that employees are paying attention to these incentives?
11. Do you believe that employees are paying close attention to the security policy? How frequently do they have to sign the security policy?
12. What is challenging about security in general, and phishing, in particular, at your organization? Is your organization vulnerable to a specific type of attack? What kinds of attacks do you see? What are the most common?
13. Have you observed any resistance toward security measures at your organization? Have you observed that employees are trying shortcuts?
14. What are the main areas of focus in IT security for your organization? Do you work with the FBI/DHS? How frequently do you exchange information?
15. Do you measure your Cyber maturity rating? What frameworks do you use? Are you comfortable sharing your rating (on a scale 1-5, 5 being the best)?
16. What conferences, related to your job, do you go to? Please name the top 3 that you don't want to miss. Why are these conferences important to you?
17. I want to ask about your budget. What is your IT budget? What percentage of the IT budget goes toward security?

Assessment of Spam and Phishing Email Detection Techniques

18. Tell me about what mechanisms your organization uses to detect spam/phishing emails. Please be as specific as you can.
19. Do you use Identity Management Solutions/ Behavioral Training (vendor developed or in-house)/ threat tracking solutions/ Network surveillance solutions/ Server-side anti-malware virus protection/ IP address tracking? How many layers of devices/SW does your email go through before it ends up in the user inbox?
20. Do you use mock phishing tests to evaluate these techniques? Do you write them yourself, or do you use a vendor? What is the name of the vendor?
21. What user groups do you feel contribute most to: Data security threats in general; The problem of phishing; And why?
22. What user groups are you currently leveraging in combating data security threats, in general, the problem of phishing, and how?
23. What user groups do you think you could be leveraging in the future to combat data security threats in general, the problem of phishing and how?
24. Have you experienced a breach because of a phishing attack? Was the employee from one of the 'vulnerable' groups? How did you find out about the breach? What actions did you take to remedy the situation? Do you have cyber insurance? Please share as much as you are comfortable sharing.
25. Do your employees report spam/phishing emails? Is there an email address to which employees can forward spam/phishing emails?
26. Do you have a policy regarding spam/phishing email reporting? How long does it take to block an IP address/email address from the time it is reported by employees?
27. Do you communicate back to your employees about current phishing threats? Why or why not? What resources do you use? What would help you adopt such a solution? Would your users find the information useful? What kinds of assessment techniques do you use to check the success of spam/phishing email detection?
28. What kinds of assessments most accurately capture your success rate? Are you involved in evaluating any of the above-mentioned detection mechanisms?
29. How is the assessment of these detection mechanisms used to improve your organization's security?
30. Describe how much spam or phishing is discussed in relation to other IT security threats? Is the amount of time and attention appropriate?
31. Is your company involved in any type of security sharing community/group with other companies within/outside your industry? What are the benefits of this? What are the costs? Would you change anything in how this group works?
32. Would you be willing to share your security policy and acceptable use policy documents with us? We can anonymize it.
33. Anything else that you would like to share that we didn't ask about?

Appendix B

Table B1. Coded Concepts and Illustrations

High-level codes	Low-level categories	Illustrative quotes
Problem or solution		
Problem Statement reflects a cybersecurity concern		▪ I would say, we are barely keeping up in [information security], and it's not from lack of trying, it's not from lack of commitment. (NRG4) ▪ But if you just look at the general [information and computer] usage sort of policies, they're not followed and enforced very well. (NRG4)
Solution Statement reflects a way of resolving or resolution to a concern		▪ One thing is that we've done is to be staffed well for this (NRG4). ▪ Technically, we do use third-party cloud provider … [to] send over email through to get first pass for spam (NRG4).
Actor		
Cybersecurity group Individual members of the group or the group as a whole		▪ We maintain firewalls to obtain email security gateways, we do response, and we also do risk assessment, so we can try to assess, the current posture of our environment, as well as the third-party companies, the partners, and then we are responsible for compliance as well … Pretty big portion of what we do on a daily basis, being a corporate entity (NRG4). ▪ So, you know, one of the things I'm dealing with right now is VPN and to the corporation assets when you're remote (NRG5).
Stakeholders Organizational members who affect and are affected by cybersecurity group policies and procedures	IT	▪ IT is very supportive of security (NRG1). ▪ A lot of times what happens is, the employee will report it to their IT and then the IT person will send it to us (HIED6).
	User(s)	▪ I would say probably less than 10% of the people use the button on reporting phishing (NRG4). ▪ We're in the process of rolling out mandatory, multifactor authentication for VPN and getting tremendous pushback from faculty and students, why are you doing this to me? (HIED6).
	Cross-functional group	▪ Those groups that deal with more sensitive information or … HR people…, they know that they're dealing with the financial people to do things like wire transfers, they know that it's when you get out of those more support functions that deal with specific types of data circuit, is more on the operation side of things (NRG4). ▪ Talk to the technology group—but it's hit/miss because of attendance (GOV2).
	Organization	▪ So [the organization is] very behind the efforts that we have to make sure that the people understand (NRG1). ▪ But we do have an aging workforce, which is not necessarily very good technically (NRG5).
Other Actors not considered in the analyses	Other organization	▪ I get e-mails from the state security folks and, you know, they run a tight ship and everything and they have the agencies and they're very corporate-like in most aspects (HIED3). ▪ But [the website builder company] also are pretty good about responding, and they'll take the link down or the website down (HIED4).
	Outside agencies	▪ The FBI has a program called InfoGuard … that we participate in. (HIED4). ▪ [Mock phishing emails are sent] by auditors [during an audit]. (GOV1).
	Vendor	▪ We're a Google … Gmail campus (HIED2). ▪ So, I mean, we were still running Forefront 2010, which Microsoft stopped essentially supporting (HIED4).
	Attacker	▪ Now, those are probably more, you know, the individuals who are looking for banking information, personal information, not necessarily credentials for the company (NRG5). ▪ The spammers figured out exactly how they wanted to do this, and every day they sent out 3,000 more spam messages (HIED2).
Cybersecurity group actions		
Bridging Cybersecurity group' effort to co-opt stakeholders into desirable cybersecurity behavior	Training	▪ And we also have training courses (FNCL1). ▪ Our privileged users, so the people who have access to social security numbers and financial records, they do have an annual refresh requirement where they have to go through some updated training and then re-attest that they're aware of the policies and that they're following the policies (HIED6).
	Knowledge exchange	▪ And we do briefings with the government daily a lot of times (NRG5). ▪ Because a lot of times, they are state sponsored, so you know, we were aware through intelligence briefings that they collect data by searching state entities to get some of the intellectual properties that we have, so we are not the only one doing that (NRG4).
	Collaboration	▪ The [IT and the IT security] put together the e-mail, they put together the statistics, they collect all the data from the exercise (GOV3). ▪ We have to do a lot more collaborative type of work, information sharing, and, you know, t2here's a lot of history with respect to how central IT is viewed on campus (HIED4).
	Mock phishing	▪ We gauge their push-through rates on mock phishing messages that we create and send out (NRG1). ▪ Given the regularity of the mock phishing attacks, the level of effort is appropriate (GOV2).

Buffering Cybersecurity groups' effort to protect their organization by erecting virtual walls	Threat detection	▪ We are blocking at least rooted devices and those types of things (NRG5). ▪ And the instant response is the detection part if the protection does not work (NRG4).
	Monitoring	▪ [Visits to unauthorized sites is] picked up as a red flag immediately by the active monitoring (GOV1). ▪ We're getting more and more into the networking monitoring piece side of things (HIED4).
	Defense	▪ When you're successfully blocking attacks you kind of forget about that (HIED3). ▪ We've put something in place to block what we believe are high-volumes of suspicious outbound e-mail and will put a person in the penalty box (HIED4).
Stakeholder actions		
Prioritizing Stakeholders' proactive support of cybersecurity initiatives	Compliance	▪ Our privileged users, people who have access to social security numbers and financial records, have an annual refresh requirement where they have to go through some updated training and then re-attest that they're aware of the policies and that they're following the policies (HIED6). ▪ Yes, [employees report spam or phishing emails]. So they're pretty responsive (HIED1).
	Conformance	▪ I've already mentioned the role-based security, where people have…if you're working in a production environment, you can't have access to the test and development environments (GOV1). ▪ Generally, the company is very supportive of where we're going and how we're evolving and maturing … so we kind of have the mantra that security is everyone's responsibility (NRG1).
	Attention and support	▪ Leadership do care about security (HIED4). ▪ We work with [the network team] to do the best practices, but when it comes to building a server, they're going to build a server and put the security controls in place…, but we work with them to decide (HIED1).
	Resource allocation	▪ One thing that we've done is to be staffed well for this. We have good folks, they are not just the technology, but the people, and then what we need to do is catch up on the process. So with good technology and good people, make sure that they're doing all those things properly (NRG4). ▪ So about two-thirds of our security budget is specifically for information security (NRG3).
	Reporting	▪ The spam's caught … by individuals assessing something as spam (GOV1). ▪ [Users] report [phishing emails] they can report it to abuse@hied1.edu, security@hied1.edu, or postman@hied1.edu (HIED1).
Hedging Stakeholders' qualified support of cybersecurity initiatives	Peripheral processing	▪ It's a very hard audience to actually reach. [Employees] do not pay attention (HIED6). ▪ Faculty go out without enough education or willingness to ask … what are the enterprise solutions, what are the consumer solutions that I should or shouldn't be using (HIED4).
Avoiding Stakeholders' evasion of cybersecurity initiatives	Apathy	▪ Our students…typically those are the ones that fall victim to [phishing] more often, either by not recognizing it. They have the horse led to water mentality. Oh, I got something from the university, I have to act on it and I don't question it. Or apathy (HIED1). ▪ Considering this particular industry, I would say that most people are really unaware, really unconcerned, if you look at an average across the entire population (NRG4).
	Doing nothing	▪ I would say that most people are really unaware, really unconcerned [about information security] (NRG4). ▪ Most … ignore those [zero-day threat] notifications (GOV3).
Thwarting Stakeholders' outright circumvention of cybersecurity initiatives	Ignoring	▪ The IT director said, well, we're not seeing [the threat] ... (GOV1). ▪ [At] the oil and gas fields, out at the wellhead level, … there's very little concern... about being vulnerable [to cyber-attacks] (NRG2).
	Resistance	▪ We had a situation about four years ago where somebody went to a pornography site (GOV1). ▪ We see pushback in terms of, you know, requiring authentication … So I think there's a level of frustration [from the information security unit]—I'm reporting [information security issues] to you [stakeholder] and you're not taking any action (NRG3).