Journal of the Association for Information Systems (2019) **20**(3), 186-212
doi: 10.17705/1jais.00533

RESEARCH PAPER

ISSN 1536-9323

It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups

Allen C. Johnston[1], Paul M. Di Gangi[2], Jack Howard[3], James Worrell[4]

[1]University of Alabama, USA., ajohnston@cba.ua.edu
[2]University of Alabama at Birmingham, USA., pdigangi@uab.edu
[3]University of Alabama at Birmingham, USA., jhoward@uab.edu
[4]University of Alabama at Birmingham, USA., worrellj@uab.edu

Abstract

An organization's ability to successfully manage information security incidents is determined by the actions of its employees, as well as the actions of various groups of employees within its organizational boundaries. To date, information security research has primarily focused on individual-level phenomena and has not yet explored group-level phenomena such as how employee groups recognize and respond to security incidents in a way that is consistent with the organization's security goals and objectives. The current study addresses this gap, thereby answering the research call for group-level security research perspectives. The present study explores how employee groups formulate their collective security efficacy, which influences how group members recognize and respond to information security incidents. Using a case study of a large healthcare research organization (HRO), we analyze two security incidents, a malware attack, and a physical security breach, to identify a unique set of ecological and social properties of employee groups that are salient to their collective security efficacy.

Keywords: Collective Security Efficacy, Information Security, Socioecological Theory, Social Disorganization Theory, Employee Groups, Thematic Analysis

Jason Thatcher was the accepting senior editor. This research article was submitted on March 8, 2016 and went through two revisions.

1 Introduction

Over the past decade, information security incidents have become a growing concern for organizations. One key takeaway is that no industry or organization is immune to security breaches (e.g., Anthem, Home Depot, JP Morgan Chase, Kaspersky Labs, RSA, and Target). When security incidents occur, an organization's ability to manage the incident depends on more than just the actions of its security professionals or its formal incident response teams. It also depends on the actions of its nonsecurity staff employees (Dutta & Roy, 2008). Of course, employees do not act solely based on their individual beliefs and experiences; rather, the workplace group to which they belong influences them (Bandura, 2000; Warkentin, Johnston, & Shropshire, 2011). These groups, termed here *employee groups*, are collections of individuals who "are interdependent because of the tasks they perform as members of a group, who are embedded in one or more larger social systems (e.g., community, organizations), and who perform tasks that affect others (such as customers or coworkers)" (Guzzo & Dickson, 1996, p. 308). An employee group explicitly or implicitly guides the employee's security response actions (Bandura, 2000; Paepcke, 1996; Sampson, Raudenbush, & Earls, 1997). These actions can include policy compliance behavior (Bulgurcu, Cavusoglu, &

Benbasat, 2010; Johnston, McBride, Carter, & Warkentin, 2016), protective security actions (Boss, Galletta, Lowry, Moody, & Polak, 2015), or proactive responses, such as reporting suspicious employee behavior (Straub & Welke, 1998). We believe that an employee group serves as the foundation upon which its members' security incident responses are formed.

An employee group influences its members' security responses based on the employee group's collective ability to recognize and respond to the incident in a manner that is consistent with the organization's security goals and objectives, defined here as *collective security efficacy*. For instance, the recent breach of the United States Office of Personnel Management (OPM) (Gallagher, 2015) was a social engineering attack that accessed the records of government workers and contractors holding US government security clearance. Several factors can influence how employees respond to such threats and one of these factors is the employee group and its ability to leverage resources and appropriate processes to successfully mitigate enterprise threats. In this context, a group security response is the coordinated and synergistic interpretation of the attack and the formation and communication of a cohesive response behavior expectation of the group's members. However, some organizational employee groups are more capable and effective in this regard than others (Chua, Wareham, & Robey, 2007; Lesser & Storck, 2001). In this research, we discover *why*.

Although academics and practitioners have focused considerable energy on understanding the factors that shape and support security incident responses (Crossler et al., 2013; Willison & Warkentin, 2013), the dominant perspective applied to this phenomenon has been at the individual level, supported by theories devoted to individual perceptions, motivations, and behaviors within the organization. These theories provide insight into how employees uniquely perceive and engage with security policies, mandates, and other activities when internal security incidents occur (Bulgurcu et al., 2010). However, research on group-level security incident response is lacking (Siponen, Willison, & Baskerville, 2008). Some authors note that the existing research on group-level security is inadequate and inconclusive, conflicted, or lacking clarity (Kubrin & Weitzer, 2003). Ultimately, academics' and practitioners' preoccupations with individual-level security perspectives and the inadequacy of group-level security insights effectively blind researchers in understanding how employee groups affect individual and organizational information security efforts.

With this view, we conducted a case study using social disorganization theory (SDT), a theoretical lens from the field of criminology, to understand group-level security efficacy. Our findings demonstrate how an employee group's collective security efficacy is influenced by its ecological properties and social properties. The ecological properties are the characteristics of the organizational setting that are imposed on an employee group and set the stage for the group's interactions. The social properties include the general social dynamics that all workplace groups leverage when faced with workplace events that warrant employee responses. [1] In the context of collective security efficacy, these social properties shape an employee group's efficacy in responding to security incidents, which ultimately shape each employee's security responses. The current study raises awareness of a gap, caused by a lack of group-level perspectives, within the existing information security strategies, and contributes to the literature by providing a more holistic understanding of how employee groups influence the individual employee's ability to effectively respond to security incidents.

In the next section, we synthesize the literature on collective security efficacy to conceptually establish the ecological and social properties that define it. We then discuss our theoretical lens to understand our focal phenomenon—the collective security efficacy of employee groups. Using semistructured interviews and the secondary data of two security incidents—a malware attack and a physical security breach—we draw conclusions about how socioecological properties influence collective security efficacy's development. We conclude with a discussion of our findings, limitations, and implications for future research.

2 The Collective Security Efficacy Phenomenon

We define collective security efficacy as *an employee group's ability to recognize and respond to information security incidents in a manner that is consistent with the organization's security goals and*

[1] A synthesis of the literature from the SDT does not coalesce around a standard label for the properties discussed in this manuscript. For instance, Kubrin and Weitzer (2003) refer to the ecological context (e.g., residential instability and poverty) and structural conditions (e.g., social ties and social capital) while Markowitz et al. (2001) refer to the macro, economic, and ecological conditions (e.g., poverty and ethnic and racial heterogeneity) and structural characteristics (e.g., cohesion). More recently, Kingston et al. (2009) refer to structural characteristics (e.g., residential mobility and population heterogeneity) and social structure (e.g., informal social control) while Mazerolle et al. (2010) explore ecological variables and structural characteristics (referring to the development of the social capital theory). Based on this review, we note how the literature recognizes two distinct groups of variables that we henceforth refer to as ecological and social properties.

objectives. As this definition suggests, an employee group's collective security efficacy depends the coordinative and synergistic interactions and shared understanding of its members (Bandura, 2000). For example, in situations in which new employees are unsure of policies or where policies are nonexistent, the group members' actions help the group recognize when it is necessary to improvise their security behaviors. More experienced employees assist others in interpreting a policy or aid in completing a security objective. This sharing of information and insight among employees within a group reinforces the social relationships and establishes the expectations for how group members should respond to security problems (Markowitz, Bellair, Liska, & Jianhong, 2001; Warkentin & Willison, 2009). Here, an employee group's ability to recognize and respond to information security incidents is defined in part by its *social properties*, or the characteristics of the social interactions and expectations among employees within a group. An employee group's social properties shape how the group interprets information and events and establish the baseline level of shared understanding for how the group's members should act when a security incident arises.

Additionally, this definition embeds employee groups within organizational settings, where security incidents are a part of the cost of doing business. Consequently, there are also the *ecological properties* of an employee group. These ecological properties influence the group's collective security efficacy and represent the characteristics of a group, serving as the foundation of its social properties. For instance, groups that experience a high rate of turnover (an ecological property) will have less effective social interactions (e.g., introduction interactions) than groups that experience less turnover (e.g., bonding interactions). In the event of a security incident, the social interactions of a group experiencing high turnover will be less interactive and more reflective of individual experiences, hence reducing the group's ability to collectively respond to the incident.

Together, an employee group's ecological and social properties define how its members interact, produce, share, and reference resources to respond to security incidents (Chua et al., 2007). To this extent, these properties and their influence on a collective outcome describe a socioecological phenomenon—an observable occurrence of interrelations among people and their environment. A socioecological theory can provide a useful lens for understanding this type of phenomenon.

3 Theoretical Background

The SDT is a socioecological theory, developed in the criminology discipline and focused on the relationships among community structure, social control, and criminal activity (Sampson & Groves, 1989; Shaw & McKay, 1942). Historically, the SDT has proven useful for understanding how community-level properties can deter a residential neighborhood's criminal activity (Shaw & McKay, 1942). The SDT posits that criminal activity within and involving communities occurs when these communities lack the appropriate structures, resources, and social maturity to protect themselves and their residents. Our review of the SDT literature indicates these structures can be decomposed into ecological and social characteristics or properties (Markowitz et al., 2001; Mazerolle, Wickes, & McBroom, 2010; Sampson & Groves, 1989) and that ecologically and socially developed communities are better able to detect and ameliorate threats to their residents' safety and property. A community's ecological and social strength dictates the degree to which it can understand how to govern and protect itself (i.e., collective security efficacy), resulting in the deterrence of criminal activity. As the social interactions among community members decrease, the social controls that influence each community member's (i.e., resident's) behavior weaken or fail to form altogether. This weakness then facilitates a disorganized environment in which community members rely less on the community and where criminal activities go undeterred (Kubrin & Weitzer, 2003; Shaw & McKay, 1942).

Although relatively untested empirically, the SDT literature presents a general relational structure: a community's ecological properties influence its social properties, which in turn influence its collective security efficacy (Kingston, Huizinga, & Elliot, 2009; Kubrin & Weitzer, 2003). Communities with a particular range of ecological properties may form and maintain stronger social interactions (Kubrin & Weitzer, 2003; Sampson & Groves, 1989). Further, it is these social properties of a community that shape its collective efficacy (Kubrin & Weitzer, 2003; Sampson & Groves, 1989). For instance, communities that have high socioeconomic status and low residential instability are more likely to have the necessary resources and consistency among their residents to develop strong social ties. These resources enable action in a cohesive and cooperative manner in the face of a threat to the community's security, facilitating a strong collective ability to coordinate and respond in an effective manner (Drukker, Kaplan, & van Os, 2005; Sampson & Groves, 1989). Alternatively, communities with high degrees of ethnic heterogeneity are not as likely to form strong social ties and may be less cohesive in situations where cohesion is paramount for success, including security incidents. Cultural attenuation and both formal and informal social control are also influential social properties, with informal social control widely seen as the most important social property for shaping a community's collective security efficacy (Sampson & Groves, 1989).

Table 1 presents an employee group's contextualized ecological properties and the indicators used to identify the presence and intensity of the properties in the contextual environment. Appendix A provides an overview of the original properties discussed within the SDT literature and a description of how we contextualized these properties to the organizational environment. For instance, diversity is a construct within organizational research that is the contextualized outcome for ethnic heterogeneity. Diversity reflects the demographic ecological properties that shape the composition of an organization's workforce and includes subdimensions such as ethnicity, gender, and religious affiliation, among others. Research on diversity in organizations generally supports the notion that heterogeneity positively affects organizational outcomes because it encourages new perspectives and experiences from dissimilar backgrounds to be shared (Hubbard, 2004). Along with a definition of each property, we also present indicators of the properties, showing how they manifest within groups in the context of collective security efficacy. These indicators allow us to differentiate between employee groups with a strong ecological foundation and those with weaker ecological foundations. This is useful because the broader SDT literature indicates that the strength of a group's ecological foundation is a determinant of the strength of the group's social structure (Kubrin & Weitzer, 2003; Sampson & Groves, 1989).

Table 2 presents an employee group's social properties and the indicators used to distinguish a group with a strong social structure from those with weaker social structures. These social properties are native to the SDT, but as also presented in Appendix A, we contextualized them to organizational employee groups. Collectively, these indicators identify employee groups with a strong social structure, which is a requirement of high-level collective security efficacy (Browning, 2002; Sampson & Groves, 1989; Sampson et al., 1997).

Table 1. SDT Contextualized Ecological Properties

Property	Definition	Source
Socioeconomic status	*The economic and social position of an employee group in terms of its members' education, income, and occupational status.*	Schulz et al. (2012); Winkleby & Cubbin (2003)
	Indicator(s): • High-performing employee groups are at least satisfied with their pay and benefits. • High-performing employee groups are paid at a rate higher than market, based on BLS data or other externally validated criteria. • High-performing employee groups have a higher rank within the organization.	
Diversity	*The degree to which an employee group is comprised of members that identify with one or more socioculturally distinct groups, including gender, educational attainment, ethnicity, cultural affiliation, and sexual orientation.*	Ely and Thomas (2001); Sampson & Groves (1989)
	Indicator(s): • High-performing employee groups are mostly of dissimilar ethnicities. • High-performing employee groups are mostly of dissimilar religions. • High-performing inside groups mostly have equal gender representation.	
Turnover	*The degree to which employee group members transfer, resign, retire, or are terminated from their position within the group.*	Drukker et al. (2005)
	Indicator(s): • High-performing employee groups rarely lose members voluntarily to other groups. • High-performing employee groups rarely have members that transfer to other groups.	

Table 2. SDT Contextualized Social Properties

Property	Definition	Source
Social ties	*The social channels that facilitate the exchange of resources among employees within an employee group.*	Oh, Chung, & Labianca (2004)
	Indicator(s): • High-performing employee groups have members that are involved in social events outside of the office. • High-performing employee groups have members who spend a great deal of time together outside of the office.	
Social capital	*The intangible resources produced via relationships among employees that facilitate actions for the mutual benefit of the employee group in terms of the group's structural, relational, and cognitive capital.*	Coleman (1988); Nahapiet & Ghoshal (1998)
	Indicator(s): • High-performing employee groups have extensive friendships among their members. • High-performing employee groups have overlapping memberships in social groups among their members. • High-performing employee groups have an obvious harmony among their members. • High-performing employee groups have members who often tell stories of people or events that took place in the past. • High-performing employee groups have members who often share metaphors at work. • High-performing employee groups have many unspoken rules that guide their practice.	
Cohesion	*An employee group's propensity for demonstrating resiliency against disruptive forces.*	Ronayne (2004)
	Indicator(s): • High-performing employee groups have a strong sense of obligation or reciprocity toward members in the group. • High-performing employee groups exhibit a high degree of trust among their members. • High-performing employee groups maintain a shared identity (e.g., "us" or "we" when referring to the employee group and "they" or "them" when referring to others).	
Cultural attenuation	*The extent to which normative conventions can be interpreted incorrectly and influence employee behavior within the employee group.*	Kornhauser (1978)
	Indicator(s): • High-performing employee groups do not distort communications or policies concerning appropriate security behavior. • High-performing employee groups review communications or policies concerning appropriate security behavior. • High-performing employee groups have the ability to direct questions or receive feedback from the organization on security policies.	

Table 2. SDT Contextualized Social Properties

Social control	*The formal and informal societal or political influences that shape and govern an employee group.*	Kubrin & Weitzer (2003)

	Indicator(s):
	• Formal social control
	  ○ High-performing employee groups question their activities to determine their accordance with the security policy.
	  ○ High-performing employee groups monitor their activities to determine their accordance with the security policy.
	• Informal social control
	  ○ High-performing employee groups question their members about their activities to determine if they are in accordance with the security policy.
	  ○ High-performing employee groups monitor the activities of their members to determine if they are in accordance with the security policy.	

In summary, as the leading socioecological theory for a collective-level understanding of security issues within a community setting (Chua et al., 2007), the SDT provides a reasonable lens through which to investigate the collective security efficacy phenomenon because (1) it is a derivative of socioecological theory, a perspective for understanding a group's ability to interact internally and with its environment to achieve a common goal; and (2) it attends to the socioecological properties that define the collective security response efficacy phenomenon.

4 Methodology

Our approach to examining the focal phenomenon utilizes the case study method (Yin, 2002, 2010). Case studies focus on "the understanding of the dynamics present in single settings" (Eisenhardt, 1989, p. 534), paying particular attention to how a phenomenon is embedded within its context (Gibbert, Ruigrok, & Wicki, 2008; Keutel, Michalik, & Richter, 2014; Yin, 2002, 2010). We conducted a case study using semistructured interviews and direct observations of several employee groups and their responses to two security events. We then used thematic analysis following the protocol established by Boyatzis (1998) to analyze the semistructured interview data and reconcile our analysis with our direct observations of an employee group's collective security efficacy. The unit of analysis was an employee group. We followed the case procedures adopted by Schlagwein and Bjørn-Andersen (2014) to ensure the robustness of our methodological approach and to present our findings in a similar fashion to highlight the abstract and concrete observations made from our thematic analysis.

Although prior research indicates that multiple cases are preferred over single cases for theoretical generalizability, single cases are preferred when a case (1) is particularly revelatory due to its inaccessibility to researchers, (2) critically evaluates or investigates a well-established theory, or (3) is unique and not easily replicated because of phenomenological circumstances (Keutel et al., 2014; Sarker, Xiao, & Beaulieu, 2013; Walsham, 1995; Yin, 2010). Our case meets these conditions by (1) investigating a large healthcare research organization (HRO) that allowed us extensive access to its employees, in-depth coverage of several employee groups, and organizational documents during a security incident event, making this case study difficult to replicate; and (2) utilizing a well-established criminology theory in a new phenomenological setting.

The HRO in this study has its headquarters in the southeastern US and has over 1.2 million outpatient visits annually, along with research facilities that employ over 20,000 individuals across the country. The HRO consists of both healthcare operations and research facilities, and it has an executive steering committee that oversees the organizational strategy. Moreover, the HRO maintains a central security IT function that is responsible for responding to security incidents and that must comply with a variety of regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA). Within such a regulatory environment, a single security incident or compliance failure may result in a financial penalty or revocation of the HRO's ability to conduct healthcare operations, sensitive research, or both. Both consequences serve as a strong incentive to the

HRO's executive steering committee to encourage security incident awareness and training for its employees.[2]

Due to the HRO's comprehensive and complex nature, multiple employee groups exist within the organization, creating an opportunity to validate our observations for analytic generalizability (Yin, 2002) while controlling for ecological influences. Although all the authors have professional working relationships with multiple employee groups within the research facilities, two authors also have collaborative working relationships with healthcare operations employee groups through consulting engagements.

During the study, we collected primary and secondary data (Boyatzis, 1998; Guest, MacQueen, & Namey, 2012; Yin, 2010). Primary data were collected through semistructured interviews with members from several employee groups (Crocker & Luhtanen, 1990; Stewart & Gosain, 2006). Semistructured interviews allow a researcher to enter the interview with some initial goals via high-level questions that begin the discussion, but also engage in improvisation to elicit greater understanding and feedback from the interviewee concerning a phenomenon (Myers & Newman, 2007). This approach enabled us to evaluate the degree to which an interviewee understood the questions being asked and allowed for reframing and refining the interview questions over time to improve our data-gathering process. The interviewed members possess intimate knowledge of the ecological properties of the HRO, the unique social dynamics of their respective employee groups, and the ability to assess how these properties influence their employee group's collective security efficacy (Segars & Grover, 1998). To avoid influencing the direction of the interviewee's responses (Myers & Newman, 2007), we did not provide examples or rephrased questions until prompted by the interviewee.

To ensure a diverse set of perspectives, we purposefully set out to interview employees with distinct roles, physical and logical placement, and responsibility to their respective employee groups, which we found to be representative of the breadth of the organization. In total, we interviewed 27 employees who self-identified with six unique employee groups; a final employee group (Group G) represented a collection of single employees from four distinct employee groups that served as verification for theoretical saturation in the data analysis. Table 3 outlines the descriptive statistics for each employee group, including educational attainment, age ranges, and gender. Appendix B includes the interview protocol.

The HRO also asked one of the paper's authors to participate in a safety and security task force as a security professional because of a physical security breach that occurred within the HRO. This created an opportunity for the author to observe, engage, and document the affected employee groups and the interactions among their respective group members. We also collected secondary source data from organizational policies (e.g., employee handbook, intellectual property agreement, and enterprise code of conduct), meeting minutes (e.g., safety and security task force), observations from organizational and employee group meetings (e.g., new employee orientation, social gatherings, etc.), and organizational communications relating to security events; this information enriched our interpretation of the primary data. In particular, we used our direct observations and the secondary data to provide a contextual background for each of the security incidents investigated in this study and to enrich our understanding of the HRO's security operations and work environment.

We followed a hermeneutic approach to our data analysis, moving between "the whole to part and back to the whole" (Gadamer, 1975, p. 75) to ascertain the meaning of our data (Boyatzis, 1998; Cole & Avison, 2007). To transition between these phases, we used a thematic analysis for translating our data to describe implicit and explicit ideas and patterns and termed themes to understand the focal phenomenon (Boyatzis, 1998; Guest et al., 2012). Thematic analysis provides a structured iterative data analysis process designed to reveal theoretical abstractions and generalizations in the data to understand the HRO, the employee groups, and the ecological and social properties that influence collective security efficacy in a reliable manner through the use of codebooks. Tables 1 and 2, shown earlier, include the definitions of the properties that inform the construction of the interview protocol (i.e., interview questions) and the indicators that serve as the codebook to conduct the thematic analysis coding. In doing so, we leverage the literature on the SDT to provide a sensitizing lens but rely on the data and our interpretations to guide our understanding.

[2] All employees received initial onboarding training relating to information security policies (e.g., acceptable use policy, data privacy and security policy, and antidiscrimination training). Research-oriented employees receive additional training that is relevant to human subjects on a biannual basis, and medical-oriented employees receive human subjects training as well as refresher training on HIPAA compliance. All employees receive organization-wide security education awareness training on an ad hoc basis periodically through several security assessments (e.g., phishing tests, security audits, etc.).

Table 3. Employee Group Demographics

Employee group (group size)	Work unit type	Number of interviews	Gender	Avg. tenure	Educational attainment
A (n = 19)	Research / Business development	4	4 male	20 years	4 doctorate
B (n = 12)	Staff / Business development	3	1 male 2 female	12 years	3 master's
C (n = 11)	Research / Applied sciences	3	3 male	7.7 years	2 doctorate 1 master's
D (n = 25)	Administrative services	6	3 female 3 male	10.4 years	1 doctorate 3 master's 2 bachelor's
E (n = 12)	Research / Basic sciences	3	2 male 1 female	13 years	3 doctorate
F (n = 14)	Research / Medical	4	2 male 2 female	15.8 years	4 doctorate
G (Misc.)	n/a	4	3 male 1 female	9.8 years	3 doctorate 1 master's

To ensure the validity of our study, we focused on ensuring our finding's credibility, reliability, and confirmability (Guba & Lincoln, 1989). First, we adopted the informant feedback approach, where members from employee groups provided feedback to reduce the potential that our findings "may be biased in favor of the perspectives of the researcher, excluding important alternative interpretations from the informants [members]" (Bygstad & Munkvold, 2011, p. 41). Second, we assessed the reliability of abstract generalizations using a thematic analysis and interrater reliability for coding themes found within our primary codebook (Landis & Koch, 1977). Using Cohen's Kappa, we calculated an interrater reliability of 95.3%, indicating excellent reliability for our findings. Lastly, we presented our findings to an employee group for discussion and feedback to ensure we properly assessed group dynamics and to verify that no single employee perspective biased our findings.

5 Overview and Findings of the Case

All organizations are susceptible to security incidents; the HRO investigated in this study is no exception. The two security incidents we describe next affected multiple employee groups and caused the collective security efficacy of each group to be tested. The first security incident enabled our research team to understand how employee groups were defined, the ecological properties of various employee groups within the organization, and how those properties helped to dictate the social structure of the respective groups, as identified through their social properties. The second incident occurred during our data collection for the first incident and allowed us to confirm the relationships between a group's ecological properties and its social properties while also demonstrating how an employee group's social properties can influence its collective security efficacy and subsequent employee security response behavior.

5.1 Malware Attack Security Incident

The first security incident was a malware attack that plagued information systems and data assets throughout the HRO and its various employee groups.[3] In 2013, malware was discovered on one of the HRO's primary domain controllers (server). Because domain controllers are integral to the network's ability to authenticate users, they are prime targets for hackers or other malicious individuals seeking to disrupt or corrupt network operations. The IT department first isolated the server to evaluate the extent to which the HRO's systems had been compromised. Following an initial investigation, the IT department issued a mandatory, organization-wide password reset and demanded enhanced requirements for

[3] Employee groups C, D, E, F, and G (misc) were impacted by the malware attack security incident.

password strength and duration.

At this point, the IT department believed the situation to be contained, and they were in the process of resuming normal operations when the central firewall detected repeated outbound requests to an unknown server on an application port that is commonly used for exploitation. Through a log analysis, the IT department determined that additional systems had been compromised, requiring further investigation. The investigation revealed that the initial access to the original server occurred several months prior to its discovery and was an entry point for a series of attacks that included installing malware and key-logging software, as well as configuring an open remote desktop server. Initially, the hackers had installed malware to create a Bitcoin mining farm on employee desktops and servers. However, further review detected additional malware applications that compromised administrative credentials (including domain administrator) through key-logging software and a brute force attack. Additionally, the initial action to force a password reset alerted the malware attackers that they had been detected, which resulted in a phishing attack against the HRO. The ensuing phishing attack mimicked the legitimate password reset message and resulted in further compromises (including payroll systems). Because the initial request for password reset occurred while still-infected systems were active within the organization, affected employees had to change account passwords a second time because the first solution resulted in the affected employees being compromised a second time. Two months after the discovery, the HRO had reconfigured all systems, and the overall operating conditions were back to normal.

From an organizational perspective, this particular malware attack impacted certain employee groups differently than others. The malware attack's resolution took approximately one month from the attack's identification to its removal. Within one employee group, roughly 22.5% of the employee systems were compromised, resulting in the systems being reinstalled. A by-product of these remediation actions was the loss of personal information. For other groups, the impact was much less severe, with some groups not being aware that the attack and recovery processes had even occurred.

Many employees pointed to their respective group's ecological properties and how these properties influenced the definition of the group's membership and established the group's foundation for social structure and collective efficacy relative to the attack. From the existing contextualized SDT properties, socioeconomic status and turnover helped define not only whom the group's members consulted, but also how they viewed their respective group's responsibilities in participating in the organization's overall attack-mitigation efforts (e.g., password reset). In terms of socioeconomic status, one employee states, "The broader the span of control an (employee) has, the greater the appreciation for the effects (of security concerns)". Because of their organizational position, some employee groups felt obligated to take leadership roles in investigating how the attack occurred, encouraging members to serve on rapid response task forces and governance review committees. Recall that for this context, groups with a high degree of formal social control would be more likely to question and monitor their group's activities and whether the group is acting in accordance with the organization's security policies; they would also help to refine and improve those policies where appropriate. They will then challenge their members through informal social control to engage in the security response activities preferred by the group.

Other groups and their members gave a far more passive response. Another employee echoed this sentiment, commenting on the difference in responses among a group of lesser paid janitors, for example, as opposed to a group of top executives: the "latitude and freedom" associated with groups comprised of people of his "pay grade" would allow for "more discretion on how we spend our days and to whom we talk to and what we do". His insinuation is that groups with a greater socioeconomic status within the organization have greater flexibility and freedom in their response to security incidents while groups of a lesser socioeconomic status act in a more individualistic fashion. Groups acting in a more engaged fashion to security incidents demonstrate harmony, a key indicator of relational social capital. Their synergistic approach is also indicative of cohesion; they work together as a group to demonstrate resilience against disruptive forces, such as the malware attack described in this case.

In terms of turnover, the groups that were more active and responsive to the attacks were the ones that also had the greatest retention among their members. Lower turnover allowed these groups to draw on the insights and experiences of a broad scope of members who had "seen it all" or "been there, done that". Conversely, the less-effective groups alluded to turnover within their group as having a negative effect on their comfort in acknowledging to each other that their role as victims in the attack and in sharing beliefs as to how "people in our role should help figure out what happened". This speaks to the importance of stability (turnover) as a defining ecological property of an employee group. Groups with high levels of cohesion have a strong sense of emotional support among their members, something absent from groups with higher turnover. Further, groups with a strong informal social influence shape their members' activities in a manner similar to what is described here.

Prior literature within the criminology discipline indicates that diversity (i.e., ethnic heterogeneity) is an influential ecological property that enables the formation of collective synergies and outcomes. However, interviewees did not cite ethnic, religious, or gender diversity as a group property that facilitated their group formation or in how they respond to security incidents. They did, however, frequently mention shared understanding and communication effectiveness within their groups as outcomes resulting from educational attainment and homogeneity. As one employee states:

> *From an education standpoint, I think diversity affects security greatly. With the more education you have, the more knowledge you know about a particular area that will influence how you go about implementing a particular security guideline or policy. It also helps to have effective communication. Rules and procedures must have a rationale. If I'm sitting here and I don't know anything, that's an issue.*

This insight, consistent with others from our interviews, suggests that for the purpose of forming a shared understanding of a security incident and establishing ongoing social exchanges concerning the incident, all group members must have high levels of educational attainment and homogeneity. As groups become less homogenous in their levels of educational attainment or begin to hold a consistent, but lesser degree of educational attainment, they are less likely to achieve coordinated, informed security incident responses. This anecdote also underscores the connection between a group's educational attainment and homogeneity and its social ties, social capital, and cultural attenuation. Groups that share a high degree of educational attainment in a consistent manner (homogeneity) across their members will contribute resources and support to their members, which is evident in the communication and information-sharing exhibited in this case. Further, groups that have a homogenous level of educational attainment exhibit a lesser degree of cultural attenuation, minimizing distortion in communication among their members because these members review and question their group's desired response.

Cumulatively, in the HRO, the ecological properties of socioeconomic status and turnover clearly defined group membership and directly affected how the groups shared details of the malware attack incident and organized themselves in establishing norms for their members' responses. Presented in Table 4, these two properties are carried forward from the SDT.

Table 4. Ecological Properties Salient to an Employee Group's Collective Security Efficacy

Ecological properties	Definition
Socioeconomic status	The economic and social position of an employee group in terms of its members' education, income, and occupational status.
Turnover	The degree to which employee group members transfer, resign, retire, or are terminated from their position within the group.

Educational attainment and homogeneity also emerged from our thematic analysis as ecological properties of employee groups, suggesting a revision to the diversity property is germane to the collective security efficacy phenomenon. Specifically, the malware incident highlights the importance of higher levels of education and the homogeneity of an employee group's education for developing a foundation for the group's collective security efficacy. Table 5 provides the definition for this emergent property and the indicators used to represent high-performing employee groups regarding this property.

As mentioned earlier, the first security incident provided us with a background for understanding the ecological properties of an employee group's social structure, as represented by its social properties. The second incident allowed us to confirm these relationships while also observing how a group's social properties inform its collective security efficacy. This observation occurred in real time while the HRO was investigating and resolving the security incident. Due to the timing of this incident, the HRO asked one author to participate on an ad hoc, employee incident response team (i.e., the safety and security task force), allowing us to directly observe and record individual employee and employee group perspectives and behavior from both an internal (participating author) and external (other authors) perspective.

Table 5. Emergent Ecological Properties Salient to an Employee Group's Collective Security Efficacy[4]

Emergent Ecological Property	Definition
Educational Attainment and Homogeneity	*The degree of educational attainment and similarity in the attainment held by group members*
	Indicator(s): • High-performing employee groups have high levels of educational attainment among their members. • High-performing employee groups have homogenous educational backgrounds among their members.

5.2 Physical Security Breach Incident

In June 2013, someone reported that one of three submaster keys for a single, multilevel building within the organization was lost.[5] This particular submaster key accessed over 60 percent of the office space within the building. Shortly after the reported loss, a series of thefts occurred, and they included both physical and electronic data. The thefts occurred in offices accessible by the lost submaster key. Based on internal security investigation reports and employee observations, the thefts began in early June 2013 and continued for a period of about one month, with relatively little awareness by most of the HRO's employees. The HRO's security department investigated these initial thefts and concluded a lapse in basic security precautions (i.e., locking office doors and failure to challenge nonbadged outsiders) was the primary cause behind the data thefts.

A few months after the HRO supposedly resolved the initial set of thefts (August 2013), a large theft of physical data occurred from a single office. Video surveillance showed two external agents posing as employees and attempting to gain access to several offices.[6] The HRO's security department once again pointed to lapses in basic security precautions as the cause. However, several employee groups questioned this assertion's validity, resulting in the creation of an incident response team. The HRO charged the newly created safety and security task force with reviewing security documentation and current security practices. Based on this review, they were to recommend improvements to security processes and infrastructure. The task force leaders were individuals with the most seniority and experience with security incidents. Their peers believed the task force's members possessed the highest amount of historical knowledge of the employee group, as well the credibility needed to share the task force's recommendations with the relevant employee groups.

During the task force's deliberations, surveillance video revealed that outsiders, posing as legitimate employees, were testing doors and not using the lost submaster key to gain entry. They were also concealing their faces from closed-circuit video monitoring. An informal inventory audit resulted in several additional data theft reports. At this point, the task force provided an initial report reaffirming the security department's conclusions regarding lapses in basic security precautions and recommended employees maintain a higher level of security awareness during business operating hours. The task force's chairperson presented these recommendations at a group meeting to reduce confusion concerning the recommendations and to explain the rationale for the recommendations in light of the evidence reviewed.

Three weeks after the task force presented this recommendation to the employee groups, two employees reported that the suspected perpetrators had approached them in their offices, seemingly surveying the offices for materials of value for future theft activity. When challenged (a specific recommendation from the task force), the suspects proceeded to ask for clarification about visitor procedures and immediately left the premises. At this point, employees within multiple groups engaged in email exchanges within

[4] We use the term "emergent" to represent properties that are not specified in the SDT literature as traditionally part of the SDT but that are revealed by our thematic analysis to be salient to an employee group's collective security efficacy.
[5] The physical security breach incident impacted employee groups A and B. Although the malware attack security incident affected both groups, the interviews for these employees focused solely on the physical security breach incident.
[6] Although the organization maintains a 24-hour operational period due to its medical center, the data theft incident occurred in a building that maintains an 8 am to 10 pm operational period, with the "busiest period" occurring between the hours of 8 am and 6 pm. As a result, the external agents purposely selected a period that reduced potential discovery to conduct their thefts (7 pm to 9 pm).

their respective groups, expressing concerns over the earlier internal security investigation's conclusions and concerns for their own physical safety; they requested further analysis by the safety and security task force in light of these social engineering attempts. They also inquired about the existing security policies to determine whether modifications should be made to both policy and security infrastructure. The security task force reviewed their previous deliberations in light of this new evidence.

Our interviews reinforced what we found from the malware attack incident: the ecological properties of socioeconomic status, educational attainment and its homogeneity, and turnover defined employee group membership and set the foundation for social exchanges to cope with the incident. We found that social properties help to refine an employee group's collective security efficacy, contributing to the group's collective ability to recognize and respond to incidents, such as the physical security breach described here. For instance, one employee comments on her group's ability to manage the physical security breach:

> *At work, it's very collaborative. We spend a lot of time together. We like meetings here. But we make a lot of group decisions, so it's not really driven down from above. So at work, I think we all spend a lot of time together, a lot of interaction. Outside of work, there's some. Not a lot, but some. When I think of within my group, we run things past me and another member before we do so with anyone else, just because we want to know how something works, why it works, is it possible.*

This illustrates that for groups with strong member relationships characterized by frequent and beneficial exchanges of knowledge and insights, their members were more aware of the physical theft and participated more in its investigation. They also used their strength of social ties and social capital to help their members understand an appropriate perspective of the theft incident and how they should navigate discussions with peers outside their groups. The group's cultural attenuation was also evident as instrumental in shaping how consistent its members were in understanding the theft incident. The groups with the most consistency among their members, in terms of their understanding of the incident and how they should respond to it, were those whose members were consistent in how they interpreted each other's perspectives and actions. For instance, one employee, when questioned about his group and its members' attenuation from the group's established norms, states the following:

> *Well, I think there are some, I do think that they are ignored, sometimes, in that people can sometimes not take precautions, perhaps, that they should. I don't think that they ignore them to willfully break rules, but it could be ignorance, literally not knowing what the, how to handle a particular some type of information or what the rules say for how long the information has to be stored and under what conditions. So there's that. I don't think it's an active defiance in most cases, but it could be laziness. I think that's more attributable to that. It's more passive than an actual defiance of rules.*

Our interviews also show the perceived relationship between position level and educational attainment, where high-level positions are associated with researchers or administrators who possess doctorates and master's degrees while lower-level positions have less formal education. Through educational attainment, groups are able to understand security incidents and the importance of security policies, hence mitigating risks to the employee group. One employee, speaking of his employee group, succinctly notes the connection between educational attainment and homogeneity to cultural attenuation:

> *I've worked with people in lower-level positions who don't really have a good grasp as to what security policy is…people in higher-level positions, they have more knowledge, or they're more computer literate to be able to handle security and be able to understand what security is about. Whereas, someone in a lower-level position, they may not be as knowledgeable.*

We also found that an employee group's cohesiveness influenced its ability to maintain a consistent tone among members regarding the incident, even when faced with information that conflicted with the group's shared understanding of the incident. This was an important condition for groups with high levels of collective security efficacy. Groups with higher levels of cohesiveness had members with more rigid perspectives on the theft incident and on the efforts of the HRO's security department. One employee notes his group's consistent sentiment about the HRO's security department's work with them:

> *I do think we are a very close-knit group. Right now, we are having a problem with the public machines. They [HRO security department] were getting updated to Windows 7, and they told us that it would take about a week…I think we have ten machines that are finished, a couple that don't work at all, and most of them still have not been done. So it's kind of like it's us against them. We're kind of pushing them to solve this problem.*

Another employee also comments about her group's cohesiveness, suggesting that the group's

unity allows it to be more relaxed about but still conscious of security threats:

> *Yeah. We're a lot more relaxed. Because I trust you, or whoever in this area, I probably am more apt to leave my office door open when I run across the hall because I know somebody's here. If I didn't have that, I probably would be a little more guarded.*

We also found that one of the ways in which highly effective groups ensured the sharing of perspectives across their members was through both formal and informal social influence. The formal social pressures were evident in how the HRO distributed policies among group members, while the informal social pressures were reminders from within the groups to act according to the formal policies. One employee comments:

> *I look not only at the ones who are the social leader, rah-rah type, but also the ones that have respect (within the community). People respect them, and if they say this is something we need to do or try to get behind something, they will probably have buy-in. The biggest factor in security is how serious your leadership takes it. It's their investment in people, time, and money. They influence it (security) in two ways: (1) by what they do, and (2) by influencing others—some individuals are more influential than others because they have garnered respect over time. People were mad and were tired of stuff getting stolen; no one was thinking about our security, and so my boss (a community employee of her community) said…we gotta do something.*

Another employee echoes the importance of an informal social influence:

> *[When a security incident occurs…I think of people that are seen as the informal social leader of the community. There's people in formal roles, but there's also people that informally are...like you have to run something through them.*

In September 2013, the task force presented an additional series of recommendations to improve the existing security policies and infrastructure. The task force evaluated evidence from the incident and composed a series of social and managerial policy and procedure recommendations, including (1) increased community awareness of social engineering tactics, (2) policy development for visitor access, (3) increased community awareness of physical security (e.g., checking locked doors), and (4) sporadic inventory audits to more precisely identify theft timings. Furthermore, the security task force recommended security infrastructure modifications including: (1) automatic door locks for individual office doors, (2) digital office suite locks that could be remotely monitored and made time-sensitive for access, and (3) the expansion and upgrade of security camera infrastructure. Critical to the task force's ability to make these recommendations was access to the organizational resources supplied by the employee group (e.g., incident reports), organizational policies on visitors and security awareness training, and reports on physical security maintenance and monitoring documentation. These resources provided additional context and understanding of the security incidents and the current effectiveness of the safeguards designed to protect the employee groups.

When presenting to the employee groups, the task force selected the member with the greatest tenure within the organization and highest administrative title to ensure that the employee groups viewed the recommendations as legitimate; this indicates social capital plays a direct role in the informal social control a nonadministrative task force has on employee group behaviors. In the days during and immediately after the efforts of the task force, it became apparent that some employee groups had members who were far more informed, proactive, and resolute in their efforts to respond to the physical data theft incident than others. Across their respective members, these groups maintained a consistent perspective about the incident and a cohesive spirit toward assisting one another in executing the shared expectations for how to respond to the incident. As one employee mentions:

> *When there is perhaps a common threat that is detected by several (community members), then we can each try to solve it individually on our own or we can collaborate and solve it collectively. Cooperation is the lifeblood of any collaborative effort (including security) because even if some portion of the group may not agree, they will cooperate because they are a member of the group and they would expect cooperation from others.*

The highly effective employee groups also drew frequently from the insights of their more experienced members and took steps to ensure that these insights and any new knowledge were processed within the group to make them accessible for future needs. We frequently observed groups leveraging institutional knowledge from senior employees to understand how best to approach the security incident, specifically how to interact and cooperate with the HRO's security officials. These senior employees not only provided direction for the group, they also helped form a consensus within the group. For instance, a previous quote notes how one employee's group would "run things past me and another member…just because we want to know how something works, why it works, is it possible". These senior people acted as resources to

help evaluate whether responses would align with the policies and goals of the HRO.

Collectively, the social properties of these employee groups defined a framework for sharing experiences and insights among group members and helped define how the members should work together to resolve the physical security breach incident. These social properties also seemed to depend on the ecological properties of the group that first shaped the group's structure and underlying collective capacity. Employees further note how ecological properties, such as turnover, directly impact social properties in terms of developing cohesion and social capital and fostering collaborative evaluation of security incidents:

> *It takes time. When someone's first just coming in, you don't know how they may handle a particular situation…I think that trust is built over time…You've got to develop some type of relationship with them. You've got to be able to understand them to a certain extent, and then you're able to come to some common ground.*

Cumulatively, the social properties of social ties, social capital, cohesion, cultural attenuation, and social control describe the social forces that shape how information and events are interpreted by employee groups and establish the norms for their members' actions in response to security incidents. Presented in Table 6, we carried forward these social properties from the SDT and found each one to be pertinent to the collective security efficacy phenomenon.

Table 6. Social Properties Salient to an Employee Group's Collective Security Efficacy

Social properties	Definition
Social ties	The social channels that facilitate the exchange of resources among employees within an employee group
Social capital	The intangible resources produced via relationships among employees that facilitate action for the mutual benefit of the employee group in terms of structural, relational, and cognitive capital
Cohesion	An employee group's propensity to demonstrate resiliency against disruptive forces
Cultural attenuation	The extent to which normative conventions can be interpreted incorrectly and influence employee behavior within the employee group
Social control	The formal and informal societal or political influences that shape and govern an employee group

Beyond the set of ecological and social properties espoused in the SDT, a set of social properties emerged that were specific to an employee group's collective security efficacy. These social properties became more apparent as the investigation into the physical breach security incident progressed. In terms of the new knowledge that was brought into the groups for refining their shared perspective of the security incident, the effective groups had members who collectively reflected on the incident and cooperatively searched for explanations for how the incident occurred and how it could be prevented in the future. As one employee comments:

> *I think as a group, we tried to collectively understand the root cause of the attack. We all looked at the documentary evidence and our interactions with relevant employees that had information that could help us to understand what happened. It led us to raise questions about whether the attack was our responsibility and how we should approach others about it.*

Furthermore, the task force heavily relied on organizational resources, such as policy databases, incident reports compiled by security personnel, and infrastructure blueprints, to understand the physical and logical security context. As a result, organizational memory emerged through direct observation of the task force and the employee groups that sought additional organizational resources to better understand existing policies and security procedures. Through the thematic analysis of our interview data, collective induction and collective reflection also emerged as employee group properties relating to the collective security efficacy phenomenon. These properties are presented in Table 7.

Table 7. Emergent Social Properties Salient to an Employee Group's Collective Security Efficacy

Emergent social properties	Definition
Organizational memory	*The mechanisms, functions, or actions taken by the employee group to encode, store, or retrieve employee knowledge.*
	Indicator(s): • High-performing employee groups follow a formal data management process to ensure detailed information is available to the organization. • High-performing employee groups are able to quickly access information or knowledge from appropriate personnel. • High-performing employee groups utilize synthesized information or knowledge provided by the organization to accomplish their work tasks.
Collective induction	*The cooperative search for descriptive, predictive, and explanatory generalizations, rules, and principles.*
	Indicator(s): • High-performing employee groups make strong efforts to collectively identify and define security problems. • High-performing employee groups frequently seek out specific information relevant to security problems.
Collective reflection	*The intellectual cooperation of employees, through which information is created, becomes meaningful and is translated and transformed into new information.*
	Indicator(s): • High-performing employee groups indicate they often take an introspective approach toward security. • High-performing employee groups frequently analyze and question why they do things regarding the security of their organization. • High-performing employee groups often explore the abstract implications of security on organizational operations.

Finally, our interviews also provide evidence of how an employee group's collective security efficacy influenced the actions of its members, increasing their effectiveness in responding to security incidents. For instance, when asked to describe how the synthesized knowledge of security issues, incidents, and policies within his group influenced the security actions of his group's members, one employee notes:

> *I just believe the nature of being part of a group brings some accountability. I think there's a lot to be said for the collective mentality of honesty or integrity or appropriate behaviors, and I think in that way we all influence one another.*

Another employee also comments on the translation of collective efficacy into security outcomes:

> *A good practice we just started that emerged from the group is we now try to shred that stuff that you can that you're no longer using. We knew we had to do something with this paper instead of just throwing it out in the trash, so we go to the shredder.*

The previous anecdotes provide examples of how highly functioning groups with high levels of collective security efficacy increased the effectiveness of their members' security responses. Poorly functioning groups, whose ecological and social properties did not support a high level of collective security efficacy, demonstrated less-effective security response outcomes among their members. One employee notes:

> *Everything is basically about business to a point because we don't really know each other. If I knew you well enough, I'd close your door. If I don't know you…if I don't feel that that would bother you because of one reason or another, I would say, "You've got your papers sitting out on your desk", and the next question would be "Why the hell are you worried about my papers on my desk?" You don't want that conversation to get started, so you just kind of back up off of it.*

Perhaps the clearest example of collective security efficacy playing a direct role in security effectiveness is the physical data breach incident. Two affected employee groups—research team and administrative services in the business development work units—each identified security issues by questioning the existing security policies regarding visitor access to the physical building. These actions led to modifications in the security policies for visitor access. No further physical data breaches occurred once the HRO implemented this new policy, suggesting the employee groups effectively addressed their security concerns and placed new safeguards for the protection of physical data and personnel.

In summary, our findings indicate that nearly all the original sets of ecological and social properties espoused by the SDT were instrumental in shaping an employee group's collective ability to respond to an information security incident. The interviews, though, do not mention the ecological property of diversity, and we did not observe it as relevant to an employee group's collective security efficacy. The findings also reveal the presence of new influential ecological and social properties; the social properties of a community depend on the community's ecological properties. These emergent properties expand our understanding of the ecological and social properties that influence a group's collective security efficacy.

6 Discussion

The ability of an organization to respond to information security incidents is influenced by the various groups of employees that emerge from within its borders. In this study, we sought to understand why some employee groups are more capable than others in recognizing and responding to information security incidents in a manner that is consistent with the organization's collective security efficacy. The vast majority of information security research focuses on the individual level, resulting in a gap within the literature at the group level. To the best of our knowledge, the current study is one of the first to identify the properties of an employee group that contribute to the organization's collective security efficacy. As such, we make several contributions to the literature. Employee groups are often cited in the information security literature, but neither defined nor characterized, much less studied as a key ingredient in an organization's response to an information security incident. In this study, we advanced this understanding. We also responded to the challenge of editorial boards for new perspectives on information security, beyond those of just the individual (Belanger & Crossler, 2011; Bélanger & Xu, 2015; Siponen et al., 2008; Willison & Warkentin, 2013).

The formation of an employee group's collective security efficacy reveals much about its ecological and social underpinnings. Organizational employee groups are logically organized and socially constructed as much as they depend on the physical structures imposed by the organization (Berger & Luckmann, 1991). The SDT has evolved from its original context of geographically bounded neighborhood community structures—including the macroconditions, such as poverty, ethnic heterogeneity, and residential turnover—that influence these structures and govern social activity within the communities. In the organizational context, these properties give way to a different set of ecological and social properties that align with the shared digital and social infrastructure that connects employee groups across an organization. We contribute to the research on collective efficacy by providing a more holistic understanding of the employee group's properties and how they influence its ability to respond to security incidents in a manner that is consistent with its organizational goals and objectives, a context previously unexamined.

Our findings show that employee groups within a broader organization act uniquely in their collective responses to information security incidents. Even though an organization has overarching security policies and procedures that dictate how security incidents should be approached, each group may form its own interpretation and enforcement of the policies that influence its members' responses to incidents differently because of variation in the ecological and social properties held by employee groups. This finding points to a security incident response as something that is practiced at a functional or social level rather than at the broader organizational level. Security incident responses are established in employee groups, and those groups will reinforce or deviate from one another with the cumulative result being some level of incident response that aligns more or less to the desired security goals and objectives of the organization. Although organizations design security incident response procedures to govern security incident response activities within organizations, the current research demonstrates that the actual implementation of the procedures occurs at the group level across multiple employee groups within an organization. Consequently, the present study challenges the notion that a single-level perspective can adequately explain an organization's security incident response. Specifically, this study indicates a multilevel perspective may best explain an organization's ability to respond to security incidents.

Our results suggest a close agreement with the general property sets and the triadic and reciprocal associations among these sets; an employee group's collective security efficacy is a product of (1) the ecological factors that define its membership, how its members become aware of an incident, and the foundation for its members' social exchanges relative to the incident;

and (2) the social properties that establish the social structure of an employee group when presented with a security incident. Of the ecological properties identified as salient to an employee group's collective security efficacy, educational attainment and homogeneity emerged from our thematic analysis of the interview data as an important property. Organizational memory, collective induction, and collective reflection also emerged as salient social properties beyond those previously established in the SDT literature. Collective induction and collective reflection are the qualities of an employee group that allow it to respond to unfamiliar threats, and these qualities rely on the employee group's organizational memory, social ties, social capital, cohesion, cultural attenuation, and social controls to provide guidance for similar incidents. By providing precision to the definitions of the traditional ecological and social properties and the associations among those properties, uncovering new ecological and social properties within the context of an employee group's collective security efficacy, we expand the range of phenomena applicable to the SDT and provide the information security discipline with a group-level lens with which to examine security incident responses within organizational settings.

6.1 Limitations

Given the single-site case study approach, the generalizability of our results is a concern. We partially chose a single-site case study because of the extensive level of access given to the authors in terms of interview time, direct observation of real-time events, and internal organizational documents concerning security incidents and group behavior. The organization investigated in this study is a complex healthcare operations and research facility, creating a unique mixture of regulations and security compliance concerns that may produce security-conscious employees atypical in comparison to other types of organizations. Moreover, our case study approach provides a richer, more descriptive understanding of the groups within the organization, including how employees worked together to mitigate security threats. Nonetheless, the research design does present a limitation due to the narrow contextualization of the findings to a single organization and the possibility that other organizations would not function in a similar manner. Future research should seek to replicate the findings of the current study in a variety of organizations and possibly conduct a quantitative test of the theoretical model derived from the current study. This will ensure the generalizability of the collective security efficacy model and test the proposed constructs and their associations.

Another limitation of this study concerns its focus on a single-group perspective; that is, the focus we asked employees to place on a single employee group throughout the interview. As described earlier, an employee can belong to multiple employee groups—or subgroups for that matter—and each group will impart its influence on the individual employee. For instance, a few employees referenced groups that included individuals—such as janitorial staff or other employees—who are more commonly associated with a geographic location or organizational entity (e.g., IT department) than defined as being members of their employee group. Because the focus of this study ultimately narrows the discussion to a focal employee group, it is possible that employees possess multiple employee groups or could extend their employee groups under certain security incident situations (e.g., physical versus electronic incidents), suggesting the need for further examination of how employee groups influence collective security incident response efficacy. In fact, our direct observations of the task force suggest that the artifacts created from other employee groups (e.g., the security personnel reports and security infrastructure blueprints that were operationalized as the organizational memory social property) could have impacted an employee group's understanding of the security incident. However, because this is the first study to attempt to capture the determinants of a group's collective security efficacy and how that efficacy influences its response to security incidents, we placed intergroup and subgroup influences outside the study's scope, but argue that such research is a necessary next step in understanding employee groups and how they influence the security outcomes for their members and firms.

7 Conclusion

The current study shifts the focus of security incident responses from an individual level to a group level, and by doing this, we see that the success of an organization when responding to an incident depends on its employee groups and the groups' influence on their respective members. From a practice perspective, one important bridge between the two levels appears to be the organizational agent representing the hierarchical structure of an organization *within* the group. With the formal social structure of an employee group having such an impact on its collective ability to respond to a security incident, employees see security as an organizational problem, something that is being pushed on them as opposed to something in which they see themselves having an integral role. For this reason, it is imperative that information security managers understand their organization's employees and the various groups with which they are associated, as well as how these groups interpret security incidents and their organization's expectations regarding employee response.

Although prior research suggests the importance of developing the individual employee, our findings suggest that it takes an employee group—a village—to

be successful when responding to information security incidents. Policies may establish the expectations of incident response behavior among employees, but how these expectations are ultimately fulfilled is determined at both the individual *and* group levels (Baskerville & Siponen, 2002). Employees engage in policy-prescribed incident response behavior based on the individual-level influence of a number of individual-level factors, including policy awareness, deterrence factors, threat and efficacy perceptions, and normative beliefs, among others. However, the incident response success of an organization also depends on the interactive, coordinative, and synergistic capabilities of the organization's employees in the form of employee groups. In many ways, the social fabric of an organization may represent the single greatest asset it has when responding to security incidents. Although the quality of each individual thread (employee) has proven to be an important component to security threat mitigation, interlaced threads (an employee group) may be able to mitigate the weaknesses of a single thread to ensure that the organization responds to security incidents in an appropriate and effective manner.

References

Bandura, A. (2000). Exercise of human agency through collective efficacy. *Current Directions in Psychological Science, 9*(3), 75-78.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5-6), 337-346.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1036.

Bélanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*, 573-578.

Berger, P. L., & Luckmann, T. (1991). *The social construction of reality: A treatise in the sociology of knowledge* (Vol. 10). London: Penguin.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: SAGE.

Browning, C. R. (2002). The span of collective efficacy: Extending social disorganization theory to partner violence. *Journal of Marriage and Family, 64*(4), 833-850.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-A527.

Bygstad, B., & Munkvold, B. E. (2011). Exploring the role of informants in interpretive case study research in IS. *Journal of Information Technology, 26*, 32-45.

Chua, C. E. H., Wareham, J., & Robey, D. (2007). The role of online trading communities in managing Internet auction fraud. *MIS Quarterly, 31*(4), 759-781.

Cole, M., & Avison, D. (2007). The potential of hermeneutics in information systems research. *European Journal of Information Systems, 16*(6), 820-833.

Coleman, J. S. (1988). Social capital in the creation of human capital. *American Journal of Sociology, 94*, 95-120.

Crocker, J., & Luhtanen, R. (1990). Collective self-esteem and ingroup bias. *Journal of Personality and Social Psychology, 58*(1), 60.

Crossler, R., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(February), 90-101.

Drukker, M., Kaplan, C., & van Os, J. (2005). Residential instability in socioeconomically deprived neighborhoods. *Health & Place, 11*(2), 121-129.

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review, 24*(3), 349-375.

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

Ely, R. J., & Thomas, D. A. (2001). Cultural diversity at work: The effects of diversity perspectives on work group processes and outcomes. *Administrative Science Quarterly, 46*(2), 229-273.

Gadamer, H.-G. (1975). *Truth and method* (2nd ed.). New York, NY: Continuum.

Gallagher, S. (Producer). (2015, January 26, 2016). Encryption "would not have helped" at OPM, says DHS official. Retrieved from http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/

Gibbert, M., Ruigrok, W., & Wicki, B. (2008). What passes as a rigorous case study? *Strategic Management Journal, 29*(3), 1465-1474.

Guba, E., & Lincoln, Y. (1989). *Fourth generation evaluation*. Newbury Park, CA: SAGE.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. Thousand Oaks, CA: SAGE.

Guzzo, R. A., & Dickson, M. W. (1996). Teams in organizations: Recent research on performance and effectiveness. *Annual Review of Psychology, 47*(1), 307-338.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, 25*(1), 111-136.

Hubbard, E. E. (2004). *The diversity scorecard: Evaluating the impact of diversity on organizational performance*. Boston, MA: Routledge.

Johnston, A. C., McBride, M., Carter, L., & Warkentin, M. (2016). Dispositional and situational factors: Influences on IS security policy violations. *European Journal of Information Systems, 25*(3), 231-251.

Keutel, M., Michalik, B., & Richter, J. (2014). Towards mindful case study research in IS: A critical analysis of the past ten years. *European Journal of Information Systems, 23*(3), 256-272.

Kingston, B., Huizinga, D., & Elliot, D. S. (2009). A test of social disorganization theory in high-risk urban neighborhoods. *Youth & Society, 41*(1), 53-79.

Kornhauser, R. R. (1978). *Social sources of delinquency: an appraisal of analytic models*. Chicago, IL: University of Chicago Press.

Kubrin, C. E., & Weitzer, R. (2003). New directions in social disorganization theory. *Journal of Research in Crime and Delinquency, 40*(4), 374-402.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*(1), 159-174.

Lesser, E., & Storck, J. (2001). Communities of practice and organizational performance. *IBM Systems Journal, 40*(4), 831-841.

Markowitz, F. E., Bellair, P. E., Liska, A. E., & Jianhong, L. (2001). Extending social disorganization theory: Modeling the relationships between cohesion, disorder, and fear. *Criminology, 39*(2), 293-320.

Mazerolle, L., Wickes, R., & McBroom, J. (2010). Community variations in violence: The role of social ties and collective efficacy in comparative context. *Journal of Research in Crime and Delinquency, 47*(1), 3-30.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2-26.

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of Management Review, 23*(2), 242-266.

Oh, H., Chung, M.-H., & Labianca, G. (2004). Group social capital and group effectiveness: The role of informal socializing ties. *Academy of Management Journal, 47*(6), 860-875.

Paepcke, A. (1996). Information needs in technical work settings and their implications for the design of computer tools. *Computer Supported Cooperative Work, 5*(1), 63-92.

Ronayne, L. S. (2004). *Effects of coaching behaviors on team dynamics: how coaching behaviors influence team cohesion and collective efficacy over the course of a season* (Unpublished master's thesis). Miami University, Oxford, OH.

Sampson, R. J., & Groves, W. B. (1989). Community structure and crime: Testing social-disorganization theory. *American Journal of Sociology, 94*(4), 774-802.

Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and violent crime: A multilevel study of collective efficacy. *Science, 277*(5328), 918-924.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly, 37*(4), iii-viii.

Schlagwein, D., & Bjørn-Andersen, N. (2014). Organizational learning with crowdsourcing: The revelatory case of LEGO. *Journal of the Association for Information Systems, 15*(11), Article 3.

Schulz, A. J., Mentz, G., Lachance, L., Johnson, J., Gains, C., & Isreal, B. A. (2012). Associations between socioeconomic status and allostatic load: Effects of neighborhood poverty and tests of mediating pathways. *American Journal of Public Health, 102*(9), 1706-1714.

Segars, A. H., & Grover, V. (1998). Strategic information systems planning success: An investigation of the construct and its measurement. *MIS Quarterly*, 139-163.

Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas*. Chicago, IL: The University of Chicago Press.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and Practice in Information Systems Security Research. *ICIS 2008 Proceedings*, 26.

Stewart, K. J., & Gosain, S. (2006). The impact of ideology on effectiveness in open source software development teams. *MIS Quarterly*, 291-314.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*, 74-81.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). Then influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Winkleby, M. A., & Cubbin, C. (2003). Influence of individual and neighborhood socioeconomic status on mortality among Black, Mexican-American, and White women and men in the United States. *Journal of Epidemiology and Community Health, 57*(6), 444-452.

Yin, R. K. (2002). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: SAGE.

Yin, R. K. (2010). *Qualitative research from start to finish*. New York, NY: Guilford.

Zahra, S. A. (2007). Contextualizing theory building in entrepreneurship research. *Journal of Business Venturing, 22*(3), 443-452.

Appendix A: SDT Contextualization

We followed the theory contextualization guidelines provided by Hong, Chan, Thong, Chasalow, and Dhillon (2014) to contextualize the applicable ecological and social properties provided by the SDT. Specifically, we heed the advice of Hong et al. (2014) (Guideline 2) to first identify a set of core constructs with which to contextualize our specified research domain. To aid in this effort, we leveraged the extensive and mature SDT literature to provide guidance for which properties would be the most relevant to a new research domain. However, our synthesis of the SDT literature found that researchers present a vast set of properties. A core model appears to be sensitive to the unique contextual elements of each particular study.

Because information systems (IS) and information security scholars have not adopted the SDT as a theoretical lens in prior research, and information security research has primarily focused on the individual level of analysis rather than the group level, we took a conservative approach to the narrowing down of the SDT's properties. We primarily focused on how the properties would translate to an organizational context. To cast this wider net concerning the core constructs, we relied on Kubrin and Wietzer's (2003) review of the SDT literature. We then followed the advice of Hong et al. (2014) and Zahra (2007) to relax the assumptions of the SDT to ensure its properties would fit the new research domain. In doing so, we contribute to the criminology literature in terms of added generalizability by identifying a core set of properties for the SDT in security-based research, identifying potential extensions to the SDT when studied from a new research domain and disciplinary perspective, and establishing the relevance of the SDT to a new discipline.

One key assumption of the SDT is that neighborhoods are social structures defined by geographic boundaries and various macroconditions—such as poverty, ethnic heterogeneity, and residential turnover—that influence and govern social activity within the communities. By relaxing the geographic boundary assumption, we account for how our focal phenomenon involves employee groups that are bound less by physical structures and more by logical and social ones. Employee groups are logically organized and socially constructed as much as they depend on the physical structures imposed by the organization (Berger & Luckmann, 1991). For instance, within a geographically bounded residential community, the SDT defines socioeconomic status as the economic and social position of a community in terms of its residents' education, income, and occupational status (Schulz et al., 2012; Winkleby & Cubbin, 2003). Contextualized to an organizational incident response context, the definition is quite similar, referencing employees instead of residents.

Additionally, the SDT has previously assumed a residential environment. Because membership in employee groups is influenced by more than just physical proximity and is subject to logical roles, administrative hierarchy, and the social structures within the organization, we must consider the social and logical perspectives when mapping the SDT's constructs, associations, values, and events to the collective security efficacy phenomenon. For example, SDT-based research has primarily focused on physical crimes against the community, such as theft, vandalism, and armed robbery, and scholars criticize the SDT for ignoring lesser offenses that may lead to more serious threats if left unchecked. We must also anticipate an organizational environment largely influenced by digital information and communication networks and negligent or malicious actions by employees or those responsible for monitoring security. These are considerations that motivate our contextualization of the SDT to employee groups and their collective security efficacy. The original and contextualized SDT ecological and social properties, along with their respective definitions and rationales for inclusion or contextualization, are included in Table A1.

Table A1. Contextualization of SDT-Espoused Community Properties

SDT-espoused community properties	Contextualized SDT-espoused employee group properties	Rationale for inclusion or contextualization to the organizational context
Ecological properties		
Socioeconomic status: The economic and social position of a community in terms of its residents' education, income, and occupational status (Schulz et al., 2012; Winkleby & Cubbin, 2003).	Socioeconomic status: The economic and social position of an employee group in terms of its members' education, income, and occupational status/rank within the organization.	In the SDT, socioeconomic status (SES) is bounded within the physical geography of a neighborhood and relates to the variation in the community's economic status (e.g., poverty). SES unbinds the physical constraint to a conceptual boundary of an organization and the variation in employee economic status.
Residential instability: The degree of turnover among neighborhood residents (Drukker, Kaplan, & van Os, 2005).	Turnover: The degree to which members of an employee group transfer, resign, retire, or are terminated from their position within the group.	Residential instability is bounded within the physical geography of a neighborhood and is primarily driven by resident choice. Turnover can be driven by organization or employee choice and is not tied to a physical boundary (e.g., transition within organization to new community).
Ethnic heterogeneity: The degree of ancestral, social, cultural, or national diversity among neighborhood residents (Sampson & Groves, 1989).	Diversity: The degree to which a group is comprised of employees that identify with one or more socioecological group (Ely & Thomas, 2001), including professionally affiliated groups, departments, task workgroups, and so forth.	Ethnic heterogeneity focuses on a singular differentiation point when comparing neighborhood residents while diversity is an overall representation of the individual differences within an organizational structure (e.g., gender, ethnicity, cultural affiliation, and sexual orientation).
Social properties		
Social ties: The information-carrying connections among neighborhood residents (Kubrin & Weitzer, 2003; Shaw & McKay, 1942).	Social ties: The social channels that facilitate the exchange of resources among the employees within a group (Oh, Chung, & Labianca, 2004).	The concept of social ties maintains a common meaning in both neighborhood and organizational settings.
Social capital: The intangible resources produced in "relations among neighborhood residents that facilitate action" for mutual benefit (Coleman, 1988; Kubrin & Weitzer, 2003, p. 377).	Social capital: The intangible resources produced via relationships among employees that facilitate action for the mutual benefit of the group (Coleman, 1988) in terms of structural, relational, and cognitive capital (Nahapiet & Ghoshal, 1998).	The SDT literature has various definitions of social capital. In an organization, social capital aligns with a definition that focuses on mutual benefits achieved through the relationships among employees.
Cohesion: The degree to which neighborhood residents work together as a united entity (Markowitz et al., 2001).	Cohesion: The degree to which members of an employee group work together as a united entity against disruptive forces (Markowitz et al., 2001; Ronayne, 2004).	Cohesion in the SDT refers to close-knit ties of neighbors within a geographically bounded location. Cohesion in organizations focuses on the perceptions of closeness in terms of harmony and trust among employees.

Table A1. Contextualization of SDT-Espoused Community Properties

Cultural attenuation: The degree to which the conventional values of a neighborhood are valued by its residents and are able to impose informal social control (Kornhauser, 1978).	Cultural attenuation: The extent to which normative conventions can be interpreted correctly and influence employee behavior within an employee group.	Cultural influence in the SDT has two approaches: (1) cultural heterogeneity (divergent value systems), and (2) cultural attenuation (ability of conventional values to provide informal social control).
Social control: The societal or political influences that shape and govern the behavior of neighborhood residents (Kubrin & Weitzer, 2003). There are two types of social control: 1. Formal social control: The practices of the authorities to maintain order and enforce legal and regulatory codes. 2. Informal Social Control: The degree to which neighborhood residents engage in efforts to prevent or sanction disorderly or criminal conduct through informal surveillance and direct intervention.	Social control: The societal or political influences that shape and govern the behavior of employee group members. There are two types of social control: 1. Formal social control: The practices of an employee group's leaders to maintain order and enforce legal and regulatory codes. 2. Informal social control: The degree to which members of an employee group engage in efforts to prevent or sanction disorderly or criminal conduct through informal surveillance and direct intervention in problems.	Social control in the SDT focuses on informal control mechanisms through alignment with cultural norms. Social control in organizations can be determined by top-down enforcement (formal control) and peer enforcement (informal control).

Appendix B: Interview Protocol

Unless noted otherwise, the interviewee gave the italicized examples when prompted for further clarification.

Demographics:

1. Please state your gender.
2. Please state your level of education.
3. Please state your tenure with your employer.
4. Please state your race.

Study Summary Statement:

The current study focuses on the collective security efficacy of employee groups (the ability of an employee group to adequately manage a security issue when present). An employee group can be defined as collections of individuals who "are interdependent because of the tasks they perform as members of a group, who are embedded in one or more larger social systems (e.g. community, organization), and who perform tasks that affect others (such as customers or coworkers)" (Guzzo & Dickson, 1996, p. 308). As such, an employee group can be interpreted widely, so we would like you to first describe your employee group.

Theme Questions:

1. Are your fellow group members compensated at a rate that is better than, consistent with, or less than what other organizations would pay for this amount and quality of work?
    a. How does variation in pay level influence security actions within the group?
2. How does the variance in employee education levels influence the security actions within your group?
3. How does the diversity of job roles (managerial, professional, administrative, skilled, semiskilled, and unskilled) influence the security actions within your group?
4. How does your group's governance structure (centralized, decentralized, and hybrid) influence the security actions within the group?
5. How would you describe the social involvement of your group's members? *(e.g., group lunch meetings, cocktails after work, social clubs / sports, etc.)*
6. How do the social ties within your group influence the security actions within the group?
    a. How do social groups and leaders influence security actions within the group?
    b. How does harmony in the group influence the security actions within the group? *(e.g., groups generally agree with each other)*
    c. How does benevolence influence the security actions within the group? *(e.g., show compassion or empathy toward others)*
    d. How does integrity influence the security actions within the group? *(e.g., honest or truthful with one another in sharing information)*
7. How do the combined abilities of the members of your group influence the security actions within the group?
8. How does your group support its members in accomplishing security actions?
    a. How does cohesion influence the security actions within the group?
9. How does your group encourage its employees to work together to accomplish security goals?
10. How are security policies interpreted within your group?
11. How would you describe the quality of the communication of security policies within your group?
12. How does your group make accessible to you the knowledge about security issues, incidents, and policies?
13. How does synthesized knowledge of security issues, incidents, and policies influence the security actions within your group? (Question added based on the emergence of organizational memory.)

a. How does organizational memory influence the security actions within the group? (Question added based on the emergence of organizational memory.) *(e.g., learning management systems, policy databases, document repositories, etc.)*

b. How does monitoring (such as tracking web usage, access to physical resources, etc.) influence the security actions within the group?

c. How does the use of metaphors and heuristics influence the security actions within the group? *(e.g., storytelling by employees, rules of thumb, etc.)*

14. How do your peers influence the security actions within your group?

15. What factors do you perceive to have the greatest influence on the security actions within your group?

About the Authors

Allen C. Johnston is an associate professor of management information systems and the management information systems graduate programs coordinator in the Department of Information Systems, Statistics, and Management Science in the Culverhouse College of Business at the University of Alabama. The primary focus of his research is in the areas of behavioral information security, privacy, data loss prevention, collective security, and innovation. His research can be found in such outlets as *MIS Quarterly*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Communications of the ACM*, *Journal of Organizational and End User Computing*, *Information Technology and People*, and *DATABASE for Advances in Information Systems*. He currently serves as an associate editor for the *European Journal of Information Systems* and for *Decision Sciences Journal*, and also serves on the editorial review board for the *Journal of the Association for Information Systems*. He is a founding member and current chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).

Paul M. Di Gangi is an associate professor and graduate program director for management information systems in the Collat School of Business at the University of Alabama at Birmingham. In 2017, Dr. Di Gangi was named Steward of the Dora and Sanjay Singh Endowed Research Fund for Information Systems. His research examines the intersection of digital networks and organizations with a focus in three areas: (1) the influence of social networks on behavioral information/cybersecurity, (2) role of online communities in business, and (3) user-driven innovation processes/ crowdsourcing. His research has been published or is forthcoming in the *Journal of the Association for Information Systems*, *Communications of the Association for Information Systems, Decision Support Systems, Information & Organization, Information Systems Frontiers*, and *MIS Quarterly Executive*, among others. Dr. Di Gangi is also a certified information systems security professional (CISSP) based on his work in public administration relating to policy, strategic planning, and risk analysis.

Jack Howard is the interim chair and professor of management in the Collat School of Business at the University of Alabama at Birmingham. He received his PhD in human resource management from the University of Illinois at Urbana-Champaign. His research focuses on organizational behavior and human resource management. He has published more than 25 research papers in academic journals, including *Human Relations, Journal of Applied Social Psychology,* and the *Academy of Management Journal*.

James L. "Jamey" Worrell is an associate professor of accounting in the Collat School of Business at the University of Alabama at Birmingham. His research examines the intersection of accounting and information systems, focusing primarily on information technology governance and risk management. His research has been published or is forthcoming in the *Journal of the Association for Information Systems, Information Technology & People, Information Systems Frontiers*, and *International Journal of Accounting Information Systems*, among others. Dr. Worrell is a certified public accountant (CPA), certified information systems auditor (CISA) and certified internal auditor (CIA).