http://pubsonline.informs.org/journal/isre

INFORMATION SYSTEMS RESEARCH
Articles in Advance, pp. 1–20
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context

Sumantra Sarkar,[a] Anthony Vance,[b] Balasubramaniam Ramesh,[c] Menelaos Demestihas,[d] Daniel Thomas Wu[e]

[a] School of Management, Binghamton University, State University of New York, Binghamton, New York 13902; [b] Fox School of Business, Temple University, Philadelphia, Pennsylvania 19122; [c] Robinson College of Business, Georgia State University, Atlanta, Georgia 30303; [d] Wellstar Kennestone Hospital, Marietta, Georgia 30060; [e] Emergency Medicine, Emory University Hospital, Emory University School of Medicine, Atlanta, Georgia 30303

Contact: ssarkar@binghamton.edu (SS); anthony@vance.name, https://orcid.org/0000-0002-4554-6176 (AV); bramesh@gsu.edu (BR); menelaos4@gmail.com (MD); dtwu@emory.edu (DTW)

Received: December 22, 2017
Revised: December 4, 2018; July 25, 2019; April 20, 2020
Accepted: April 29, 2020
Published Online in Articles in Advance: September 17, 2020

https://doi.org/10.1287/isre.2020.0941

Abstract. In recent years, we have witnessed substantial increases in the frequency, scope, and cost of data breaches. Accordingly, information security researchers have sought to understand why employees comply with or violate information security policies (ISPs) designed to prevent security incidents. Research suggests that compliance is not uniform but rather depends on contextual and individual factors, such as national culture. Scholars have long recognized that organizational subculture may be equally influential. A key example is professional subcultures, within which members typically share similar education, training, values, and identity. Research shows that behavior can vary widely across professional subcultures, and thus a single approach to promoting ISP compliance may not be equally effective across these subcultures. However, it is presently unclear how subculture influences ISP compliance. To address this need, we adopt a mixed-methods design to examine differences in ISP violation behavior among different professional subcultures in a healthcare organization. We first conducted an exploratory qualitative study to identify different attitudes toward ISP violations among three prominent professional healthcare groups: physicians, nurses, and support staff. Then, using a combination of qualitative interviews, observational fieldwork, and a quantitative survey, we explored how professional group membership moderates (1) the influence of perceptions of sanctions on intentions to violate the ISP and (2) the effect of intentions to violate on actual ISP violation behaviors. Our findings highlight the substantial effect of professional subculture on ISP violations in organizations and provide insights for researchers and managers that may be used to improve overall ISP compliance.

History: Alessandro Acquisti, Senior Editor; Gordon Burtsch, Associate Editor.
Supplemental Material: The online appendices are available at https://doi.org/10.1287/isre.2020.0941.

Keywords: professional subculture • information security policy violations • mixed methods • healthcare

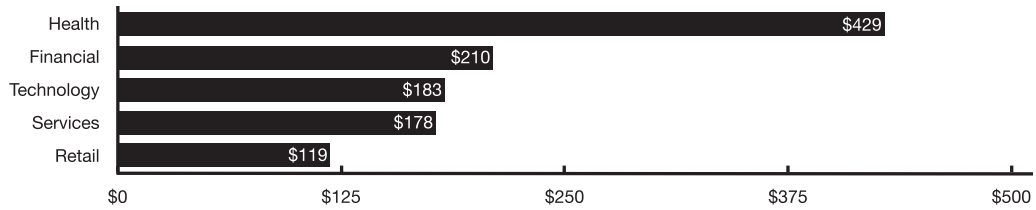
1. Introduction

In recent years, the frequency of data breaches has increased tenfold from 2005–2017 (Identity Theft Resource Center 2018); the cost of data breaches has likewise risen, with an average incident cost of $8.19 million in the United States (IBM 2019). This is especially true of the healthcare industry, which has experienced increased numbers of personal health information (PHI) breaches (Kwon and Johnson 2018; U.S. Department of Health and Human Services 2020, Sarkar et al. 2020). Further, among all industries, the cost of data breaches is by far the highest in healthcare: the per capita cost is over twice that of the next highest industry (Figure 1).

Importantly, an analysis of U.S. healthcare breaches from 2009–2017 shows that 53% were due to actions, intentional or otherwise, of healthcare employees (Bai et al. 2017), underscoring the critical role of human behavior in information security (Chatterjee et al. 2019). As a case in point, in 2015, Anthem Inc. suffered a breach affecting 79 million people, the largest PHI breach to date. This resulted in a $115 million class action settlement in 2017 (Pierson 2017) and a fine of $16 million in 2018 for violating the Health Insurance Portability and Accountability Act (HIPAA) (U.S. Department of Health and Human Services 2018a), both the largest of their kind. Highlighting people as the weakest link in the security chain, the Anthem breach was initiated through a spear phishing attack in which "at least one employee responded to the malicious email and opened the door to further attacks" (U.S. Department of Health and Human Services 2018a, p. 1).

Against this backdrop, information systems (IS) researchers have studied ways to reduce employees' violation of information security policies (ISPs) designed

Figure 1. Per Capita Cost of a Data Breach by Industry Sector (IBM 2019)



to prevent security incidents. One of the primary techniques investigated is sanctions used to deter employees from violating ISPs (Straub 1990, D'Arcy et al. 2009, Cram et al. 2017). However, research suggests that the effect of sanctions on employees' compliance is not always uniform but rather depends on contextual and individual factors (D'Arcy and Herath 2011). For example, national culture has been found to significantly influence the efficacy of sanctions (Hovav and D'Arcy 2012, Cram et al. 2019, Vance et al. 2020). Organizational scholars have long recognized another aspect of culture that may similarly affect employee behavior—professional subculture, in which individuals share similar education, training, values, and identity (West et al. 2014).

Professional subcultures are especially salient in the healthcare industry, which is differentiated along clear professional lines (Scott et al. 2003b) and includes multiple distinct professional groups, such as physicians, nurses, and support staff (Hall 2005). These professional groups exhibit wide differences in rule compliance (Erasmus et al. 2010) and use of technology, such as electronic health record (EHR) systems (Callen et al. 2009). Compliance with ISPs is particularly important in healthcare because inappropriately handling even a single PHI record can result in a fine of between $100 and $50,000 depending on the type of violation and past history of offenses (Health and Human Services 2018b). It is therefore crucial that all employees with access to PHI comply with established ISPs, regardless of their professional subculture.

To address this need, this study aims to investigate how ISP violation behaviors vary by professional subculture in a healthcare organization. Additionally, because sanctions are often explored in the ISP literature and known to influence such behavior (Cram et al. 2019), our investigation includes how professional subculture influences perceptions of sanctions for ISP violations. Further, a focus on sanctions makes sense for the context of this study because sanctions are particularly salient in healthcare. For example, HIPAA expressly requires that healthcare institutions apply sanctions to all organizational members who violate ISPs, and healthcare institutions have been fined between $125,000 and $2,000,000 for failing to do so (Mountenay and Brady 2019).

We pursued this research objective using a three-phase, mixed-methods design, which is useful "to holistically explain a phenomenon" (Venkatesh et al. 2016, p. 437). In Phase 1, because the influence of professional subcultures on sanctions in the ISP context has not been previously explored, we performed a qualitative exploratory case study (Sarker et al. 2018a) to examine the following research question:

Research Question 1. *What dimensions of professional subculture explain differences in perceptions of sanctions and ISP violation behaviors across professional groups?*

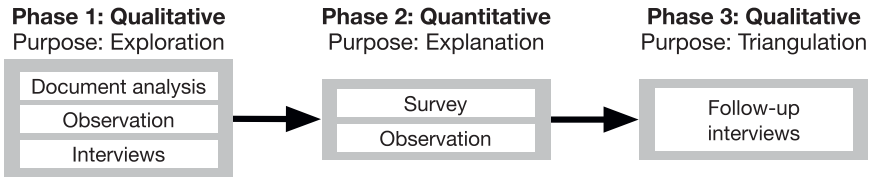
We conducted document analysis, observation, and interviews (Figure 2) with three professional groups with distinct subcultures: physicians, nurses, and support staff. We used this exploratory case study "to interpretively discern the key context-related constructs" to support later quantitative investigation (Sarker et al. 2018, p. 105). In doing so, we identified three dimensions of professional subculture—power, prestige, and multitasking—that explain differences in perceptions of sanctions and ISP violation behaviors across professional groups.

In Phase 2, we conducted an explanatory quantitative study to examine the following questions:

Research Question 2. *How does professional subculture moderate the influence of perceptions of sanctions on intention to violate the ISP?*

Research Question 3. *How does professional subculture moderate the influence of intention to violate the ISP on actual ISP violation behaviors?*

Figure 2. The Three-Phase Mixed-Method Research Design



To do this, we surveyed physicians, nurses, and support staff to test the moderating influence of professional group membership within the nomology of the Extended General Deterrence Theory (EGDT) developed by D'Arcy et al. (2009), an established model in the ISP literature. In addition to measuring intention to violate using the survey, we used observation to record actual ISP violation behaviors.

Finally, in Phase 3, we conducted additional qualitative interviews after the survey to triangulate the quantitative findings of the survey with qualitative insights from the interviews (Bryman 2006). As Jick (1979, p. 603) notes, when using multiple methods to build a more holistic picture, "qualitative methods, in particular, can play an especially prominent role by eliciting data and suggesting conclusions to which other methods would be blind. Elements of the context are illuminated." Together, this three-phase, mixed-method approach provides valuable meta-inferences and a more holistic understanding than could be provided by a single method.

Our findings provide a number of contributions. First, we found an undeclared informal hierarchy across the professional subcultures of physicians, nurses, and support staff, each of which exhibited different ISP violation behaviors, attributable to differences in power, prestige, and multitasking dimensions. Second, our results show that, like national culture, professional subculture moderates the relationship between perceptions of sanctions and intentions to violate the ISP. This study therefore reveals another contextual difference that helps explain the mixed findings of prior research on sanctions in the ISP context (D'Arcy and Herath 2011, Cram et al. 2019). Moreover, we found that subculture also moderates the relationship between intention and actual ISP violation behavior. Third, from a methodological perspective, this study combined qualitative and quantitative methods to provide a more complete view of the influence of professional subculture on actual ISP violation behavior.

Finally, our findings offer a more nuanced understanding of the ISP violation concept by highlighting pseudocompliance, a behavior that appears on the surface to be compliant but in reality is an ISP violation and is thus doubly harmful for noncompliance and for engendering a false sense of security. Interestingly, engaging in pseudocompliance behavior also varied by professional subculture. Our qualitative interviews revealed that this superficial compliance was largely due to goal conflict (DiBenigno 2018); employees were motivated by a desire to comply with the ISP at least in part, tempered by an unwillingness to spend the time and effort required for full compliance at the expense of patient care. This suggests the need for organizations to tailor ISPs to better align with the goals and workflows of specific groups of employees (Adams and Sasse 1999). Together, these contributions reveal the considerable impact of professional subculture on perceptions of sanctions and violation behaviors in the ISP context.

The remainder of this paper is organized as follows. We first review background literature on violation sanctions and professional subculture. We then introduce our mixed-method design and investigation of each phase. Finally, we discuss our results, contributions, limitations, and avenues for future research.

2. Literature Review

2.1. Deterrence Theory and Culture

Deterrence theory, which has its roots in the Enlightenment thinking of Cesare Beccaria (1738–1794) and Jeremy Bentham (1748–1832), is one of the oldest theories in criminology and one of the most widely applied theories in the area of ISP compliance (Cram et al. 2017). It explains that individuals' willingness to break a rule is a function of their perceptions of the severity of related punishments or sanctions and the certainty that they will receive those sanctions. However, previous research suggests that perceptions and effectiveness of sanctions differ by culture (D'Arcy and Herath 2011, Cram et al. 2019). For example, Hovav and D'Arcy (2012) found that national culture influenced perceptions of certainty and severity of sanctions. Because professional subculture is known to influence perceptions (Lok et al. 2005), it is likely that professional subculture also influences perceptions of sanctions.

2.2. Professional Subculture

Too often, "organizational culture is treated as a monolithic phenomenon—one culture to a setting" (Martin and Siehl 1983, p. 53). In reality, any organization's culture comprises a collection of subcultures (Hofstede 1998). Professional subcultures arise through the socialization of new members:

> If an occupation involves an intense period of education and apprenticeship, there will certainly be a shared learning of attitudes, norms, and values that eventually will become taken-for-granted assumptions for the members of those occupations. It is assumed that the beliefs and values learned during this time will remain stable as assumptions even though the person may not always be in a group of occupational peers. (Schein 2010, p. 20)

Although all employees may understand what an organization's strategic objectives are, employees in various professional subcultures can interpret them differently (Huang et al. 2003). Therefore, the implementation of organizational strategies through policies may not have the same desired effect on all professional subcultures in an organization (Martin and Siehl 1983).

Further, professional subcultures may not be aligned with the overall organizational culture and policies, and any misalignment may result in conflicts (Robey and Azevedo 1994, Huang et al. 2003). Also, professional subcultures can be stronger than a given organizational culture, in which case, the professional subculture will influence employee attitudes and behaviors more than the overarching organizational culture (Harris and Ogbonna 1998).

In the field of IS, research has documented the substantial influence of professional subcultures on implementation of new systems, conflicts over technology innovation (von Meier 1999), team coordination (Huang et al. 2003), and system requirements gathering (Tuunanen and Kuo 2015), to name a few examples. In the area of information security, although it is recognized that the culture of an organization has a significant influence on whether employees comply with or violate ISPs (Vroom and von Solms 2004), no study has examined the effect of professional subculture on ISP violation behavior. Thus, although the management and IS literature show the substantial effects of professional subculture, its effects on ISP violation remain unknown.

2.3. Professional Subcultures in Healthcare

The existence of professional subcultures in healthcare is clear. Scott et al. (2003a, p. 25) observed that "a key characteristic of health care organizations is the range of distinctive and vivid occupational subcultures which provide the 'raw' material for its organizational culture." The professionalization and enculturation of healthcare workers

> takes place over long periods of time as a result of occupational groups … that enjoy status and recognition from the general public and governments. Members of such professions tend to share not only similar training and knowledge, but also schemas for the way they interpret their professional encounters, the technologies they employ, individuals they interact with (e.g., patients and other professions) and the organizations of which they are a part. By developing basic values, beliefs, shared understanding, and identity within a profession, a professional (sub) culture is developed. Such groups can accumulate power in organizations and accrete considerable decision-making influence. (West et al. 2014, p. 349)

Within a hospital, members of various professional subcultures inherit different values, attitudes, and expectations from their "professionalization" processes (Haas and Shaffir 1977). The culture they bring from their professional training is rarely replaced by the organizational culture (Bloor and Dawson 1994), and this may lead to conflicts and differences in following organizational guidelines (Gershon et al. 1995).

We argue that a study of the influence of professional subculture on ISP violation is especially appropriate in the healthcare context for two reasons. First, because patient data are increasingly vulnerable to theft and misuse because of the accessibility of electronic health information, healthcare is a highly regulated industry with a strong emphasis on information security and compliance (Angst and Agarwal 2009). Second, because professional subcultures in healthcare are so salient, the influence of professional subculture on ISP violation, if such an interaction exists, is likely to be observable. However, to our knowledge to date, no research has examined the role of professional subculture in the ISP compliance context, such as how professional subculture influences perceptions of sanctions and subsequent ISP violations. Motivated by this gap in the literature, we designed a mixed-methods study to explore these relationships.

3. Mixed-Methods Design

Mixed-methods designs have advantages for studying complex organizational and social phenomena because different methods used within a single study complement each other in data collection and analysis (Cao et al. 2006, Venkatesh et al. 2013). Further, multiple methods enrich results and make them more reliable compared with those obtained from a single method (Mingers 2001, Vance et al. 2018). In addition, mixed methods can provide meta-inferences that integrate findings across individual methods. However, despite its advantages, few IS researchers have embraced this approach (Venkatesh et al. 2013). A further explanation of our mixed-method design is provided in Online Appendix A. Details of meta-inferences drawn from the study are given in Online Appendix B.

3.1. Research Site and Background

Our study was part of a broader research program aiming to develop a deeper understanding of the way EHRs are used in hospitals. In this research program, which lasted for more than two years, one of the researchers was embedded in a premier 950+ bed hospital located in the Southeastern United States to observe informants, conduct interviews, and analyze documents as part of data collection. This hospital recently implemented one of the largest EHR systems in the world, at an implementation cost of ~$40 million. The study was conducted in the emergency department (ED), an urban Level 1 trauma center. The ED receives nearly 120,000 patients per year and employs nearly 120 emergency attending physicians, 50 resident physicians, 150 nurses, and more than 100 support staff. All healthcare professionals at the hospital use the EHR system.

To enable gathering of reliable data, we designed several strategies. First, the chief medical information officer (CMIO) of the hospital agreed to sponsor the research and serve as the primary contact. Based on discussions with the CMIO and other senior executives, a strategy was developed to fully integrate the primary researcher as a member of the organization so that data collection was seamless (Schouten and McAlexander 1995). The CMIO informed all staff members of the goals of the broader research program and noted that the researcher would be observing their work and interviewing them over an extended period of time. The researcher received a special identification card granting access to all departments in the institution. The primary researcher was required to complete regular employee training on the EHR system, ISPs, HIPAA, and ethical employee conduct and was invited to participate in EHR optimization project meetings.

4. Phase 1: Qualitative Study—Purpose: Exploration

4.1. Information Security Policy Review

As depicted in Figure 2, we initially studied the organization's 51 ISPs to obtain a comprehensive understanding of required security practices. Strong ISPs were prescribed to protect patient data per HIPAA guidelines. Further, all employees of the organization were made aware of the ISPs, which were documented on the organization's intranet. Employees were required to attend a security awareness training upon hiring and to attend annual awareness trainings thereafter. Employees were also made aware of sanctions for violating ISPs, ranging from written warnings, monetary penalties, termination, and even to criminal investigation and prosecution.

4.2. Observation

Because actual behavior can deviate substantially from what is prescribed by the ISP or even from what employees say they intend or do (Vance et al. 2014, Cram et al. 2019), we determined to observe the level of actual compliance with ISPs. To do so, we required an ISP that was directly observable, yet was nonintrusive to observe so that we would not interfere with the critical work of the emergency department. We selected an ISP for the EHR system that required that users enable the lock screen of their workstation whenever they left their workstation unattended (see Table 1). The choice of this ISP was appropriate given that its violation represented a breach of HIPAA and thus posed serious risks to the organization, as described previously. In effect, this ISP served as a proxy for all of the other ISPs of the organization.

While observing informants, the researcher maintained the role of a "neutral observer," without "strong prior views of specific people, systems or processes based on previous work in the organization" (Walsham 2006, p. 321). Observations were made "at a distance" (Chisholm et al. 2000, p. 1240) of 2–3 meters to collect data in a natural setting and elicit less self-conscious responses from the informants (Barley 1990). Moreover, most informants were accustomed to having researchers at the site collecting data, implying that the influence of social desirability on collected data were minimal. On most days, at least two or three research teams were collecting data at the hospital.

Healthcare professionals updated the EHR from one of multiple computers at a C-shaped table in the center of the ED. The researcher was stationed here for observations, interviews, and, later, distribution of surveys. Healthcare professionals were observed individually through the full process of updating the EHR when caring for a particular patient; it was frequently observed that these professionals did not complete the patient documentation in the EHR in a single sitting. Often, they would start entering data, leave the desk to perform other tasks, and return later to finish updating the EHR record (in one or more subsequent sittings). Additionally, it was observed that healthcare professionals frequently did not log out of the EHR or lock the screen when they left the workstation unattended.

Data were analyzed and the following patterns were observed: users would (a) lock the workstation when they left it unattended and unlock the workstation to continue data entry after they returned; (b) leave the screen as it was and continue the data entry from where they left off when they returned; or (c) minimize the EHR application screen when they left and continue the data entry after maximizing the screen when they returned. The ISP stipulated locking the screen when leaving the workstation unattended (e.g., behavior (a) above). Behaviors (b) and (c) were in violation of the ISP. Although behavior (b) is an obvious violation, behavior (c)—minimizing the EHR application screen upon leaving the computer—is an example of a type of ISP violation we term "pseudocompliance." This intentional behavior gives the appearance of compliance but is actually in violation of the ISP and provides no real security benefit. Pseudocompliance is dangerous because it lulls actors and observers into a false sense of security.

In all, we observed 28 medical professionals who were purposefully sampled to allow us to better investigate the "unique contexts" of the environment of our study (Miles et al. 2014). For example, we ensured that those observed belonged to different professional groups to gain a holistic understanding of actual ISP compliance practices. These groups included physicians, nurses, and support staff. Interestingly, we observed that these three groups exhibited different patterns of compliance, with physicians being generally

Table 1. Observations that Violate ISPs and Suggested Constructs

ISP artifact	Observation	Constructs suggested
"Users must lock their workstations when leaving it unattended. This may quickly be done by pressing the Windows key (⊞) and 'L' key simultaneously."	Users do not lock the EHR screen when they leave the workstation	Violation behavior
	Users will minimize the screen such that the EHR window is not visible on the screen	Pseudocompliance behavior

the least compliant. However, there were also differences within professional groups suggesting that informants' violation of the ISP was more nuanced than a division of groups alone.

4.3. Interviews

To better understand the reasons behind the observed ISP violations, we conducted semistructured interviews with the 28 informants previously observed (Myers and Newman 2007). Some informants were interviewed multiple times for clarification and to gain additional insights. Narratives from different informants were compared against each other and were validated by two physicians on the research team. Our analysis of the qualitative data were guided by principles laid out by Klein and Myers (1999) and Walsham (Walsham 1995, 2006). For data analysis, we followed the guidelines of the less-procedural versions of the grounded theory method (Strauss and Corbin 1994, Bryant and Charmaz 2007) as used by IS scholars previously (Boudreau and Robey 2005, Sarker and Sarker 2009, Seidel et al. 2013). Data from interview transcripts, observational field notes, and documents were first categorized using initial coding, followed by axial and selective coding (Corbin and Strauss 2015). Key codes, categories, and themes were identified through this analysis process, which continued until reaching theoretical saturation (Charmaz 2006). Details of the coding process are given in Online Appendix C.

Analysis of the data provided interesting insights. First, we learned that leaving EHR data entry midtask was due to the nature of the work, such as a nurse needing clarification from a physician or the arrival of a higher acuity patient requiring immediate attention. Second, although informants expressed vague general recall of ISPs (Siponen and Vance 2014), all interviewees understood the requirement to lock the EHR when leaving the workstation. Third, and most importantly, the reasons for leaving the EHR workstation unlocked varied among distinct professional groups—physicians, nurses, and support staff. These groups also exhibited differences in their perceptions of sanctions for violating ISP and their intentions to do so, even though the ISP was mandatory for all members of the organization.

These differences in perceptions, intentions, and behaviors indicated different subcultures for the professional groups. This finding is consistent with past literature that found distinct professional subcultures within organizations (Bloor and Dawson 1994) with different perceptions and behavior with regard to organizational norms (Lok et al. 2005). As these insights emerged, the objective of the exploratory study evolved from studying mere ISP compliance to examining dimensions of professional subculture that explained differences in perceptions of sanctions and ISP violation behaviors observed across professional groups.

4.4. Subculture Dimensions

Our analysis of the observational and interview data identified three salient dimensions that explained the differences in perceptions and behaviors among the professional subcultures—power hierarchy, occupational prestige, and multitasking. *Power hierarchy* describes differences in power among employees according to the positions they occupy in the organization (Fagenson 1990). Although the organization did not have any formal reporting structure, an informal power hierarchy existed in the organization. For example, though not practiced often, we observed that physicians had the power to influence nurse schedules to exclude a particular nurse from their shift. Acknowledging this, one nurse observed that "*physicians are very powerful here*." In one observed interaction between a physician and a nurse, the nurse suggested an alternative way of intubating a patient but was sharply interrupted by the physician: "*This is how I am going to do it. Please do not disturb me.*" In turn, the nurses displayed a commanding tone while interacting with support staff. For instance, one nurse demanded of a support staff member, "*Why haven't the vitals been taken every 20 minutes as I had asked you to?*"

Occupational prestige refers to the degree of social honor attached to a particular occupation (Klein 2016). For example, although there were no written rules about priority of computer use in common areas for updating EHRs, a nurse might log out an idle support staff session to update a patient record but not an idle physician session. We interpret this as a practice of respect for the occupational prestige of the physician. Also, although there was no protocol attached to who would respond to a walkie-talkie message from a helicopter with advance information of a high-acuity incoming patient, the nurses and support

staff would let the physician respond to the message out of respect for the physician. Each professional group was acutely aware of their relative occupational prestige, and instances occurred in which someone would refuse to do something because they viewed the task as beneath the prestige of their occupation. A physician reminisced how the prestige of the physician profession was her childhood dream: "*Putting on this white coat has been my dream. This gives me an identity . . . a significance.*" A senior nurse who has been in the field for more than 20 years complained that the new physician graduates were not willing to learn anything from her because "*it is below their prestige to learn the art of not hurting a patient* [with a syringe] *from a nurse.*" Similarly, a support staff member complained, "*There is a shortage of support personnel today and I needed help. The nurse refused to help me in that critical period since it would be below her paygrade.*"

The last concept that emerged from the data were multitasking, which refers to "situations where individuals are asked to shift their attention between several independent, but concurrent, tasks" (Mattarelli et al. 2015, p. 7). The work environment in an emergency department requires participants to multitask because of the large number of patients under their care as well as the number of distributed tasks across various members of the care team. Each professional group practiced multitasking to different degrees. For example, a physician explained doing multiple things at the same time: "*At some point of time I am attending 4–5 high acuity patients at the same time.*" This problem is more acute for physicians in teaching hospitals (such as the one in our study), where the attending physician is also responsible for the residents and medical students. In addition to working with nurses and other physicians in the ED, physicians also need to collaborate with consulting physicians from various other disciplines because of the wide variety of illnesses that are treated in EDs (Laxmisan et al. 2007).

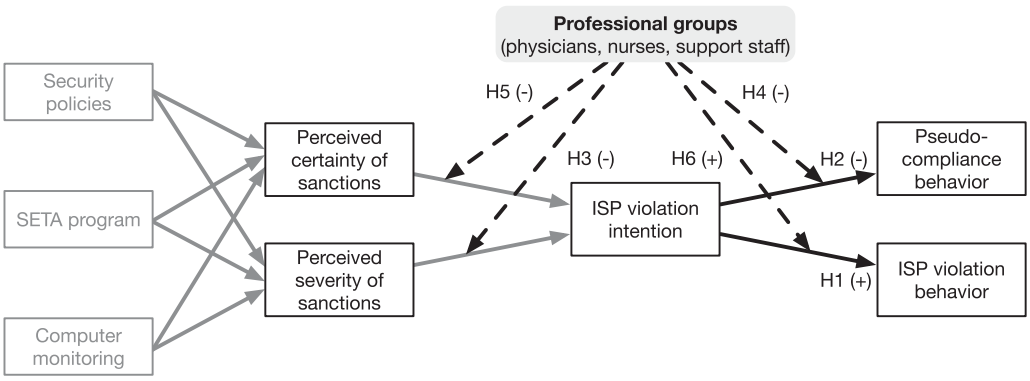
In contrast, members of support staff were often focused on finishing a given task before engaging with other tasks: "*I like to do my work one thing at a time. If I am taking vitals of a patient, I would concentrate on that. I am amazed to see how these physicians manage it* [multiple activities together]." The nurses were somewhere in between in their approach. A nurse explained, "*Our patient load is lower than an attending* [physician's] *at any point of time.*" Another nurse added, "*I assign myself four to five patients on an average since that is what I can manage. I think the physicians manage more than ten.*" Similar phenomena have been reported in past literature (Schneider et al. 2003).

5. Theoretical Framework and Hypotheses

We examined the influence of professional subcultures on ISP violations in the context of the Extended General Deterrence Theory developed by D'Arcy et al. (2009), as depicted in Figure 3. For the sake of brevity, we only hypothesize the new paths in the model but we include all the paths established by D'Arcy et al. (2009) for nomological validity (Straub et al. 2004). We chose this model because it is well established in the ISP literature and because it explains how perceptions of sanctions influence ISP violations. It thus provides a nomology in which to highlight the effect of professional subculture on perceptions of sanctions and ISP violation behavior.

We extend EGDT in three ways. First, whereas the original includes "intention" as the dependent variable, we add "ISP violation behavior" to the model. This is consistent with the call by D'Arcy et al. (2009, p. 94). for extensions that reexamine the model "in a context where actual IS misuse can be measured to add additional credibility to the model." Second, we include another behavioral construct, pseudocompliance behavior, as defined previously. Third, and most importantly, we introduce professional subcultures,

Figure 3. Research Model



Note. Bolded arrows show effects tested in this study.

specifically examining differences among groups of physicians, nurses, and support staff.

5.1. Hypotheses

5.1.1. The Influence of Intention on Violation Behavior.

In this research, we define "the extent of ISP violation behavior" (EXTENT) as a dependent variable to capture not only violations of ISPs but also the extent of the violation. The longer a workstation is unlocked, the greater the level of exposure, providing greater opportunity for unauthorized access to patient records. It is also a reflection on the employee's attitude toward leaving the workstation unlocked, as those who are concerned about leaving the terminal unlocked will try to minimize their time away compared with those who don't care. This conceptualization allows us to distinguish the extent of violations in terms of potential severity.

It is well established that intention leads to behavior (Ajzen 1985). Although some researchers have questioned the validity of the causality of the relationship between intention and behavior (Bagozzi 2007), recent work by Boss et al. (2015) shows that intention leads to behavior, specifically in the context of security intentions and behaviors. Therefore, we hypothesize the following:

Hypothesis 1. *Intention to violate ISP is positively associated with ISP violation behavior.*

5.1.2. The Influence of Intention on Pseudocompliance Behavior.

Pseudocompliance behavior, as defined earlier, is a behavior that appears on the surface to be compliant but is in reality an intentional ISP violation. As a classic example, an employee could create a password that technically complies with a password ISP (e.g., regularly changing a password, creating a complex password, etc.) but then write down the password and store it in an insecure place (such as under a keyboard) (Siponen et al. 2020). Although this may superficially appear to be compliant, he or she is actually undermining the efficacy of the ISP out of expedience. In an example of a physical ISP, employees might appear to keep a door to a secure area (e.g., data center) always closed, but in actuality keep the door slightly ajar using a wedge. Again, the behavior looks compliant but in fact is an intentional violation.

Some of these violations may occasionally be due to thoughtlessness or ineptitude (Willison and Warkentin 2013), but they become pseudocompliance when they are intentional and routine. In this sense, pseudocompliance is conceptually similar to workarounds, in which workers obviate established practices or policies that represent "obstacles to doing work in a preferred manner and misalignment of goals and incentives of actors, principals, and other stakeholders (Alter 2014, p. 1043). Other common examples of this behavior include (1) intentionally sending sensitive data in encrypted form via email but later sending the decrypting password in clear text in a subsequent email out of convenience (Schofield 2018); (2) redacting content from a confidential document by covering text with black boxes but intentionally not applying the extra effort to remove the underlying text and metadata from the document (Franceschi-Bicchierai 2019); (3) or locking a mobile device with a passcode but intentionally choosing a weak passcode (e.g., "1234"). All these examples share a same common thread: they superficially appear to be in compliance with an ISP but upon closer scrutiny are shown to be violations. Finally, employees may not always be trying to fool an onlooker into thinking that they are compliant. Instead, they may simply believe that their partial compliance is better than nothing (and more expedient than full compliance).

In healthcare contexts such as ours, pseudocompliance can be the result of goal conflict, in which two or more institutional goals are at odds with each other (DiBenigno 2018, Franceschi-Bicchierai 2019). For example, healthcare providers are acutely aware of the need to maintain the confidentiality of patient records and comply with ISPs designed to ensure compliance with HIPAA and other regulations (Gaunt 2000). However, the primary goal of healthcare professionals is patient care (Ammenwerth and Spötl 2009), and any activity that distracts from direct patient care (such as logging in and out of the EHR terminal) is typically avoided (Mellott et al. 2013). Thus, although healthcare professionals may not want to violate the ISP, desire to avoid the cost to patient care in time and effort needed for full compliance can lead to pseudocompliance behavior. The appeal to their overriding mission of patient care can become an "appeal to higher loyalties" rationalization (Sykes and Matza 1957) to justify noncompliance with the ISP (Siponen and Vance 2010). Health professionals may also rationalize that pseudocompliance is "close enough" to full compliance, further allowing them to justify the violation, especially if they do not perceive any adverse effects on patient care (Silic et al. 2017). We identified this phenomenon through observation, which was further informed in subsequent interviews. Therefore, we hypothesize the following:

Hypothesis 2. *Intention to violate ISPs is negatively associated with pseudocompliance behavior.*

5.1.3. The Effect of Power Hierarchy on Intention and Behavior Across Groups.

Elevated power hierarchy is typically associated with greater financial and social capital (Anderson and Berdahl 2002), which an individual can use to reduce the severity of a sanction

(e.g., paying a criminal fine in lieu of imprisonment, using social capital to obtain an exception to a penalty). Therefore, the higher the power hierarchy of a person, the weaker will be perceptions of severity of sanctions. Conversely, it has also been reported that people having low power hierarchy are more susceptible to more material and social penalties, through which they are under persistent danger of losing favor from the powerful (Anderson and Berdahl 2002).

Historically, physicians have held a dominant power position (Abernethy and Vagnoni 2004, Raman and Bharadwaj 2012) compared with nurses and other support staff (Keddy et al. 1986). This difference in attitude stems from physician culture, which is built around individualism, discretion, and autonomy (Freidson 1970), in contrast to nursing culture, which is more characterized by compliance with policies from higher authorities (Evans et al. 2006, Nylinder 2011). Additionally, Abraham et al. (2008) suggest that there lies a significant power difference between support staff and clinical practitioners.

Instances of power play were clearly observable in the interview data as well as in the interactions between physicians and nurses and nurses and support staff. Knowing very well that there is a whistleblower process in place in the hospital, a nurse confided "*I do not want to be around to report any mistakes done by a physician*." A similar sentiment was shown by a support staff member when she described the following incident: "*I saw that nurse dispensing medicine to a patient without hand-washing after her lunch, but I am not the person to point that out. No way*." In fact, in one instance, the researcher observed that a physician, not satisfied with a nurse's actions, was exploring the possibility of requesting a shift change of that nurse from the nursing director.

The power differential between groups drives the perception that higher power entails more job security. Power over the other groups is also an indication of physicians' general attitude of being powerful and untouchable and thus able to exercise more violation behavior compared with nurses or support staff. Mackay (1993) attributes this power imbalance to the widely differing educational backgrounds of the three professions (Sweet and Norman 1995). Considering the significant differences between the educational levels and aptitudes of people in the three groups, significant differences in their capabilities are also expected, which leads to a power difference.

Nurses can sometimes feel oppressed by physicians (Roberts 1983) and may dread being reprimanded by them for committing errors (Calvin et al. 2009), sometimes even fearing losing their license (Stratton et al. 2004). Therefore, nurses are more diligent in ensuring they do not commit errors or violate ISPs for fear of severe sanctions. Support personnel, who are even lower in the power hierarchy, are even more fearful, so the perceived severity of sanctions on the part of support staff is even higher than that of nurses. We therefore hypothesize the following:

Hypothesis 3. *The higher a professional group is in the dimension of power hierarchy, the weaker will be the negative effect of perceived severity of sanctions on intention to violate the ISP.*

Employees may attempt to defy organizational policies if they hold powerful positions or occupations. For example, Crozier (1964, p. 153) reports that the maintenance workers at a French factory held the most power because they were the only ones who knew how to repair the equipment, which they kept a secret. They exhibited power by completely disregarding maintenance policies and preserved the "group's absolute control" in the organization. Similarly, in a healthcare organization, the power lies with the physicians (Raman and Bharadwaj 2012); they may choose to not attend training programs or not comply with policies because they do not fear sanctions, as they sit at the top of the power hierarchy. Our data show that when asked about compliance training (like HIPAA), support staff were more aware of and spoke more respectfully of it compared with nurses. Physicians were even less interested than nurses and felt that such administrative tasks hampered their work. Kim et al. (2001) confirm this in a study on improving safety measures in a hospital, where the attendance rate of physicians was 20% lower than that of nurses for a mandatory security training session.

Given these findings, we expect that for professional groups high in the power hierarchy, the relationship between intentions to violate the ISP and pseudocompliance will be weaker. Because physicians are high in the power hierarchy, we expect that they do not feel the need to create a false impression of compliance (pseudocompliance) when violating the ISP. In contrast, because nurses rank below physicians in the power structure, we expect them to exhibit higher levels of pseudocompliance. Similarly, we expect support staff, who have less power than nurses, to show even higher levels of pseudocompliance behavior than nurses. Therefore, we hypothesize the following:

Hypothesis 4. *The higher a professional group is in the dimension of power hierarchy, the weaker will be the negative effect of intention to violate the ISP on pseudocompliance.*

5.1.4. The Effect of Professional Prestige on Intention Across Groups. Individual behavior is influenced by the prestige or symbolic honor attached to the position of the group or social structure to which the

individual belongs (Klein 2016). Prestige is often derived from one's profession (Chan and Goldthorpe 2007). According to the Expectation States Theory (Correll and Ridgeway 2006), power and prestige are closely related. People in prestigious occupations (like physicians) are more likely to be accorded more power, even when their occupation has little to do with the task at hand. Additionally, people in prestigious occupations have the resources and network to influence decisions that affect themselves (Anderson and Berdahl 2002).

In our interviews, we found that physicians exhibited great pride in their profession. For example, a physician commented, "My grandfather was a physician, my dad is, and my wife is a physician too. I am surely going to have my daughter grow up to be a physician. I will be proud of it." In our context, nurses enjoyed less occupational prestige compared with the physicians. For example, similar to ISPs, a nurse explained an incident related to a violation of the hand-hygiene policy: "I was called out one day [by an administrative supervisor] for hand-washing compliance and I had to explain [myself]." In contrast, physicians had no supervisors because of their position. This is in agreement with previous literature that indicates that nurses have less prestige compared with physicians (Kalisch and Kalisch 1977). As the lowest in the professional group hierarchy, support staff tend to have the least prestige.

Previous research has shown that severity and certainty of sanctions operate in similar ways in deterring computer abuse and ISP violations (Straub and Nance 1990, Peace et al. 2003, Ugrin et al. 2007). Therefore, consistent with the logic of Hypothesis 3, we expect that the higher the occupational prestige, the lower will be the influence of certainty of sanctions. Because physicians have very high professional prestige (Shortell 1974), we expect that certainty of sanctions will affect them the least of the three groups, which in turn will decrease the effect of perceived certainty of sanctions on intentions to violate ISPs. In contrast, because nurses and support staff enjoy relatively less occupational prestige, we expect that the influence of certainty of sanctions on intentions to violate the ISP will be more pronounced. We therefore hypothesize the following:

Hypothesis 5. *The higher a professional group is in the dimension of occupational prestige, the weaker will be the negative effect of perceived certainty of sanctions on intention to violate the ISP.*

5.1.5. The Effect of Multitasking on Behavior Across Groups. Physicians, especially in an emergency department, are known to display a high degree of multitasking, that is, engaging in multiple tasks simultaneously (Chisholm et al. 2000, Laxmisan et al. 2007). The researcher observed that the physicians manage multiple high-acuity patients at the same time, especially during peak periods of activity. Physicians are required to constantly prioritize their decisions because of the wide variation in the nature of the tasks to which they must attend. The Emergency Medical Treatment and Active Labor Act of 1986 requires "emergency departments to provide medical screening and stabilizing care to all patients, regardless of their ability to pay," (American College of Emergency Physicians 1986). This has resulted in significant overcrowding in EDs and places significant multitasking demands on ED staff. Interview data clarified that physicians were trained to prioritize patients above all. Because physicians have the ultimate responsibility for patient care, their intention to serve the patient is stronger than that of the other groups.

The Theory of Planned Behavior (Ajzen 1985) suggests that the strongest intention will lead to the strongest behaviors. This explains why a physician does not place higher priority on complying with ISPs over clinical responsibility. Therefore, intention to violate ISP (in order to focus on patient care) will have a stronger positive association with actual violation for a physician than for a nurse. Similarly, observation and interview data showed that nurses were less prone to multitasking, whereas support staff exhibited the least multitasking. Multitasking and, hence, prioritization of work highly depend on the demands on the professional group (Bluedorn et al. 1992). Consistent with the observations in prior studies, our interview data suggest that physicians are required to multitask significantly more than nursing and support staff (Bellandi et al. 2018). We hypothesize this relationship as follows:

Hypothesis 6. *The higher a professional group is in the dimension of multitasking, the stronger will be the positive effect of intention to violate the ISP on the extent of ISP violation behavior.*

6. Phase 2: Quantitative Study—Purpose: Explanation

Following the development of the model depicted in Figure 3, we performed a quantitative study utilizing a field survey with hypothetical scenarios (Weber 1992) to test the hypotheses that grew out of our qualitative study and literature review. In this method, subjects are given vignettes (Alexander and Becker 1978) that describe realistic situations to which they respond using rating scales that measure dependent variables (Trevino 1992). Vignettes have been used in the social sciences (Wallander 2009) because they are a realistic, nonintrusive, and unintimidating way to obtain user feedback on sensitive issues (Nagin and Pogarsky 2001).

In IS research, this approach has been used widely to examine ISP violations (Siponen and Vance 2010).

To aid in the development of the survey instrument, interviews were conducted to understand the general ISP awareness culture and behavior in the institution under study. The vignettes were developed based on real-world stories and were therefore contextually relevant (Siponen and Vance 2014). Several experts in the domain, including the CMIO, senior physicians, nurses, and support staff from the institution, provided feedback on the appropriateness of the vignettes. The following four vignettes were developed for the study: workstations not locked when leaving the desk, unauthorized access to celebrity patient data, sharing of passwords, and unauthorized sharing of confidential patient data.

Wherever possible, the measurement items for constructs in this model were adapted from existing literature (Boudreau et al. 2001). Specifically, the items used were adapted to the healthcare domain from a validated instrument used by D'Arcy et al. (2009). The full instrument is given in Online Appendix D. Additionally, the validity of the instrument items within the healthcare context was evaluated by three information security and compliance experts from the healthcare domain. Pilot tests of the adapted instrument were then conducted with physicians, nurses, and support staff to check for clarity and contextual validity. Feedback was incorporated to refine the instrument as deemed necessary.

The first section of the survey instrument consisted of four vignettes with six items each to measure the variables perceived certainty of sanctions (PC), perceived severity of sanctions (PS), and intention to violate ISP (IVP). Following the procedure used by D'Arcy et al. (2009), composite measures of PC, PS, and IVP were created by summing each item across the four vignettes and then averaging the items by construct. The second section of the survey instrument consisted of items measuring informants' perceptions about the existence of ISPs; security education, training, and awareness (SETA) programs; and computer activity monitoring capabilities. The last section captured the demographics of the informants, including the professional group to which they belonged.

6.1. Survey

Informants were approached during their shift to complete a paper-based survey. This both ensured that the surveys were completed and provided an opportunity to observe whether informants locked the EHR screen according to the ISP when they left their station to complete the survey. Upon returning the completed survey, a brief semistructured interview was conducted with that informant by the primary researcher to obtain deeper insights into ISP violation behaviors.

The convenience sample, which included 123 physicians, nurses, and support staff who updated EHRs after interacting with patients, was obtained based on the availability of healthcare professionals during the particular shifts for which the researcher was present. As the researcher was accustomed to lengthy shifts (three to eight hours), informants were not hurried to complete the survey. All approached informants completed the survey and agreed to be interviewed. Two surveys were incomplete and were therefore dropped from the analysis, leaving 121 responses in our data set. A summary of the informants' demographics is given in Online Appendix E.

6.2. Observation During Survey Completion

In this phase of the study, the primary researcher observed each informant's actions during administration of the survey instrument, recording the time the informant left the desktop computer unattended and returned, and the state of the desktop (e.g., minimized EHR screen, locked desktop, etc.) during the informant's absence. Duration of absence varied from 20–45 minutes. While observing the informants, the researcher maintained a distance of at least 2–3 meters from the healthcare providers so as to observe providers' actions and take notes while not interfering with provider–patient or provider–provider interactions (Chisholm et al. 2000). The researcher also did not initiate any conversation with informants while they completed the survey (Hollingsworth et al. 1998). Of the 121 informants who completed the survey, 18 informants left their EHR screen unlocked and not minimized when they left their desk, exhibiting clear ISP violation behavior. The remaining 103 informants minimized the EHR window when they left their desk but did not lock the screen, exhibiting pseudocompliance behavior. Only two locked their screens when they left their computers, exhibiting compliance behavior.

This observed behavior was coded to create two dependent variables. First, "pseudocompliance behavior" (PSCOMP) was measured as a binary variable indicating whether the screen was minimized when the informant left the workstation rather than being locked according to the ISP. Second, based on data from the qualitative study and the time it took an informant to complete the survey, the "extent of ISP violation behavior" (EXTENT) was operationalized as a range, captured in four ordinal groups: informant was absent from the desk (1) for 5 minutes or less, (2) between 5 and 10 minutes, (3) between 10 and 20 minutes, and (4) 20 or more minutes. Creating these two dependent variables allowed us to incorporate actual behavior into our data and avoid common

method variance issues that can arise from collecting dependent and independent variables via the same instrument.

6.3. Analysis

Data were analyzed using tests for equality of means and partial-least squares (PLS) because of their facility in handling both formative and reflective indicators (Gefen et al. 2011; Hair et al. 2011; Petter 2018). We used SmartPLS version 2 in our analyses (Ringle et al. 2005). We document validations tests in Online Appendix F, including those for convergent and discriminant validity and those for multicollinearity and common method bias. The results show that our model meets or exceeds the rigorous standards expected for positivist IS research (Gefen et al. 2011).

Tests for equality of means were used to investigate the differences in perception, intent, and subsequent behavior related to ISPs between different professional groups in the organization. The Kruskal-Wallis H test (Kruskal and Wallis 1952), a conservative nonparametric statistical test, was used to check whether the differences across the groups were statistically significant. This test was used because it can compare more than two groups at a time, unlike the commonly used Mann-Whitney U test. Means of endogenous and dependent variables—perceived certainty of sanctions, perceived severity of sanctions, pseudocompliance behavior, intention to violate ISP, and extent of ISP violation behavior—were compared across the groups and were found to differ significantly. This implies that despite all groups belonging to the same organization, they exhibit differences in perceptions, intent, and behavior related to ISP. A graphical representation of the difference in means and the results are given in Figure 4 and Table 2, respectively.

Three dimensions of the model are analyzed: (1) the path coefficients (β), which denotes the strength of the relationship between the independent and the dependent variables; (2) whether the path is statistically significant; and (3) the R^2 value, which is the variance explained by the independent variables (Hair et al. 2013). Although β and R^2 values were derived by running the model, a bootstrapping resampling (5,000 samples) procedure was run separately to test for significance, per Hair et al. (2013, p. 186).

To test Hypothesis 1 and Hypothesis 2, the model was run with the complete data set to check for significance and the effects of intention to violate ISP on pseudocompliance behavior and on the extent of violation. Values of the path coefficient together with their significance level are given in Table 3. IVP has a significant effect on both EXTENT ($\beta = 0.419$, $p < 0.001$) and PSCOMP ($\beta = -0.270$, $p < 0.001$), as hypothesized, thus supporting both Hypothesis 1 and Hypothesis 2. The R^2 value for the dependent variable EXTENT was 0.176, indicating that IVP explained a substantive portion of the variance (Falk and Miller 1992). The R^2 for PSCOMP was 0.073, implying that IVP explains only 7.3% of the variance. The variance explained in our study is in line with meta-analyses that report that intentions predict actual behavior with an R^2 of between 0.16 and 0.67, with an average of 0.28 (Sheeran 2002).

To test the variation of the moderation effect with the three different groups (physicians, nurses, and support staff), the model was tested three times using a multiple group approach, as suggested by Frazier et al. (2004). All data were split into three groups: (a) physicians versus nurses, (b) physicians versus support staff, and (c) nurses versus support staff. Hypotheses 3–6 were then each tested by running the model with data for one group at a time (Keil et al. 2000). For example, Hypothesis 3(a) tested Hypothesis 3 for the physicians versus nurses group. Sample mean and standard errors of the path coefficients are noted for each run (Lowry and Gaskin 2014). The path coefficients and the standard error values were compared between groups using a *t*-test, as used in past IS research (Keil et al. 2000). The results are given in Table 4.

Figure 4. Means Across Groups

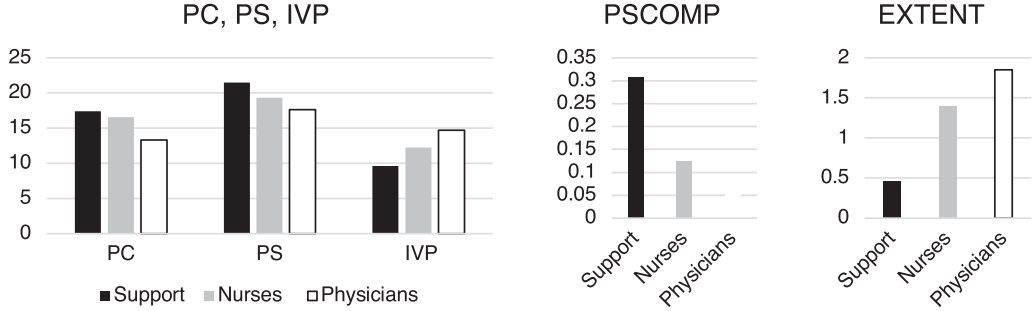


Table 2. Means of Variables Across Groups (Kruskal-Wallis H Test)

Construct	Physicians	Nurses	Support	Range	Significance
PC	13.309	16.583	17.404	4–24	$p < 0.001$
PS	17.606	19.354	21.461	4–24	$p < 0.001$
IVP	14.702	12.260	9.653	4–24	$p < 0.001$
PSCOMP	0.085	0.125	0.308	0–1	$p < 0.033$
EXTENT	1.851	1.396	0.462	0–3	$p < 0.001$

7. Phase 3: Qualitative Study—Purpose: Triangulation

Following an informant's completion of the survey, a semistructured interview (lasting no longer than ten minutes) was conducted with the informant. These interviews were designed to uncover the reasons for their behavior and gain further insight into the differences in security behaviors across the professional groups. The interviews were conducted in private and in an informal tone. The researcher did not confront the informants, even if the actions they reported in the interview were contrary to their observed actions. All 123 informants who were invited to take the survey were interviewed. The qualitative analysis provided insights into the behaviors examined in Phase 2. In Sections 7.1–7.3, we discuss the ISP behaviors of each group.

7.1. Physicians

One of the physicians who kept the screen of his EHR application open when he left to attend to a patient, demonstrating ISP violation, made the following comment: *"I am more interested in treating the patient. When there is a gun-shot wound to be addressed, I am not bothered about anything else. That* [ISP compliance] *can wait. . .the patient can't."* Another physician explained her similar behavior as follows: *"This is the practice that I saw and learned from my seniors. I am not sure why you are asking me this."* These sentiments were echoed by several physicians, suggesting that physicians demonstrate the lowest amount of pseudocompliance behavior relative to the other professional groups.

7.2. Support Staff

Compared with the physicians, the support staff showed the largest divergence in ISP compliance behavior. As a representative example, one support staff member who complied with the ISP by logging out of the EHR application explained: *"This job is too precious to me, and I do not want to lose this job because of running into problems with HIPAA."* Another support staff member who demonstrated pseudocompliance behavior summed up the sentiment of several others by stating that although he wanted to follow the spirit of the ISP, he was unwilling to spend the considerable time and effort required to fully comply with the ISP because of the potential negative impact on patient care. He stated: *"I know about HIPAA and that logging out is what I should do. But look at it this way: I am minimizing this screen when I go to take the temperature of a patient. I will be back soon and resume work from the same screen. Logging out and logging in to* [the EHR application] *will take me more time than the time it takes to go measure the patient's temperature and be back at my desk."* These excerpts help explain why support staff demonstrate the least ISP violation behavior yet the most pseudocompliance behavior.

7.3. Nurses

Analysis of nurses' interview data showed that commitment to ISP compliance and demonstration of pseudocompliance was higher than that of physicians and lower than that of support staff. That is, they neither showed behavior similar to the physicians' nor did they overwhelmingly demonstrate pseudocompliance behavior similar to that of the support staff. A nurse who left the screen open (ISP violation behavior) when she went to the supply room to pick up a syringe came back hurriedly and explained her behavior: *"I am not supposed to do that. However, this patient* [pointing to a patient in the room] *needs the medication now. I am attending to three more patients in parallel. I cannot login and logout every time I leave the desk."* She acknowledged that she violated the ISP and expressed that she was sorry, in contrast to physicians, who ignored the ISP and did not express regret regarding the violation. Another nurse who minimized the screen (and did not log out before leaving the desk), thus demonstrating pseudocompliance, had this rationalization: *"This place has physical controls in place. No one without a badge is allowed here. So how does it matter whether I log out or keep the screen on? And moreover, we know when the* [HIPAA] *audits are."* The nurses appeared to be more aware of the environment and knew the audit procedures and the timing of the HIPAA audits better than the support staff;

Table 3. Hypotheses Test Summary

No.	Hypothesis and direction	Path coefficient (β)	*t*-value	Significance (one-tailed)	Supported?
Hypothesesis 1	IVP → EXTENT (+)	0.419	4.915	$p < 0.001$	Yes
Hypothesesis 2	IVP → PSCOMP (-)	–0.270	2.875	$p < 0.001$	Yes

Table 4. Hypotheses Test Summary

	Hypotheses		Path coefficient (β) sample means				
No.	Group A: β	Group B: β	Group A	Group B	Direction supported?	*t*-value	Supported?
Hypothesis 3	$(PS \rightarrow IVP)_p$	$(PS \rightarrow IVP)_n$	−0.157	−0.610	Yes	3.154**	Yes
	$(PS \rightarrow IVP)_p$	$(PS \rightarrow IVP)_s$	−0.157	−0.542	Yes	2.655**	Yes
	$(PS \rightarrow IVP)_n$	$(PS \rightarrow IVP)_s$	−0.610	−0.542	No	0.490 ns	No
Hypothesis 4	$(IVP \rightarrow PSCOMP)_p$	$(IVP \rightarrow PSCOMP)_n$	−0.177	−0.326	No	1.139 ns	No
	$(IVP \rightarrow PSCOMP)_p$	$(IVP \rightarrow PSCOMP)_s$	−0.177	−0.071	Yes	0.675 ns	No
	$(IVP \rightarrow PSCOMP)_n$	$(IVP \rightarrow PSCOMP)_s$	−0.326	−0.071	Yes	2.049*	Yes
Hypothesis 5	$(PC \rightarrow IVP)_p$	$(PC \rightarrow IVP)_n$	−0.046	0.231	No	1.873*	No
	$(PC \rightarrow IVP)_p$	$(PC \rightarrow IVP)_s$	−0.046	0.488	No	3.226***	No
	$(PC \rightarrow IVP)_n$	$(PC \rightarrow IVP)_s$	0.231	0.488	No	1.810*	No
Hypothesis 6	$(IVP \rightarrow EXTENT)_p$	$(IVP \rightarrow EXTENT)_n$	0.411	0.055	Yes	3.378***	Yes
	$(IVP \rightarrow EXTENT)_p$	$(IVP \rightarrow EXTENT)_s$	0.411	0.181	Yes	1.953*	Yes
	$(IVP \rightarrow EXTENT)_n$	$(IVP \rightarrow EXTENT)_s$	0.055	0.181	No	1.079 ns	No

Notes. All tests are directional (one-tailed). ns, not significant.
*$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

no support staff member mentioned HIPAA audits. The informants' justification for pseudocompliance behavior centered on perceiving the action as a reasonable compromise between fully complying with the ISP and minimizing effort on nonclinical activities, because the physical area is already secured and pseudocompliance is unlikely to be caught. Collectively, the nurses' behavior toward violation of the ISP was in between that of the physicians and that of the support staff, in agreement with our hypotheses.

8. Discussion

The results of this study offer a number of contributions, which are summarized in Table 5.

First, although the construct of professional subcultures is well established in the management literature and has been shown in past research to substantially influence behavior, to our knowledge prior to this study, the influence of professional subculture on perceptions of sanctions in the ISP context has not been recognized. In this study, we show that analogous to the effect of national culture on sanctions in the ISP context (Hovav and D'Arcy 2012, Kam et al. 2015, Menard et al. 2018, Cram et al. 2019), different professional subcultures may exist within an organization and members of these subcultures can perceive ISP-related sanctions very differently. These insights into the influence of professional subculture on perceptions of sanctions and consequent violation behavior represent an important contribution to our understanding of ISP compliance. Further, we explain that in healthcare, because of (1) high penalties for ISP violations and (2) deeply ingrained professional subcultures, the influence of professional subcultures on ISP violation is especially relevant.

Second, we performed a three-phase, mixed-methods study in which we collected and analyzed both qualitative (documentary analysis, observation, and interviews) and quantitative (scenario-based field survey and observation) data to provide a holistic view of professional subculture and ISP violations. Following the mixed-methods guidelines of Venkatesh et al. (2013, 2016), we were able to develop an integrated view of professional subculture and its influence on ISP violations in a large emergency department comprising physicians, nurses, and support staff. An exploratory qualitative study helped identify three dimensions of professional subculture that explain differences in ISP violations (power, prestige, and multitasking) as well as the construct of pseudocompliance behavior, all of which were used in the quantitative study to develop a holistic understanding of ISP violation behaviors. Further, a qualitative study produced further insights into the differences in ISP violation behavior among the three different subcultures.

Third, we found empirical evidence that professional subcultures influence ISP violations. Analysis of the data in the qualitative phases of this study showed that there is an undeclared hierarchy of authority and power among physicians, nurses, and support staff, despite that these groups do not have a formal structure for reporting to each other. This is an interesting finding because healthcare organizations are organized collaboratively (Adler et al. 2008) in contrast to the hierarchical organization of most businesses. Our analysis seems to suggest that this healthcare institution has an informal hierarchy that is reflected in ISP-related behavior, even though the institution nominally follows a professional bureaucratic structure. One potential explanation might be that in a professional

Table 5. Research Contributions

Element of research	Type	Contributions
Mechanisms of professional subculture	Theoretical, empirical	Identified through an exploratory qualitative study three dimensions of professional subculture that explain differences in behavior among professional subcultures in a healthcare context: power, prestige, and multitasking
Theorizing the influence of professional subculture on ISP violation	Theoretical, empirical	Examined the influence of professional subcultures on ISP violation behaviors and pseudocompliance behavior in the context of the Extended General Deterrence Theory of D'Arcy et al. (2009)
Demonstrating and theorizing the effect of professional subculture on ISP violations	Empirical, theoretical	Demonstrated that different professional subcultures in a healthcare organization have different degrees of ISP violation intentions and behaviors. Theorized why mechanisms of professional subculture influence perceptions of sanctions and ISP violation intentions and behaviors
Pseudocompliance	Theoretical, empirical	Theorized about the construct of "pseudocompliance behavior" to examine behaviors that outwardly appear compliant but are not actually compliant and showed how professional subculture influences pseudocompliance behavior
Integrated intentional and behavioral data	Methodological, empirical	Integrated data on intention to violate the ISP with actual violation behavior data, providing a more complete view of the influence of professional subcultures on ISP violations
Mixed-methods data collection	Methodological, empirical	Performed a three-phase, mixed-methods study involving qualitative (documentary analysis, observation, and interviews) and quantitative (scenario-based field survey and observation) data to provide a holistic view of professional subcultures and ISP violations

bureaucracy, power resides in the skill or the expertise, which possibly justifies this hierarchy because the physicians are the most educated and highly skilled, followed by nurses and then support staff.

Fourth, our results highlight pseudocompliance behavior as an important type of ISP violation. Pseudocompliance is essentially "window dressing" that appears beneficial but doesn't actually provide any real security (Skårderud 2007). Past research has differentiated ISP violation constructs depending on the underlying motivation (e.g., volitional but not malicious noncompliance vs. malicious noncompliance), each requiring different approaches to address them (Willison and Warkentin 2013, Cram et al. 2019). In this light, pseudocompliance may be another category of ISP violation with a motivation distinct from those described above. For example, in our study we found that employees wanted to comply but were unwilling to do so if that meant impeding their patient care workflow. They saw pseudocompliance as a compromise, rationalizing that partial compliance was better than nothing. This motivation suggests that pseudocompliance may need to be addressed by calling out this rationalization during SETA training. A more ideal solution would be to streamline the authentication process so that employees do not feel that compliance with ISPs impinges upon patient care. Nevertheless, our findings are preliminary and additional work is warranted to clearly establish pseudocompliance as a construct distinct from other types of ISP violations.

Fifth, this study integrated intentional and behavioral data. From a methodological perspective, research on information security is challenging because it is difficult for researchers to gain access to the actual information security behaviors and practices enacted in an organization (Kotulic and Clark 2004). In particular, Crossler et al. (2013) note the difficulty of observing ISP violations in the field. Therefore, with very few exceptions, self-reported or perceptual measures are used as the dependent variable in ISP compliance research (Cram et al. 2019). However, Crossler et al. (2013) point out that this practice is problematic because intentions do not always lead to behaviors, and they call for research that objectively measures ISP violation behavior. To our knowledge, only Jenkins et al. (2010) and Workman et al. (2008) have measured ISP compliance behavior objectively,

and only the latter did so in the field. This field study responds to their call as one of the few studies to measure ISP violation behavior objectively.

8.1. Implications for Practice

Organizations contain different professional subcultures, and not every group will respond in the same way to organization-wide ISPs and/or the associated sanctions. We therefore argue that the effectiveness of ISPs must be evaluated across different professional groups in an organization. This research can help management and security practitioners tailor ISPs and SETA programs to various professional groups and help managers develop measures to promote ISP compliance. In doing so, it is important to elicit feedback from the various professional groups about ISPs. Their feedback will likely lead to ISPs that better accommodate all professional groups, thus reducing ISP violations.

More importantly, we found in this study that most healthcare workers exhibiting violation of ISPs or pseudocompliant behavior still expressed a desire to comply with the ISPs but were unwilling to sacrifice their ability to quickly respond to patient needs to do so. Patient care will always take precedence over procedural concerns in an acute healthcare setting. Thus, this study identifies another practical situation in which existing ISPs are too cumbersome to engender full compliance (Adams and Sasse 1999). Rather than holding up healthcare employees' behavior as observed in this study as a reason to modify training and introduce mechanisms to force compliance, we argue that there is a critical need to find ways to redesign the systems and processes so that security controls create less friction and do not introduce a conflict of priorities for employees. For example, in the context of this study, touchless, proximity-based authentication mechanisms could be put into place that would automatically unlock and lock EHR workstations when an employee approaches or leaves the workstation.

8.2. Limitations and Future Research

This work has several limitations. First, it may be argued that the findings of this research have limited generalizability. Although we examined the influence of professional subculture in a healthcare context, our findings are likely relevant to a variety of organizational contexts where subcultures exhibit clear differences in power distribution, prestige, and multitasking. Klein et al. (1995) note that inside organizations, there exist subcultures and that these subcultures can vary in terms of their norms. Thus, the findings from this study have the potential to apply more widely not only to other healthcare organizations but also to other organizations in industries, such as aviation, nuclear safety, and petrochemicals, examples of fields in which very different strata of professional groups with potentially different subcultures coexist. To the extent that such professional subcultures do exist, security managers should take them into account when designing ISPs.

Second, because the research setting was an emergency department, it may be argued that the hospital's physical security measures acted as compensating controls for failures to lock EHR workstations and therefore may have contributed to the prevalence of pseudocompliance behavior. However, although outsiders may have limited physical access to EHR workstations, a critical risk still lies in healthcare professionals abusing their access rights as insiders to view records for patients whom they are not assigned to serve (Vance et al. 2013). This is a major problem and routinely results in HIPAA penalties to hospitals and sanctions to individuals (Mountenay and Brady 2019). Further, requiring each employee to authenticate identity to access EHRs is the primary means of ensuring accountability and reducing the risk of unauthorized access (Vance et al. 2015). Therefore, the physical security of the hospital environment is unlikely to fully explain the observed pseudocompliance. Nonetheless, future research should explore whether pseudocompliance is observable in organizations with less strict physical security or with less goal conflict between performing job duties and following the ISP. For example, can pseudocompliance be triggered by ISPs in conflict with departmental goals that are less serious than patient care? Further, future research should examine methods of designing ISPs with other organizational goals, such as operational efficiency (Acosta 2017).

Third, because data for two of the dependent variables were collected via observation, one can argue that data could be influenced by the Hawthorne effect. However, the influence of this effect is likely minimal for the following reasons. The primary researcher was introduced to the key members in the healthcare institution by the CMIO, who informed all staff members that the researcher would be observing their work for an extended period. Additionally, the researcher spent more than 200 hours on work shifts with the physicians, nurses, and support staff to gain familiarity and trust and to observe their usage of the EHR application before the survey was administered. Therefore, the presence of the researcher for observation was unlikely to be perceived as intrusive. Finally, because the study site was a teaching institution, several researchers worked routinely with the staff making their presence routine.

8. Conclusion

This research examined how different professional subcultures influence ISP compliance in a

healthcare institution. The results suggest that although there is no formal hierarchy in the reporting structure between physicians, nurses, and support staff, there is nonetheless wide variance in ISP violation behavior because of differences in professional subcultures. A key implication of our findings is that professional subcultures should be taken into account in addressing the problem of ISP violations because substantial differences in intentions and behaviors exist based on professional subcultures. Also, developers of ISPs as well as the designers of user interfaces of software should be cognizant of the differences in behaviors of different professional subcultures within organizations.

Acknowledgments

The authors thank the senior editor, associate editor, and reviewers for their developmental feedback throughout the review process. The authors also thank the hospital management for their cooperation and the informants for allowing them to spend time with them and to learn from the important work they do.

References

Abernethy MA, Vagnoni E (2004) Power, organization design and managerial behaviour. *Accounting Organ. Soc.* 29(3):207–225.

Abraham J, Reddy MC (2008) Moving patients around: A field study of coordination between clinical and non-clinical staff in hospitals. *Proc. 2008 ACM Conf. Comput. Supported Cooperative Work* (ACM, San Diego, CA), 225–228.

American College of Emergency Physicians (1986) EMTALA fact sheet. Accessed May 2, 2020, https://www.acep.org/life-as-a-physician/ethics--legal/emtala/emtala-fact-sheet/.

Acosta DER (2017) Smashing the information security policy for fun and profit. *ISACA J.* (1):1–6.

Adams A, Sasse MA (1999) Users are not the enemy. *Commun. ACM* 42(12):40–46.

Adler PS, Seok-Woo K, Charles H (2008) Professional work: The emergence of collaborative community. *Organ. Sci.* 19(2):359–376.

Ajzen I (1985) From intentions to actions: A theory of planned behavior. Kuhl J, Beckmann J, eds. *Action Control: From Cognition to Behavior* (Springer-Verlag, New York), 11–39.

Alexander CS, Becker HJ (1978) The use of vignettes in survey research. *Public Opinion Quart.* 42(1):93–104.

Alter Steven (2014) Theory of workarounds. *Comm. Assoc. Inform Systems* 34(1):1041–1066.

Ammenwerth E, Spötl H (2009) The time needed for clinical documentation vs. direct patient care. *Methods Inform. Medicine* 48(1): 84–91.

Anderson C, Berdahl JL (2002) The Experience of Power: Examining the Effects of Power on Approach and Inhibition Tendencies. *J. Personality Soc. Psych.* 83(6):1362–1377.

Angst CM, Agarwal R (2009) Adoption of Electronic Health Records in the presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quart.* 33(2):339–370.

Bagozzi RP (2007) The legacy of the technology acceptance model and a proposal for a paradigm shift. *J. Assoc. Inform. Systems* 8(4):244–254.

Bai G, Jiang J, Flasher R (2017) Hospital risk of data breaches. *JAMA Internal Medicine* 177(6):878–880.

Barley SR (1990) Images of imaging: Notes on doing longitudinal work. *Organ. Sci.* 1(3):220–245.

Bellandi T, Cerri A, Carreras G, Walter S, Mengozzi C, Albolino S, Mastrominico E, Renzetti F, Tartaglia R, Westbrook J (2018) Interruptions and multitasking in surgery: A multicentre observational study of the daily work patterns of doctors and nurses. *Ergonomics* 61(1):40–47.

Bloor G, Dawson P (1994) Understanding professional culture in organizational context. *Organ. Stud.* 15(2):275–295.

Bluedorn AC, Kaufman CF, Lane PM (1992) How many things do you like to do at once? An introduction to monochronic and polychronic time. *Acad. Management Perspective* 6(4):17–26.

Boss SR, Galletta DF, Benjamin Lowry P, Moody GD, Polak P (2015) What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quart.* 39(4):837–864.

Boudreau M-C, Robey D (2005) Enacting integrated information technology: A human agency perspective. *Organ. Sci.* 16(1):3–18.

Boudreau M-C, Gefen D, Straub DW (2001) Validation in information systems research: A state-of-the-art assessment. *MIS Quart.* 25(1):1–16.

Bryant A, Charmaz K (2007) *The SAGE Handbook of Grounded Theory* (Sage, Thousand Oaks, CA).

Bryman A (2006) Integrating quantitative and qualitative research: How is it done? *Qualitative Res.* 6(1):97–113.

Callen J, Braithwaite J, Westbrook J (2009) The importance of medical and nursing sub-cultures in the implementation of clinical information systems. *Methods Inform. Medicine* 48(2):196–202.

Calvin AO, Lindy CM, Clingon SL (2009) The cardiovascular intensive care unit nurse's experience with end-of-life care: A qualitative descriptive study. *Intensive Critical Care Nursing* 25(4): 214–220.

Cao J, Crews JM, Lin M, Deokar A, Burgoon JK, Nunamaker JF Jr (2006) Interactions between system evaluation and theory testing: A demonstration of the power of a multifaceted approach to information systems research. *J. Management Inform. Systems* 22(4): 207–235.

Chan TW, Goldthorpe JH (2007) Class and status: The conceptual distinction and its empirical relevance. *Amer. Soc. Rev.* 72(4): 512–532.

Charmaz K (2006)Theoretical sampling, saturation and sorting. Charmaz K, ed. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis* (Sage, Thousand Oaks, CA), 96–122.

Chatterjee S, Gao X, Sarkar S, Uzmanoglu C (2019) Reacting to the scope of a data breach: The differential role of fear and anger. *J. Bus. Res.* 101:183–193.

Chisholm CD, Collison EK, Nelson DR, Cordell WH (2000) Emergency department workplace interruptions are emergency physicians "interrupt-driven" and "multitasking"? *Acad. Emergency Medicine* 7(11):1239–1243.

Corbin JM, Strauss AL (2015) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 4th ed. (Sage Publications, Newbury Park, CA).

Correll SJ, Ridgeway CL (2006) Expectation states theory. DeLamater J, ed. *Handbook of Social Psychology* (Springer, Boston), 29–51.

Cram WA, D'arcy J, Proudfoot JG (2019) Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quart.* 43(2):525–554.

Cram WA, Proudfoot JG, D'Arcy J (2017) Organizational information security policies: A review and research framework. *Eur. J. Inform. Systems* 26(6):605–641.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. *Comput. Security* 32(0):90–101.

Crozier M (1964) Power and uncertainty. Crozier M, ed. *The Bureaucratic Phenomenon* (University of Chicago Press, Chicago), 145–174.

D'Arcy J, Herath T (2011) A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *Eur. J. Inform. Systems* 20(6):643–658.

D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inform. Systems Res.* 20(1):79–98.

DiBenigno J (2018) Anchored personalization in managing goal conflict between professional groups: The case of U.S. Army mental healthcare. *Adm. Sci. Quart.* 63(3):526–569.

Erasmus V, Daha TJ, Brug H, Richardus JH, Behrendt MD, Vos MC, van Beeck EF (2010) Systematic review of studies on compliance with hand hygiene guidelines in hospital care. *Infection Control Hospital Epidemiology* 31(3):283–294.

Evans SM, Berry JG, Smith BJ, Esterman A, Selim P, O'Shaughnessy J, DeWit M (2006) Attitudes and barriers to incident reporting: A collaborative hospital study. *Quality Safety Health Care* 15(1):39–43.

Fagenson EA (1990) Perceived masculine and feminine attributes examined as a function of individuals' sex and level in the organizational power hierarchy: A test of four theoretical perspectives. *J. Appl. Psychol.* 75(2):204–211.

Falk RF, Miller NB (1992) *A Primer for Soft Modeling* (University of Akron Press, Akron, OH).

Franceschi-Bicchierai L (2019) How a simple copy/paste revealed explosive new detail in Manafort's case. Accessed May 2, 2020, https://www.vice.com/en_us/article/8xpye3/paul-manafort-russia-case-redaction-fail.

Frazier PA, Tix AP, Barron KE (2004) Testing moderator and mediator effects in counseling psychology research. *J. Counseling Psychol.* 51(1):115–134.

Freidson E (1970) *Profession of Medicine: A Study in the Sociology of Applied Knowledge* (University of Chicago Press, Chicago).

Gaunt N (2000) Practical approaches to creating a security culture. *Internat. J. Medical Inform.* 60(2):151–157.

Gefen D, Rigdon EE, Straub D (2011) An update and extension to SEM guidelines for administrative and social science research. *MIS Quart.* 35(2):iii–xiv.

Gershon RRM, Vlahov D, Felknor SA, Vesley D, Johnson PC, Delcios GL, Murphy LR (1995) Compliance with universal precautions among healthcare workers at three regional hospitals. *Amer. J. Infection Control* 23(4):225–236.

Haas J, Shaffir W (1977) The professionalization of medical students: Developing competence and a cloak of competence. *Symbolic Interaction* 1(1):71–88.

Hair JF, Ringle CM, Sarstedt M (2011) PLS-SEM: Indeed a silver bullet. *J. Marketing Theory Practice* 19(2):139–152.

Hair JFJ, Hult GTM, Ringle CM, Sarstedt M (2013) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (Sage Publications, Inc., Thousand Oaks, CA).

Hall P (2005) Interprofessional teamwork: Professional cultures as barriers. *J. Interprofessional Care* (19):188–196.

Harris LC, Ogbonna E (1998) Employee responses to culture change efforts. *Human Resource Management J.* 8(2):78–92.

Hofstede G (1998) Identifying organizational subcultures: An empirical approach. *J. Management Stud.* 35(1):1–12.

Hollingsworth JC, Chisholm CD, Giles BK, Cordell WH, Nelson DR (1998) How do physicians and nurses spend their time in the emergency department? *Ann. Emergency Medicine* 31(1):87–91.

Hovav A, D'Arcy J (2012) Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Inform. Management* 49(2):99–110.

Huang JC, Newell S, Galliers RD, Shan-Ling P (2003) Dangerous liaisons? Component-based development and organizational subcultures. *IEEE Trans. Engrg. Management* 50(1):89–99.

IBM (2019) 2019 cost of data breach report. Accessed May 2, 2020 https://www.ibm.com/security/data-breach.

ID Theft Resource Center (2018) ID Theft Resource Center (ITRC) data breach overview 2005 to 2017. Accessed May 2, 2020, https://www.idtheftcenter.org/images/breach/Overview20052017.pdf.

Jenkins JL, Durcikova A, Ross G, Nunamaker Jr JF (2010) Encouraging users to behave securely: Examining the influence of technical, managerial, and educational controls on users' secure behavior. *Internat. Conf. Inform. Systems (ICIS), St. Louis, MO*, 1–18.

Jick TD (1979) Mixing qualitative and quantitative methods: Triangulation in action. *Admin. Sci. Quart.* 24(4):602–611.

Kalisch BJ, Kalisch PA (1977) An analysis of the sources of physician nurse conflict. *J. Nursing Admin.* 7(1):50–57.

Kam H-J, Katerattanakul P, Hong S-G (2015) A tale of two cities: Information security policy compliance of the banking industry in the United States and South Korea. *23rd Eur. Conf. Inform. Systems (ECIS 2015)* (Association for Information Systems, Atlanta), Paper 90.

Keddy B, Gillis MJ, Jacobs P, Burton H, Rogers M (1986) The doctor-nurse relationship: An historical perspective. *J. Advanced Nursing* 11(6):745–753.

Keil M, Tan BCY, Wei K-K, Saarinen T, Tuunainen V, Wassenaar A (2000) A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quart.* 24(2):299–325.

Kim LE, Jeffe DB, Evanoff BA, Mutha S, Freeman B, Fraser VJ (2001) Improved compliance with universal precautions in the operating room following an educational intervention. *Infection Control Hospital Epidemiology* 22(8):522–524.

Klein M (2016) Educational expansion, occupational closure and the relation between educational attainment and occupational prestige over time. *Sociology* 50(1):3–23.

Klein HK, Myers MD (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quart.* 23(1):67–94.

Klein RL, Bigley GA, Roberts KH (1995) Organizational culture in high reliability organizations: An extension. *Human Relations* 48(7):771–793.

Kotulic AG, Clark JG (2004) Why there aren't more information security research studies. *Inform. Management* 41(5):597–607.

Kruskal WH, Wallis WA (1952) Use of ranks in one-criterion variance analysis. *J. Amer. Statist. Assoc.* 47(260):583–621.

Kwon J, Johnson E (2018) Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quart.* 42(4):1043–1067.

Laxmisan A, Hakimzada F, Sayan OR, Green RA, Zhang J, Patel VL (2007) The multitasking clinician: Decision-making and cognitive demand during and after team handoffs in emergency care. *Internat. J. Medical Inform.* 76(11):801–811.

Lok P, Westwood R, Crawford J (2005) Perceptions of organisational subculture and their significance for organisational commitment. *Appl. Psych.* 54(4):490–514.

Lowry PB, Gaskin J (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use It. *IEEE Trans. Professional Comm.* 57(2):123–146.

Mackay L (1993) *Conflicts in Care Medicine and Nursing* (Chapman & Hall, London).

Martin J, Siehl C (1983) Organizational culture and counter-culture. *Organ. Dynam.* 12(2):52–64.

Mattarelli E, Bertolotti F, Incerti V (2015) The interplay between organizational polychronicity, multitasking behaviors and organizational identification: A mixed-methods study in knowledge intensive organizations. *Internat. J. Human Comput. Stud.* 79(July):6–19.

Mellott M, Thatcher JB, Roberts N (2013) Electronic medical record compliance and continuity in delivery of care: An empirical investigation in a combat environment. *Health Systems (Basingstoke)* (2):147–161.

Menard P, Warkentin M, Lowry PB (2018) The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Comput. Security* (75):147–166.

Miles MB, Huberman MA, Saldana J (2014) *Qualitative Data Analysis: A Methods Sourcebook*, 3rd ed. (Sage Publications, Thousand Oaks, CA).

Mingers J (2001) Combining IS research methods: Toward a pluralist methodology. *Inform. Systems Res.* 12(3):240–259.

Mountenay B, Brady C (2019) What your staff doesn't know about HIPAA can kill you. Accessed May 2, 2020 https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-what-your-staff-doesnt-know-about-hipaa-can-kill-you.

Myers MD, Newman M (2007) The qualitative interview in IS research: Examining the craft. *Inform. Organ.* 17(1):2–26.

Nagin DS, Pogarsky G (2001) Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology* 39(4):865–891.

Nylinder P (2011) Perception of budgetary control: A study of differences across managers in Swedish public primary healthcare related to professional background and sex. *J. Nursing Management* 19(5):664–672.

Peace AG, Galletta DF, Thong JYL (2003) Software piracy in the workplace: A model and empirical test. *J. Management Inform. Systems* 20(1):153–177.

Petter S (2018) Haters gonna hate': PLS and information systems research. *Data Base Adv. Inform. Systems* 49(2):10–13.

Pierson B (2017) Anthem to pay record $115 million to settle U.S. lawsuits over data breach. Accessed May 2, 2020, https://www.reuters.com/article/us-anthem-cyber-settlement-idUSKBN19E2ML.

Raman R, Bharadwaj A (2012) Power differentials and performative deviation paths in practice transfer: The case of evidence-based medicine. *Organ. Sci.* 23(6):1593–1621.

Ringle CM, Wende S, Will A (2005) SmartPLS 2.0 (M3). Accessed June 6, 2020, http://www.smartpls.com.

Roberts SJ (1983) Oppressed group behavior: Implications for nursing. *ANS. Adv. Nurs. Sci.* 5(4):21–30.

Robey D, Azevedo A (1994) Cultural analysis of the organizational consequences of information technology. *Account. Management. Inform. Tech.* 4(1):23–27.

Sarker S, Sarker S (2009) Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context. *Inform. Systems Res.* 20(3):440–461.

Sarker S, Ahuja M, Sarker S (2018) Work–life conflict of globally distributed software development personnel: An empirical investigation using border theory. *Inform. Systems Res.* 29(1):103–126.

Sarkar S, Ghosh K, Petter S (2020) Using secondary data to tell a new story: A cautionary tale in health information technology research. *Comm. Assoc. Inform. Systems*. Forthcoming.

Sarker S, Xiao X, Bealieu T, Lee AS (2018a) Learning from first-generation qualitative approaches in the IS discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). *J. Assoc. Inform. Systems* 19(8):752–774.

Schein EH (2010) *Organizational Culture and Leadership*, 4th ed. (Jossey-Bass, San Francisco).

Schneider SM, Gallery ME, Schafermeyer R, Zwemer FL (2003) Emergency department crowding: A point in time. *Ann. Emergency Medicine* 42(2):167–172.

Schofield J (2018) GDPR: How can I email data securely to comply with the new regulations? *The Guardian* (March 29), https://www.theguardian.com/technology/askjack/2018/mar/29/gdpr-email-data-protection-regulations-secure.

Schouten JW, McAlexander JH (1995) Subcultures of consumption: An ethnography of the new bikers. *J. Consum. Res.* 22(1):43–61.

Scott T, Mannion R, Davies H, Marshall M (2003a) *Healthcare Performance and Organisational Culture* (Radcliff Medical Press, Oxon, UK).

Scott T, Mannion R, Davies HTO, Marshall MN (2003b) Implementing culture change in healthcare: Theory and practice. *Internat. J. Qual. Health Care* 15(2):111–118.

Seidel S, Recker J, Brocke J (2013) Sensemaking and sustainable practicing: Functional affordances of information systems in green transformations. *MIS Quart.* 37(4):1275–1299.

Sheeran P (2002) Intention-behaviour relations: A conceptual and empirical review. *Eur. Rev. Soc. Psych.* 12(1):1–36.

Shortell SM (1974) Occupational prestige differences within the medical and allied health professions. *Soc. Sci. Medicine (1967)* 8(1):1–9.

Silic M, Barlow JB, Back A (2017) A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Inform. Management* 54(8):1023–1037.

Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quart.* 34(3):487–502.

Siponen M, Vance A (2014) Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *Eur. J. Inform. Systems* 23(3):289–305.

Siponen M, Puhakainen P, Vance A (2020) Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Comput. Security* 88:1–12.

Skårderud F (2007) Eating one's words: Part III. Mentalisation-based psychotherapy for anorexia nervosa—an outline for a treatment and training manual. *Eur. Eating Disorder Rev.* 15(5):323–339.

Stratton KM, Blegen MA, Pepper G, Vaughn T (2004) Reporting of medication errors by pediatric nurses. *J. Pediatric Nurse* 19(6):385–392.

Straub DW (1990) Effective IS security: An empirical study. *Inform. Systems Res.* 1(3):255–276.

Straub DW, Nance WD (1990) Discovering and disciplining computer abuse in organizations: A field study. *MIS Quart.* 14(1):45–60.

Straub D, Boudreau M-C, Gefen D (2004) Validation guidelines for IS positivist research. *Comm. Assoc. Inform. Systems* (13):380–427.

Strauss AL, Corbin J (1994) *Grounded Theory Methodology: An Overview* (Sage, Thousand Oaks, CA).

Sweet SJ, Norman IJ (1995) The nurse-doctor relationship: A selective literature review. *J. Advanced Nursing* 22(1):165–170.

Sykes GM, Matza D (1957) Techniques of neutralization: A theory of delinquency. *Amer. Sociol. Rev.* 22(6):664–670.

Trevino LK (1992) Experimental approaches to studying ethical-unethical behavior in organizations. *Bus. Ethics Quart.* 2(2):121–136.

Tuunanen T, Kuo IT (2015) The effect of culture on requirements: a value-based view of prioritization. *Eur. J. Inform. Systems* 24(3):295–313.

Ugrin JC, Pearson JM, Odom MD (2007) Profiling cyber-slackers in the workplace: Demographic, cultural, and workplace factors. *J. Internet Commerce* 6(3):75–89.

U.S. Department of Health and Human Services (2018a) Anthem pays OCR $16 million in record HIPAA settlement following largest U.S. health data breach in history. Accessed May 2, 2020, https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html.

U.S. Department of Health and Human Services (2018b) Federal register. Accessed May 2, 2020, https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

U.S. Department of Health and Human Services (2020) U.S. Department of Health and Human Services Office for Civil Rights. Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. Accessed June 6, 2020, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Vance A, Benjamin Lowry P, Eggett D (2015) Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quart.* 39(2):345–366.

Vance A, Lowry PB, Eggett D (2013) Using accountability to reduce access policy violations in information systems. *J. Management Inform. Systems* 29(4):263–290.

Vance A, Siponen M, Straub D (2020) Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Inform. Management* 57(4):1–9.

Vance A, Brinton Anderson B, Brock Kirwan C, Eargle D (2014) Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *J. Assoc. Inform. Systems* 15(10):679–722.

Vance A, Jenkins JL, Anderson BB, Bjornn DK, Kirwan CB (2018) Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS. Quart.* 42(2):355–380.

Venkatesh V, Brown SA, Bala H (2013) Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quart.* 37(1):21–54.

Venkatesh V, Brown SA, Sullivan YW (2016) Guidelines for conducting mixed-methods research: An extension and illustration. *J. Assoc. Inform. Systems* 17(7):435–495.

von Meier A (1999) Occupational cultures as a challenge to technological innovation. *IEEE Trans. Engrg Management* 46(1):101–114.

Vroom C, von Solms R (2004) Toward information security behavioural compliance. *Comput. Security* 23(3):191–198.

Wallander L (2009) 25 Years of factorial surveys in sociology: A review. *Soc. Sci. Res.* 38(3):505–520.

Walsham G (1995) Interpretive case studies in IS research: Nature and method. *Eur. J. Inform. Systems* 4(2):74–81.

Walsham G (2006) Doing interpretive research. *Eur. J. Inform. Systems* 15(3):320–330.

Weber J (1992) Scenarios in business ethics research: Review, critical assessment, and recommendations. *Bus. Ethics Quart.* 2(2): 137–160.

West M, Topakas A, Dawson J (2014) Climate and culture for healthcare performance. Barbera KM, ed. *The Oxford Handbook of Organizational Climate and Culture* (Oxford University Press, New York), 335–359.

Willison R, Warkentin M (2013) Beyond deterrence: An expanded view of employee computer abuse. *MIS Quart.* 37(1): 1–20.

Workman M, Bommer WH, Straub D (2008) Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Human Behavior* 24(6): 2799–2816.