Organizational Cybersecurity Journal: Practice, Process and People

19

Employees are not the weakest link: an occupational safety view of information security

Alan R. Dennis
Kelley School of Business, Indiana University, Bloomington, Indiana, USA

Received 2 June 2023
Revised 16 December 2023
Accepted 13 April 2024

Abstract

Purpose – I adapt the Integrated Model of Workplace Safety (Christian *et al.*, 2009) to information security and highlight the need to understand additional factors that influence security compliance and additional security outcomes that need to be studied (i.e. security participation).

Research limitations/implications – This model argues that distal factors in four major categories (employee characteristics, job characteristics, workgroup characteristics and organizational characteristics) influence two proximal factors (security motivation and security knowledge) and the security event itself, which together influence two important outcomes (security compliance and security participation).

Practical implications – Safety is a systems design issue, not an employee compliance issue. When employees make poor safety decisions, it is not the employee who is at fault; instead, the system is at fault because it induced the employee to make a poor decision and enabled the decision to have negative consequences.

Social implications – Security compliance is as much a workgroup issue as an individual issue.

Originality/value – I believe that by reframing information security from a compliance issue to a systems design issue, we can dramatically improve security.

Keywords Safety, Security, Security participation, Employee characteristics, Job characteristics, Workgroup characteristics, Organizational characteristics

Paper type Conceptual paper

Introduction

Information security remains a critical issue facing information systems managers (Cram *et al.*, 2020; Kappelman *et al.*, 2022), with losses from security breaches continuing to increase (EY, 2020; PWC, 2022). Several industry studies have concluded that employee behavior is the largest single root cause of security breaches, and most often, it is *not* deliberate malfeasance that causes breaches but rather a failure to comply with security policies without malicious intent (EY, 2020; PWC, 2022). It is often said that employees are the weakest link in information security (Bernard, 2023; Chalico, 2022; Harbert, 2021).

In this paper, I argue that one reason information security remains a critical issue is *because* we view employees as the weakest link. To make major improvements in information security, we need to make major changes in how we view the root cause of information security problems. In the early 20th century, one measure of the success of construction projects was the number of employees killed or injured; employees were viewed as the source of industrial accidents and it was expected that many would be killed or injured on major construction projects because they failed to comply with good safety practices (Pérezgonzález, 2005). Today, we understand that occupational safety is a systems design

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 4 No. 1, 2024
pp. 19-31
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-06-2023-0013

issue, not an employee compliance issue (Manuele, 2008; Michaels, 2018; Pérezgonzález, 2005). When an employee makes an unsafe choice and is injured, it is *not* the employee who is at fault; instead, the system is at fault because it induced the employee to make a poor decision and enabled the decision to have negative consequences. This shift in understanding has led to profound improvements in safety in many countries and industries (Pérezgonzález, 2005).

I argue that we need to make this same shift in our approach to information security. I argue that we need to stop viewing information security as an employee compliance problem and instead view security as a systems problem. This means adopting a security by design perspective (cf. Manuele, 2008), in which security is viewed as a system design issue so that the system inhibits employees from making poor decisions that have negative consequences. I adapt the Integrated Model of Workplace Safety (IMWS) (Christian *et al.*, 2009) to information security and highlight the need to understand additional factors that influence security and additional security outcomes that need to be studied. I also present several implications for security practice.

Information security as a safety practice

Information security research has used a variety of different theoretical lenses, including theories from public health, criminology and psychology (Moody *et al.*, 2018). Many of these theories are based on extrinsic motivation using threats, sanctions and negative consequences in an attempt to deter undesirable behaviors (Moody *et al.*, 2018), although some research has begun to consider more positive approaches (Jensen *et al.*, 2020; Silic and Lowry, 2020). In this paper, I use the lens of occupational safety to develop theoretical and practical implications for information security.

There are many parallels between safety and security. Like safety (Dov, 2008; Humphrey *et al.*, 2004; Michaels, 2018; Zohar, 2003), information security is an additional job responsibility requiring specific knowledge that must be prioritized among a host of responsibilities competing for employees' time (Beautement *et al.*, 2014; D'Arcy *et al.*, 2014). Employees often deal with competing operational demands. For example, in manufacturing, production speed often competes with safety so managers have to balance these competing priorities (Humphrey *et al.*, 2004). Job pressure is a key factor influencing safety compliance (Christian *et al.*, 2009), so it may also influence security compliance because security is similar to safety compliance—an additional responsibility that must be balanced and prioritized among a host of responsibilities competing for the employee's time and attention (Beautement *et al.*, 2014; D'Arcy *et al.*, 2014). Security tasks can interfere with job responsibilities (Bulgurcu *et al.*, 2010), so employees balance them against job priorities.

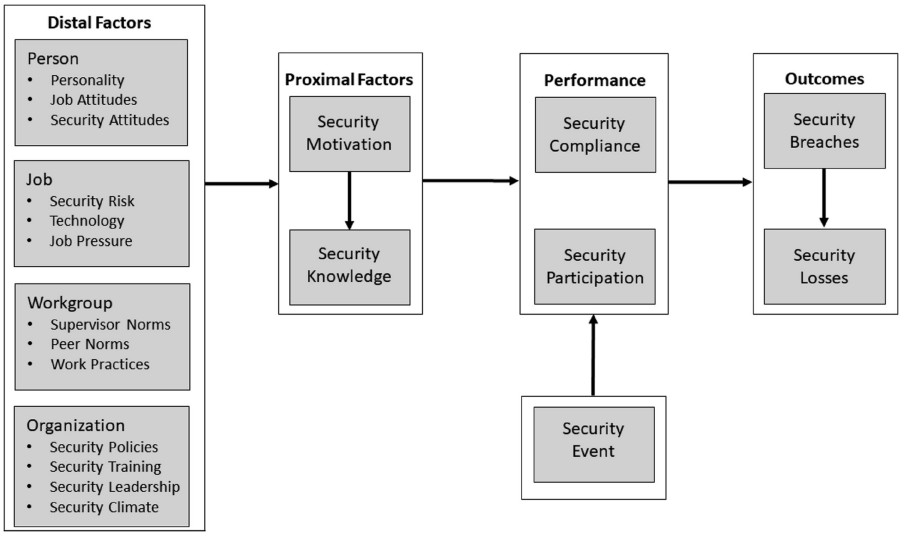
Like safety (Basahel, 2021; Cornelissen *et al.*, 2014; Ford and Tetrick, 2008; Griffin and Neal, 2000; Neal *et al.*, 2000; Saari, 1990), security success is achieved through the non-occurrence of incidents. Unlike other job tasks where success is visible through some accomplishment (e.g. winning a contract, or launching a product), security success has few visible accomplishments. For example, preventing an intrusion by setting strong passwords or installing software updates will not be noticed by users.

Safety research and advice to safety practitioners have long viewed safety compliance as a function of knowledge and motivation (Basahel, 2021; Cornelissen *et al.*, 2014; Ford and Tetrick, 2008; Griffin and Neal, 2000; Neal *et al.*, 2000; Saari, 1990). Information security researchers have also begun to recognize the importance of security knowledge and security motivation (Crossler and Bélanger, 2019). Knowledge is necessary, because security requires the knowledge to act (Chen *et al.*, 2018; Cram *et al.*, 2019; Ifinedo, 2022; Silic and Lowry, 2020). Motivation is important because knowledge alone is not sufficient to actually perform the tasks (Lebek *et al.*, 2014; Lowry *et al.*, 2015; Menard *et al.*, 2017). Education and training providing security knowledge is widespread in organizations (EY, 2020; PWC, 2022), and

extensive research shows that it has a modest effect on security compliance (Cram *et al.*, 2019). In contrast, less organizational effort and research attention have addressed security motivation (Boss *et al.*, 2009; Lebek *et al.*, 2014; Menard *et al.*, 2017). Research in occupational safety indicates that safety compliance depends as much on motivation as knowledge and that motivation is central to the acquisition of knowledge (Basahel, 2021; Christian *et al.*, 2009; Cornelissen *et al.*, 2014; Neal *et al.*, 2000; Saari, 1990).

Information security behavior is a function of multiple factors, including individual differences and the situational context (Cram *et al.*, 2019). Research on workplace safety has long focused on the effects of two fundamental individual differences: safety knowledge and safety motivation (Basahel, 2021; Cornelissen *et al.*, 2014; Neal *et al.*, 2000; Saari, 1990). The IMWS is based on the theoretical safety model of Neal *et al.* (2000) and uses a meta-analysis of prior occupational safety research to identify the key factors (Christian *et al.*, 2009). The IMWS concludes that safety compliance is primarily influenced by these two proximal factors (motivation and knowledge) and that these two factors are influenced by a set of distal factors such as individual traits and organizational factors (e.g. policies, leadership, social influence and job pressure). A meta-analysis using IMWS shows that motivation and knowledge have similar-sized effects on safety compliance (Christian *et al.*, 2009). Motivation and knowledge tend to have stronger effects than the several dozen distal factors investigated, although some distal factors also have large effects (Christian *et al.*, 2009).

Figure 1 presents an adaptation of the IMWS for the study of information security. This model argues that four distal factors (e.g. the person, the job, the workgroup and the organization) influence the proximal factors of security motivation and security knowledge, which, combined with the security event, influence security compliance and security participation, which lead to breaches and losses. Many of these factors are well-known in security research (Cram *et al.*, 2019), which shows that the IMWS and its central constructs fit comfortably into the information security context. Some constructs are relatively new to information security research.



Source(s): Christian *et al.* (2009)

Figure 1.
Research model adapted from IMWS

Security performance and outcomes

The central outcome of much information security research is security compliance (Cram *et al.*, 2019). Similarly, safety research has a central focus on compliance (Christian *et al.*, 2009). But safety research has an equally important second central focus: safety participation (Christian *et al.*, 2009; Griffin and Neal, 2000; Neal *et al.*, 2000). "Safety participation involves helping coworkers, promoting the safety program within the workplace, demonstrating initiative, and putting effort into improving safety in the workplace" (Neal *et al.*, 2000, p. 101). Safety participation (Christian *et al.*, 2009; Griffin and Neal, 2000; Neal *et al.*, 2000) is similar to the advocacy component of the consumer loyalty construct (Oliver, 1999). In addition to complying with safety policies, safety participation is the advocacy of safety behaviors, similar to the advocacy of a product by loyal users (Chow and Holden, 1997; Galletta *et al.*, 2006; Kim *et al.*, 2002; Nordstrom and Swan, 1976; Oliver, 1999; Saga and Zmud, 1994; Tucker, 1964).

Thus, I argue that we need to add information security participation to the constructs we routinely study in the area of information security. I define information security participation as the advocacy of information security to others, a construct that is separate and distinct from security compliance. A loyal security employee is someone who both complies with security policies and advocates for security. Such employees are "supporting users" in the terms of van Offenbeek *et al.* (2013), they both comply with security policies and advocate for them. In contrast, a "resisting user" (one who complies with policies but does not value them) (van Offenbeek *et al.*, 2013) is not an employee loyal to information security, despite even extensive routine compliance; mandatory compliance does not constitute loyal compliance, as is compelled behavior, not loyal behavior.

There has been some security research on security breaches and the losses they have caused (e.g. Cavusoglu *et al.*, 2004; Furnell *et al.*, 2020; Gordon *et al.*, 2011; Reshmi, 2021). In general, these two outcomes have received less research attention than compliance (Cram *et al.*, 2019). Safety research suggests that motivation is at least as important as knowledge – if not more important – in reducing accidents and losses (Christian *et al.*, 2009). This suggests that we need more research on how security motivation and knowledge and security compliance and participation are linked to security breaches and losses.

Proximal factors

Security knowledge, like safety knowledge (Christian *et al.*, 2009), is a key factor in security compliance (Cram *et al.*, 2019) and companies spend millions of dollars every year on security education, training and awareness (SETA) programs to provide knowledge (EY, 2020; PWC, 2022). However, knowledge is only a modest predictor of security compliance (Cram *et al.*, 2019). From a theoretical perspective, knowledge is necessary because employees need to know what security behaviors are important and how to implement them (Cram *et al.*, 2019; Ifinedo, 2022; Silic and Lowry, 2020). Without knowledge, employees are unable to act (Cram *et al.*, 2019). SETA is an important antecedent to employee compliance with ISPs (Cram *et al.*, 2019) because it provides both security knowledge and knowledge about the ISP. Research shows that greater security knowledge increases security compliance (Al-Omari *et al.*, 2012, 2018; Bulgurcu *et al.*, 2010; Dinev and Hu, 2007; Ifinedo, 2022).

Safety motivation is a strong predictor of safety compliance and safety participation (Christian *et al.*, 2009). Information security is not an intrinsically motivating task so most users do not have a strong desire to perform it (D'Arcy *et al.*, 2014). Like safety, security is a task that competes with other tasks (Beautement *et al.*, 2014; Bulgurcu *et al.*, 2010; D'Arcy *et al.*, 2014). Individuals need to manage their limited resources so that they can focus on what they perceive to be the most important (Bulgurcu *et al.*, 2010). Information security researchers have begun to recognize the importance of motivation (Crossler and Bélanger, 2019), but research is sparse (Boss *et al.*, 2009; Lebek *et al.*, 2014; Lowry *et al.*, 2015; Menard *et al.*, 2017).

Both knowledge and motivation should be important to compliance (Christian *et al.*, 2009; Neal *et al.*, 2000). An individual must understand security and have the knowledge to perform security tasks. Interestingly, safety research shows that motivation is a key predictor in the acquisition of knowledge (Christian *et al.*, 2009), so to understand security knowledge, we need to begin with research on security motivation. Motivation should play a much stronger role in security participation than security knowledge because advocating for security does not require specific security knowledge, just a general understanding of the principles and practices, and participatory activities are voluntary, whereas compliance is generally mandated (Neal *et al.*, 2000).

One construct that is lacking in IMWS but past security research shows is important are characteristics of the security event itself (Cram *et al.*, 2019). For example, threat vulnerability and severity and response cost and efficacy from Protection Motivation Theory (Haag *et al.*, 2021). As a result, I include them in the model in Figure 1. What matters is how the individual employee understands the characteristics of the security event, which are influenced by its actual characteristics, but different individuals may have very different understandings and interpretations of the event. Individuals act on their understandings, not on the actual event characteristics that a putative "objective" third-party observer might see (James *et al.*, 1978; Pondy, 1967), so what matters are employee perceptions of the security event.

Distal factors

The IMSW argues that a set of distal factors act over time to influence the two proximal factors of safety motivation and knowledge (Christian *et al.*, 2009). I group these distal factors into four major categories: person, job, workgroup and organization.

Person. Individual differences are known to be a primary factor influencing information security decisions (Cram *et al.*, 2019). Personality is an important individual difference that can affect security decisions (Johnston *et al.*, 2016). The most commonly used model of personality is the Five Factor Model (FFM), which has five main factors: agreeableness, conscientiousness, extraversion, neuroticism (also called emotional stability) and openness to new experience (Costa and McCrae, 1992; McCrae and Costa, 1987). Safety research shows that conscientiousness matters, but other personality traits are less important (Christian *et al.*, 2009).

Security research shows that individuals high in conscientiousness are more likely to be aware of and comply with security policies (Alohali *et al.*, 2018; Gratian *et al.*, 2018; Halevi *et al.*, 2017; Johnston *et al.*, 2016; Kajzer *et al.*, 2014; McCormac *et al.*, 2017; Pattinson *et al.*, 2015; Shappie *et al.*, 2020; Shropshire and Gowan, 2017; Shropshire *et al.*, 2015; van der Schyff and Flowerd, 2021; Warkentin *et al.*, 2012; Weems *et al.*, 2019). Security research shows mixed results for the other four personality traits (Alohali *et al.*, 2018; Gratian *et al.*, 2018; Halevi *et al.*, 2013; Jaeger and Eckhardt, 2021; Johnston *et al.*, 2016; Kajzer *et al.*, 2014; McCormac *et al.*, 2017; Pattinson *et al.*, 2015; Shappie *et al.*, 2020; Shropshire and Gowan, 2017; Weems *et al.*, 2019; Welk *et al.*, 2015).

Safety research suggests two other personality traits are also important to safety compliance and thus are likely to be important for information security. The first is the locus of control, the extent to which people believe that they personally control the events in their lives as opposed to those events being beyond their control (Christian *et al.*, 2009). The second is a propensity for risk-taking – the extent to which people are impulsive sensation seekers (Christian *et al.*, 2009). Both had stronger effects than conscientiousness on safety performance (Christian *et al.*, 2009) and neither has received much research attention in information security, suggesting two promising avenues for future research.

Safety research has found two other person-specific factors to have important effects on safety compliance. The first is general job attitudes, such as job satisfaction and organizational commitment; more positive attitudes might lead to greater motivation to behave safely (Christian *et al.*, 2009). The second is safety attitudes, individual perceptions of

safety-related policies, practices and procedures pertaining to safety (Christian *et al.*, 2009). Job attitudes and security attitudes have received only a little research in information security, suggesting two promising avenues for future research.

Job. Individuals hold different job roles over their careers and different jobs influence safety motivation and knowledge (Christian *et al.*, 2009). Thus, the employee's job may also influence the motivation and knowledge of security. Different jobs present different security decisions to employees, depending on the data and information they have access to and the tasks they perform. Some job roles are critical and are widely targeted by hackers (e.g. senior managers and their direct reports), whereas other roles are not. Likewise, the technology available to employees can change their motivation to comply with security policies. For example, has the organization deployed single sign-on or cloud storage with automated backups?

One important job factor from safety that also applies to information security is job pressure (Christian *et al.*, 2009), the pressure to complete work-related tasks that are the primary responsibility of the employees, rather than associated tasks like safety and information security. When workloads are low, employees have the capacity to perform both their primary job tasks and security tasks; there are few competing priorities between job duties and security tasks. But, as the demands from primary responsibilities become stronger, competing priorities become significant and employees need to choose between tasks – and the choice becomes more difficult, especially when compliance poses a noticeable impediment to primary job productivity (Goel and Chengalur-Smith, 2010; Posey *et al.*, 2011). Practitioner surveys note that one major reason why employees report not complying with ISP is that they are too busy with other tasks (D'Arcy *et al.*, 2014).

Workgroup. The workgroups in which employees spend much of their work lives have important effects on safety behavior (Christian *et al.*, 2009). These workgroups create norms and work practices that guide how their members think about and practice safety. Information security researchers are also beginning to understand the importance of workgroup norms and practices in influencing security behaviors (Herath and Rao, 2009; Wang *et al.*, 2023; Yoo *et al.*, 2020). When attitudes are shared among individuals in a workgroup, there are social pressures to conform to the prevailing norms and adopt the work practices of other group members (Christian *et al.*, 2009). Membership in the workgroup can also be an important source of identity, so conforming to norms and practices becomes identity display behaviors (Christian *et al.*, 2009).

Organization. Security research has long studied organizational security policies and security training activities (Barlow *et al.*, 2018; Cram *et al.*, 2019; D'Arcy *et al.*, 2009; EY, 2020; Kirova and Baumöl, 2018; PWC, 2022; Straub and Nance, 1990). These are some of the few obvious direct actions that organizations can take to manage security. Research shows that they have a *modest* effect on security compliance, not strong effects (Cram *et al.*, 2019).

Two other important ways organizations can influence security are through the actions of the organization's leadership and the climate that organizational leaders create (Christian *et al.*, 2009). Information security *should be* a top concern of organizational leadership (Alassaf and Alkhalifah, 2021), but this is not always the case. Leaders motivate employees and help develop and maintain the organizational culture, which may or may not include prioritizing information security (Alassaf and Alkhalifah, 2021).

Information security climate (also called information security culture (Kessler *et al.*, 2020)) has significant effects on security compliance (Chan *et al.*, 2005; Goo *et al.*, 2014; Kessler *et al.*, 2020; Orehek and Petrič, 2021). The security climate is established by the organization's leaders and managers and influences behavior by helping to establish what is accepted and meaningful practices within the organization (Chan *et al.*, 2005). Security climate can have direct effects on compliance or may be an important distal factor that is mediated by more proximal factors (Goo *et al.*, 2014; Kessler *et al.*, 2020). Safety climate influences safety participation more than safety compliance, because of the voluntary nature of participation.

Discussion

Information security research has used theoretical lenses from public health, criminology and psychology (Moody *et al.*, 2018). In this paper, I argue that information security research can benefit by adapting theory and research from occupational safety (Basahel, 2021; Cornelissen *et al.*, 2014; Ford and Tetrick, 2008; Griffin and Neal, 2000; Neal *et al.*, 2000; Saari, 1990). The IMWS (Christian *et al.*, 2009) is likely to be particularly useful because it is based on a meta-analysis of prior safety research.

Implications for theory and research

I see four important theoretical implications from occupational safety that have the potential to reshape how we think about information security theory, research and practice. First, it suggests a new important outcome variable: security participation (the advocacy of information security behaviors). Much security research has focused on compliance (Cram *et al.*, 2019), which is also an important outcome, but the addition of security participation is important as it offers a broader understanding of information security performance; security is not just about the immediate act of compliance but also includes internalization and advocacy of security, like consumer loyalty (Oliver, 1999). A security loyalist not only complies but also advocates; someone who complies reluctantly is not a security loyalist.

Second, safety research separates the constructs that influence performance into two categories; proximal and distal. Motivation and knowledge are the two key proximal factors that influence the in-the-moment decisions of employees, with a host of other distal factors shaping these two factors. The separation of constructs into proximal and distal factors can help us sharpen information security theory (and practical actions by organizations and managers). We can focus more on how the distal factors influence security motivation and knowledge and then how motivation and knowledge influence specific security decisions.

Third, the IMWS includes four distinct sets of distal factors. The person (e.g. individual differences such as personality) and the organization (e.g. policies) have long been studied in information security (Cram *et al.*, 2019). One interesting aspect from the IMWS that has received less research attention in security research is the role of senior leadership; organizations say security is important, but how many CEOs truly provide security leadership? The other two categories have received less research attention in the security area. Security researchers are beginning to study the effects of the employee's workgroup(s) on security performance (Herath and Rao, 2009; Wang *et al.*, 2023; Yoo *et al.*, 2020), but more research is needed to better understand how workgroups develop social norms and work practices around security. Perhaps more important, is the nature of the employee's job; little research has examined job characteristics and job pressure as factors influencing security decisions.

Finally, one of the interesting differences between safety research and security research has been the focus on specific aspects of compliance/violation. Security research has focused extensively on specific security threats (Cram *et al.*, 2019), and several theories include beliefs about specific threats (e.g. threat severity and threat likelihood (Haag *et al.*, 2021)). In contrast, threat-specific factors are absent from the IMWS. This rather starkly highlights the different philosophical stances of the two streams of research: security focusing on the individual actor responding to the influence of the moment and safety research focusing more holistically on an individual within a larger ecosystem. This suggests opportunities for both research areas by reconsidering their implicit assumptions.

Implications for practice

The research model adapted from IMWS in Figure 1 offers value to practice by highlighting a larger set of factors that managers can use to influence security compliance (e.g. job and workgroup). Most organizations are focused on SETA training to provide security

knowledge as the primary means to improve the security behavior of their employees. Figure 1 shows that security motivation drives the acquisition of security knowledge, so influencing employee motivation is essential and comes before providing knowledge. Figure 1 also highlights the importance of security participation as an important practical aspect that organizations can measure and track over time.

Perhaps the most important implication for security practice that we can take from occupational safety is not clearly highlighted in Figure 1. Information security takes employee time and can be an impediment to work practices (Bulgurcu *et al.*, 2010) forcing employees to choose between security compliance and other job responsibilities (D'Arcy *et al.*, 2014). This trade-off between work and safety has long played out in manufacturing, where safety often competes with production efficiency, requiring employees to balance the two (Humphrey *et al.*, 2004; Michaels, 2018; Zohar, 2003).

Safety managers no longer see poor employee decisions as the *source* of safety problems, but rather as the *consequences* of poor safety processes (Michaels, 2018). When an employee makes a poor safety decision, the employee is not at fault (except for egregious cases). Instead, the primary cause of the safety violation is a poorly designed workplace ecosystem that induced an employee to make a poor decision and permitted that decision to have consequences (Manuele, 2008; Michaels, 2018; Pérezgonzález, 2005). This shift in understanding and the move to design safety in workplace ecosystems (Manuele, 2008) has dramatically improved safety (Pérezgonzález, 2005).

We need to stop thinking of employees as a *source* of security problems and instead recognize that employee behavior is a *consequence* of the ecosystem in which they work (e.g. business processes, technology, social systems). When a security breach occurs, it is likely a result of a poorly designed workplace ecosystem that induced an employee to make a poor security decision and permitted that decision to have consequences. When an individual fails to comply with security policy, it is not an individual failure; it is a *system* failure and indicates that the system needs to be redesigned, not that the employee needs to be disciplined. We need to redesign workplace business processes and information systems to design security into the systems and procedures to prevent employees from making poor decisions and prevent those decisions from having consequences.

For example, phishing has been a major source of security breaches; we know that employees will click on phishing links. Therefore, we need to change the ecosystem so that clicking on phishing links has few security consequences. For example, we can change Web browser technology so that if an employee visits a fake Web site masquerading as an organizational website (or their bank), the browser can recognize this because the employee has never logged into the Web site before. Password managers (both third-party and those integrated into web browsers) routinely save and track websites where the user has previously logged in, so it would be simple to extend this functionality to vividly display warning information when an employee attempts to login to a website they have never visited before (thereby warning employees this is not their normal site). Microsoft recently implemented a new feature in Outlook that flags emails from users you do not commonly receive emails from in an attempt to help users separate phishing emails from emails from firms they deal with regularly (e.g. their bank). The intent and explanation of this is not clear, but it is a good first step to building phishing security into the technology. Likewise, many firms are beginning to change their websites to eliminate passwords by emailing users links to login, so phishing has no consequences.

Conclusion

In summary, I argue that occupational safety is a useful reference discipline for information security research. By adapting theory and research from safety into our security research, we can

develop better theories of information security. We can also improve security practices by adapting the perspective from the safety that individual employees are not the source of information security breaches, but rather the real culprit is workplace ecosystems that induce employees to make poor security decisions and permit those decisions to have negative consequences.

References

Al-Omari, A., El-Gayar, O. and Deokar, A. (2012), "Information security policy compliance: the role of information security awareness", *Americas Conference on Information Systems*, Seattle.

Al-Omari, A., El-Gayar, O. and Deokar, A. (2018), "Security policy compliance: user acceptance perspective", *Hawaii International Conference on System Sciences*, Maui.

Alassaf, M. and Alkhalifah, A. (2021), "Exploring the influence of direct and indirect factors on information security policy compliance: a systematic literature review", *IEEE Access*, Vol. 9, pp. 162687-162705, doi: 10.1109/ACCESS.2021.3132574.

Alohali, M., Clarke, N., Li, F. and Furnell, S. (2018), "Identifying and predicting the factors affecting end-users risk-taking behavior", *Information and Computer Security*, Vol. 26 No. 3, pp. 306-326, doi: 10.1108/ICS-03-2018-0037.

Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2018), "Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance", *Journal of the Association for Information Systems*, Vol. 19 No. 8, pp. 3-715, doi: 10.17705/1jais.00506.

Basahel, A.M. (2021), "Safety leadership, safety attitudes, safety knowledge and motivation toward safety-related behaviors in electrical substation construction projects", *International Journal of Environmental Research and Public Health*, Vol. 18 No. 8, p. 4196, doi: 10.3390/ijerph18084196.

Beautement, A., Sasse, M.A. and Wonham, M. (2014), *The Compliance Budget: Managing Security Behaviour in Organisations*, New Security Paradigms Workshop, Lake Tahoe CA.

Bernard, A. (2023), "Humans still weakest link in cybersecurity", available at: https://www.techrepublic.com/article/humans-weakest-link-cybersecurity/

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 151-164, doi: 10.1057/ejis.2009.8.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Q*, Vol. 34 No. 3, pp. 523-548, doi: 10.2307/25750690.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers", *International Journal of Electronic Commerce*, Vol. 9 No. 1, pp. 70-104, doi: 10.1080/10864415.2004.11044320.

Chalico, C.P. (2022), "Your employees are the weakest link in your cybersecurity chain", available at: https://www.ey.com/en_ca/cybersecurity/your-employees-are-the-weakest-link-in-your-cybersecurity-chain

Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security in the workplace: linking information security climate to compliant behavior", *Journal of Information Privacy and Security*, Vol. 1 No. 3, pp. 18-41, doi: 10.1080/15536548.2005.10855772.

Chen, X., Chen, L. and Wu, D. (2018), "Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective", *Journal of Computer Information Systems*, Vol. 58 No. 4, pp. 312-324, doi: 10.1080/08874417.2016.1258679.

Chow, S. and Holden, R. (1997), "Toward an understanding of loyalty: the moderating role of trust", *Journal of Managerial Issues*, Vol. 9 No. 3, pp. 275-298.

Christian, M.S., Bradley, J.C., Wallace, J.C. and Burke, M.J. (2009), "Workplace safety: a meta-analysis of the roles of person and situation factors", *Journal of Applied Psychology*, Vol. 94 No. 5, pp. 1103-1127, doi: 10.1037/a0016172.

Cornelissen, P.A., van Hoof, J.J. and van Vuuren, M. (2014), "Enabling employees to work safely: the influence of motivation and ability in the design of safety instructions", *Technical Communication*, Vol. 61 No. 4, pp. 232-244.

Costa, P.T. and McCrae, R.R. (1992), "Revised NEO personality inventory (NEO-PR-I)", in Boyle, G.J., Matthews, G. and Saklofske, D.H. (Eds), *The SAGE Handbook of Personality Theory and Assessment*, Sage, Vol. 2, pp. 179-198.

Cram, A.W., D'Arcy, J. and Proudfoot, J.G. (2019), "Seeing the forest and the trees: a meta-analysis of the antecedents to information security polict compliance", *MIS Quarterly*, Vol. 43 No. 2, pp. 525-554, doi: 10.25300/misq/2019/15117.

Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2020), "Maximizing employee compliance with cybersecurity policies", *MIS Quarterly Executive*, Vol. 19 No. 1, pp. 183-198, doi: 10.17705/2msqe.00032.

Crossler, R.E. and Bélanger, F. (2019), "Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap", *Information Systems Research*, Vol. 30 No. 3, pp. 1047-7047, doi: 10.1287/isre.2019.0846.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: 10.1287/isre.1070.0160.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285-318, doi: 10.2753/MIS0742-1222310210.

Dinev, T. and Hu, Q. (2007), "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of the AIS*, Vol. 9 No. 7, pp. 386-408, doi: 10.17705/1jais.00133.

Dov, Z. (2008), "Safety climate and beyond: a multi-level multi-climate framework", *Safety Science*, Vol. 46 No. 3, pp. 376-387, doi: 10.1016/j.ssci.2007.03.006.

EY (2020), *Global Information Security Survey*, available at: www.ey.com/GISS (accessed 2 Febrauary 2021).

Ford, M.T. and Tetrick, L.E. (2008), "Safety motivation and human resource management in North America", *The International Journal of Human Resource Management*, Vol. 19 No. 8, pp. 1472-1485, doi: 10.1080/09585190802200231.

Furnell, S., Heyburn, H., Whitehead, A. and Shah, J.N. (2020), "Understanding the full cost of cyber security breaches", *Computer Fraud and Security*, Vol. 12, pp. 30127-30135.

Galletta, D.F., Henry, R.M., McCoy, S. and Polak, P. (2006), "When the wait isn't so bad: the interacting effects of website delay, familiarity, and breadth", *Information Systems Research*, Vol. 17 No. 1, pp. 20-37, doi: 10.1287/isre.1050.0073.

Goel, S. and Chengalur-Smith, I.N. (2010), "Metrics for characterizing the form of security policies", *Journal of Strategic Information Systems*, Vol. 19 No. 4, pp. 281-295, doi: 10.1016/j.jsis.2010.10.002.

Goo, J., Yim, M.S. and Kim, D.J. (2014), "A path to successful management of employee security compliance: an empirical study of information security climate", *IEEE Transactions on Professional Communication*, Vol. 57 No. 4, pp. 286-308, doi: 10.1109/TPC.2014.2374011.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2011), "The impact of information security breaches: has there been a downward shift in costs?", *Journal of Computer Security*, Vol. 19 No. 1, pp. 33-56, doi: 10.3233/jcs-2009-0398.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018), "Correlating human traits and cyber security behavior intentions", *Computers and Security*, Vol. 73, pp. 345-358, doi: 10.1016/j.cose.2017.11.015.

Griffin, M.A. and Neal, A. (2000), "Perceptions of safety at work: a framework for linking safety climate to safety performance, knowledge, and motivation", *Journal of Occupational Health Psychology*, Vol. 5 No. 3, pp. 347-358, doi: 10.1037/1076-8998.5.3.347.

Haag, S., Siponen, M. and Liu, F. (2021), "Protection motivation theory in information systems security research: a review of the past and a road map for the future", *SIGMIS Database*, Vol. 52 No. 2, pp. 25-67, doi: 10.1145/3462766.3462770.

Halevi, T., Lewis, J. and Memon, N. (2013), "A pilot study of cyber security and privacy related behavior and personality traits", *Proceedings of the 22nd International Conference on World Wide Web*. doi: 10.1145/2487788.2488034.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F. and Chen, J. (2017), "Cultural and psychological factors in cyber-security", *Journal of Mobile Multimedia*, Vol. 13 Nos 1 and 2, pp. 43-56.

Harbert, T. (2021), "The weakest link in cybersecurity", available at: https://www.shrm.org/hr-today/news/all-things-work/pages/the-weakest-link-in-cybersecurity.aspx

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125, doi: 10.1057/ejis.2009.6.

Humphrey, S.E., Moon, H., Conlon, D.E. and Hofmann, D.A. (2004), "Decision-making and behavior fluidity: how focus on completion and emphasis on safety changes over the course of projects", *Organizational Behavior and Human Decision Processes*, Vol. 93 No. 1, pp. 14-27, doi: 10.1016/j.obhdp.2003.08.003.

Ifinedo, P. (2022), "Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors", *Journal of Computer Information Systems*, Vol. 63 No. 2, pp. 380-396, doi: 10.1080/08874417.2022.2065553.

Jaeger, L. and Eckhardt, A. (2021), "Eyes wide open: the role of situational information security awareness for security-related behaviour", *Information Systems Journal*, Vol. 31 No. 3, pp. 429-472, doi: 10.1111/isj.12317.

James, L.R., Hater, J.J., Gent, M.J. and Bruni, J.R. (1978), "Psychological climate: implications from cognitive social learning theory and interactional psychology", *Personnel Psychology*, Vol. 31 No. 4, pp. 783-813, doi: 10.1111/j.1744-6570.1978.tb02124.x.

Jensen, M.L., Wright, R.T., Durcikova, A. and Karumbaiah, S. (2020), "Improving phishing reporting using security gamification", *Journal of Management Information Systems*, Vol. 39 No. 3, pp. 793-823, doi: 10.1080/07421222.2022.2096551.

Johnston, A.C., Warkentin, M., McBride, M. and Carter, L. (2016), "Dispositional and situational factors: influences on information security policy violations", *European Journal of Information Systems*, Vol. 25 No. 3, pp. 231-251, doi: 10.1057/ejis.2015.15.

Kajzer, M., D'Arcy, J., Crowell, C.R., Striegel, A. and Bruggen, D.V. (2014), "An exploratory investigation of message-person congruence in information security awareness campaigns", *Computers and Security*, Vol. 43, pp. 64-76, doi: 10.1016/j.cose.2014.03.003.

Kappelman, L., Torres, R., McLean, E.R., Maurer, C., Johnson, V.L., Snyder, M. and Guerra, K. (2022), "The 2021 SIM IT issues and trends study", *MIS Quarterly Executive*, Vol. 21 No. 1, pp. 75-114, doi: 10.17705/2msqe.00060.

Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A. and Spector, P.E. (2020), "Information security climate and the assessment of information security risk among healthcare employees", *Health Informatics Journal*, Vol. 26 No. 1, pp. 461-473, doi: 10.1177/1460458219832048.

Kim, J., Forsyth, S., Gu, Q. and Moon, S. (2002), "Cross-cultural consumer values needs and purchase behavior", *The Journal of Consumer Marketing*, Vol. 19 No. 6, pp. 481-502, doi: 10.1108/07363760210444869.

Kirova, D. and Baumöl, U. (2018), "Factors that affect the success of security education, training, and awareness programs: a literature review", *Journal of Information Technology Theory and Application*, Vol. 19 No. 4, pp. 56-82.

Lebek, B., Guhr, N. and Breitner, M.H. (2014), *Transformational Leadership And Employees' Information Security Performance: the Mediating Role of Motivation and Climate*, International Conference on Information Systems, Auckland.

Lowry, P.B., Posey, C., Bennett, R.J. and Roberts, T.L. (2015), "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust", *Information Systems Journal*, Vol. 25 No. 3, pp. 193-230, doi: 10.1111/isj.12063.

Manuele, F.A. (2008), "Prevention through design (PtD): history and future", *Journal of Safety Research*, Vol. 39 No. 2, pp. 127-130, doi: 10.1016/j.jsr.2008.02.019.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017), "Individual differences and information security awareness", *Computers in Human Behavior*, Vol. 69, pp. 151-156, doi: 10.1016/j.chb.2016.11.065.

McCrae, R.R. and Costa, P.T. (1987), "Validation of the Five-Factor Model of personality across instruments and observers", *Journal of Personality and Social Psychology*, Vol. 52 No. 1, pp. 81-90, doi: 10.1037/0022-3514.52.1.81.

Menard, P., Bott, G.J. and Crossler, R.E. (2017), "User motivations in protecting information security: protection motivation theory versus self-determination theory", *Journal of Management Information Systems*, Vol. 34 No. 4, pp. 1203-1230, doi: 10.1080/07421222.2017.1394083.

Michaels, D. (2018), "7 ways to improve operations without sacrificing worker safety", *Harvard Business Review*, available at: https://hbr.org/2018/03/7-ways-to-improve-operations-without-sacrificing-worker-safety

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward A unified model of information security policy compliance", *MIS Quarterly*, Vol. 42 No. 1, pp. 285-A222, doi: 10.25300/misq/2018/13853.

Neal, A., Griffin, M.A. and Hart, P.M. (2000), "The impact of organizational climate on safety climate and individual behavior", *Safety Science*, Vol. 34 Nos 1-3, pp. 99-109, doi: 10.1016/s0925-7535(00)00008-4.

Nordstrom, R. and Swan, J. (1976), "Does a change in customer loyalty occur when a new car agency is sold?", *Journal of Marketing Research*, Vol. 13 No. 2, pp. 173-177, doi: 10.2307/3150854.

Oliver, R. (1999), "From where consumer loyalty", *Journal of Marketing*, Vol. 63 No. 4_suppl1, pp. 33-44, doi: 10.1177/00222429990634s105.

Orehek, Š. and Petrič, G. (2021), "A systematic review of scales for measuring information security culture", *Information and Computer Security*, Vol. 29 No. 1, pp. 133-158, doi: 10.1108/ics-12-2019-0140.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. and Calic, D. (2015), "Factors that influence information security behavior: an Australian web-based study", in Tryfonas, T. and Askoxylakis, I. (Eds), *Human Aspects of Information Security, Privacy, and Trust*, Vol. 9190, pp. 231-241, doi: 10.1007/978-3-319-20376-8_21.

Pérezgonzález, J.D. (2005), *Construction Safety Management, A Systems Approach*, The Author, New York.

Pondy, L.R. (1967), "Organizational conflict: concepts and models", *Administrative Science Quarterly*, Vol. 12 No. 2, pp. 296-320, doi: 10.2307/2391553.

Posey, C., Bennett, R.J. and Roberts, T.L. (2011), "Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes", *Computers and Security*, Vol. 30 No. 6, pp. 486-497, doi: 10.1016/j.cose.2011.05.002.

PWC (2022), *2022 Global Digital Trust Insights*, available at: https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights.html (accessed 7 January 2022).

Reshmi, T.R. (2021), "Information security breaches due to ransomware attacks - a systematic literature review", *International Journal of Information Management Data Insights*, Vol. 1 No. 2, 100013, doi: 10.1016/j.jjimei.2021.100013.

Saari, J. (1990), "On strategies and methods in company safety work: from informational to motivational strategies", *Journal of Occupational Accidents*, Vol. 12 Nos 1-3, pp. 107-117, doi: 10.1016/0376-6349(90)90081-6.

Saga, V. and Zmud, R.W. (1994), "The nature and determinants of information technology acceptance, routinization and infusion", in Levine, L. (Ed.), *Diffusion, Transfer and Implementation of Information Technology*, North-Holland, pp. 67-86.

Shappie, A.T., Dawson, C.A. and Debb, S.M. (2020), "Personality as a predictor of cybersecurity behavior", *Psychology of Popular Media Culture*, Vol. 9 No. 4, pp. 475-480, doi: 10.1037/ppm0000247.

Shropshire, J. and Gowan, A. (2017), "Identifying traits and values of top-performing information security personnel", *Journal of Computer Information Systems*, Vol. 57 No. 3, pp. 258-268, doi: 10.1080/08874417.2016.1184026.

Shropshire, J., Warkentin, M. and Sharma, S. (2015), "Personality, attitudes, and intentions: predicting initial adoption of information security behavior", *Computers and Security*, Vol. 49, pp. 177-191, doi: 10.1016/j.cose.2015.01.002.

Silic, M. and Lowry, P.B. (2020), "Using design-science based gamification to improve organizational security training and compliance", *Journal of Management Information Systems*, Vol. 37 No. 1, pp. 129-161, doi: 10.1080/07421222.2019.1705512.

Straub, D.W. and Nance, W.D. (1990), "Discovering and disciplining computer abuse in organizations: a field study", *MIS Quarterly*, Vol. 14 No. 1, pp. 45-60, doi: 10.2307/249307.

Tucker, W. (1964), "The development of brand Loyalty", *Journal of Marketing Research*, Vol. 1 No. 3, pp. 32-35, doi: 10.1177/002224376400100304.

van der Schyff, K. and Flowerd, S. (2021), "Mediating effects of information security awareness", *Computers and Security*, Vol. 106, 102313, doi: 10.1016/j.cose.2021.102313.

van Offenbeek, M., Boonstra, A. and Seo, D. (2013), "Towards integrating acceptance and resistance research: evidence from a telecare case study [Article]", *European Journal of Information Systems*, Vol. 22 No. 4, pp. 434-454, doi: 10.1057/ejis.2012.29.

Wang, D., Durcikova, A. and Dennis, A.R. (2023), "Security is local: the influence of immediate workgroup on information security", *Journal of the Association for Information Systems*, Vol. 24 No. 4, pp. 1052-1101, doi: 10.17705/1jais.00812.

Warkentin, M., McBride, M., Carter, L., and Johnston, A. (2012), "The role of individual characteristics on insider abuse intentions. AMCIS".

Weems, C.F., Ahmed, I., Richard, G.G., Russell, J.D. and Neill, E.L. (2019), "Susceptibility and resilience to cyber threat: findings from a scenario decision program to measure secure and insecure computing behavior", *PLoS ONE*, Vol. 13 No. 12, e0207408, doi: 10.1371/journal.pone.0207408.

Welk, A.K., Hong, K.W., Zielinska, O.A., Tembe, R., Murphy-Hill, E. and Mayhorn, C.B. (2015), "Will the 'Phisher-Men' Reel You In? Assessing individual differences in a phishing detection task", *International Journal of Cyber Behavior, Psychology and Learning*, Vol. 5 No. 4, pp. 1-17, doi: 10.4018/ijcbpl.2015100101.

Yoo, C.W., Goo, J. and Rao, H.R. (2020), "Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness", *Mis Quarterly*, Vol. 44 No. 2, pp. 907-931, doi: 10.25300/MISQ/2020/15477.

Zohar, D. and Luria, G. (2003), "The use of supervisory practices as leverage to improve safety behavior: a cross-level intervention model", *Journal of Safety Research*, Vol. 34 No. 5, pp. 567-577, doi: 10.1016/j.jsr.2003.05.006.

Corresponding author
Alan R. Dennis can be contacted at: ardennis@iu.edu