An Examination of How Security-Related Stress, Burnout, and Accountability Design Features Affect Security Operations Decisions

Early stage paper

Mary Grace Kozuch
The University of Texas
at Dallas
mary.kozuch@utdallas.edu

Adam Hooker
The University of Texas
at San Antonio
adam.hooker@my.utsa.edu

Philip Menard
The University of Texas
at San Antonio
philip.menard@utsa.edu

Tien N. Nguyen
The University of Texas
at Dallas
tien.n.nguyen@utdallas.edu

Raymond Choo
The University of Texas
at San Antonio
raymond.choo@utsa.edu

ABSTRACT

Security analysts are under increased pressure to perform protective activities for organizations. Even in contexts where analysts are assisted by artificial intelligence, increased pressure is placed on analysts to successfully perform their duties, including the competing efforts of balancing the protection of organizational information security and ensuring information privacy of consumers. Although system accountability features are shown to improve security behaviors among employees, contextual and external pressures could affect the influence of such features. Security-related stress (SRS) and burnout may also contribute to the perceived demands on security analysts in modern threat landscapes. In this manuscript, we propose a study where we examine the competing forces that may influence the decision-making capabilities of a security analyst working as a "human-in-the-loop" within an AI-enhanced security system. We will use the factorial survey method and multilevel analysis to detect the potential effects of accountability, threat severity and probability, and data sensitivity at the situational, decision-making level, as well as the influence exerted by SRS and burnout at the employee level. We also discuss potential implications of our work.

Keywords

Security-related stress, burnout, accountability, human-in-the-loop

INTRODUCTION

As the diversity and number of Internet of Things (IoT) systems and devices increase in our interconnected cyber-physical society, so will the number and frequency of cyberattacks on our cyber-infrastructure. IoT devices, such as smart home devices (e.g., Ring cameras) and industrial control systems (referred to as industrial IoT (IIoT) devices), are generally capable of capturing a broad range of information. Advanced persistent threats (APTs) are becoming even more prevalent and sophisticated, chiefly due to the increasing number of low-level pathways into a system though IoT devices that are not adequately secure (Menard & Bott, 2020). To combat the highly evolved threat landscape, advanced security countermeasures that incorporate artificial intelligence (AI) or machine learning (ML) are needed for adequate cyber defense. Such systems can automate low-level security analysis and identify anomalous patterns indicative of an imminent threat. While high-powered computing can assist with analysis, human security operators are still needed for conducting further analysis and making decisions based on security system outputs and recommendations. This type of employee is sometimes referred to as a "human-in-the-loop," meaning that rather than relying completely on AI in a closed-loop, organizations ensure that a human is always involved in some level of decision making within the system.

Although AI/ML-enhanced security systems should in theory ease the demands placed on security analysts, various factors could lead to increased pressure on security analysts operating in a human-in-the-loop capacity. One such unintended consequence is the potential for ML-based privacy leakages. In several privacy violation cases, plaintiff consumers have alleged that technology companies have illegally obtained, used, or shared personal biometric identifiers (e.g., fingerprints, voiceprints, and retinal/facial scans) without consent in violation of privacy laws. Illinois state and federal courts, e.g., have sustained some of these claims and approved settlements (see *Rivera v. Google, Inc., 366 F. Supp. 3d 998 (N.D. Ill. 2018)* (Illman, 2017); *Sekura v.~L.A.~Tan Enterprises, Inc., No. 2015-CH-16694 (Ill. Cir. Ct. Cook Cty.) First Amended Class Complaint filed Apr. 8, 2016)* (Neuburger, 2016)).

Additionally, a security analyst must consider varying privacy regulations enacted by global governments. For example, the European Union's (EU) General Data Protection Regulation (GDPR) introduces new privacy considerations for investigations related to EU citizens beyond physical national borders, such that their private data is protected even if the database systems storing the data are physically located outside of the EU. There may be situations that require a security analyst to investigate a threat within systems where personally identifiable information (PII) has either been stored or has been processed by ML algorithms for prediction refinement. The result of security-based threat exploration could actually expose PII further than the scope stated in an organization's privacy policy. This context highlights the types of pressures experienced by security analysts in modern security situations.

The considerations described above may present a security analyst with a potentially stressful work environment susceptible to burnout over time. As such, researchers have called for more examination of the specific demands placed on security professionals (Singh et al., 2023). Relatedly, researchers recommend the inclusion of an IT artifact as a focal point technostress-related theoretical adaptations (Muzumdar et al., 2023). A prominent design-based theory recently adapted for information security contexts is accountability theory (Vance et al., 2013), which posits that certain system design features (identifiability, monitoring awareness, evaluation awareness, and social presence) will encourage better security compliance. These features are common in AI-enhanced security systems; therefore, the human-in-the-loop security context is an ideal domain for assessing the effects of stress, burnout, accountability features, and situationally specific security demands in modern security environments. In addition to the features highlighted by accountability theory, we specify key factors that may influence the decision-making of a human-in-the-loop security analyst – an employee's explicit awareness of an information privacy policy, the oversight provided by organizational legal counsel, the severity and probability of a detected threat, and the level of sensitivity of the private data at risk by examining the threat within the system. Our study is positioned to explore this emerging phenomenon by answering the following research questions:

RQ1: How do accountability-based design features in an AI/ML security implementation influence analysts' security and privacy decisions?

RQ2: How do security-related stress and burnout interact with system design features to influence analysts' security and privacy decisions?

In the remainder of the manuscript, we will review the relevant literature related to our research context and develop the hypotheses presented in our research model. We will then propose our intended research methods and statistical analyses. Finally, we will discuss the potential implications of exploring this phenomenon.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Accountability Theory

To build the arguments within our research model, we must first understand how users' perceptions of specific system features can lead to their perception of increased user accountability within the systems and, ultimately, to their intention to not comply with organizational ISPs. Based on the Vance et al. (2013) adaptation of Accountability Theory to the IS domain, accountability perceptions are formed by four IS design artifacts – identifiability, monitoring, evaluation, and social presence.

Identifiability is defined as one's "knowledge that his outputs could be linked to him" (Williams et al., 1981, p. 309). Identifiability fosters perceptions of accountability because it emphasizes that a person's behaviors can be attributed to him or her (Lerner & Tetlock, 1999). When an individual perceives that his or her actions are identifiable, the individual is more prone to perform actions for which he or she would take responsibility. Therefore, implementing identifiability features in security situations should result in elevated perceptions of accountability among users.

H1a: Identifiability will negatively affect non-compliance intention.

Monitoring is recording someone's actions (Boss et al., 2009; Griffith, 1993). In the information security domain, monitoring has increased policy compliance (Boss et al., 2009; Herath & Rao, 2009). However, monitoring is only helpful as a compliance mechanism when details of how monitoring occurs are articulated in the ISP (Boss et al., 2009; Kirsch & Boss, 2007). Therefore, if an employee is aware of the monitoring features built into their organizational systems, they will be less likely to violate policies related to information access.

H1b: Monitoring will negatively affect non-compliance intention.

Evaluation is one's awareness that performance will be reviewed based on preconceived norms, implicitly resulting in consequences (Lerner & Tetlock, 1999). Awareness of evaluation leads to the performance of more socially acceptable behaviors (Hochwarter et al., 2007; Lerner & Tetlock, 1999) and fewer unacceptable actions (Sedikides et al., 2002). This behavioral change occurs due to evaluation apprehension, which is the anxiety associated with the approval or disapproval of one's actions as judged by others (Geen, 1991). When experiencing evaluation apprehension, one's self-awareness is elevated such that incongruencies between socially acceptable standards and one's behaviors are emphasized (Sedikides et al., 2002). In such a state, an individual will perform behaviors that match social norms and avoid actions that would damage his or her social standing (Baumeister, 1982).

H1c: Evaluation awareness will negatively affect non-compliance intention.

Social presence is the knowledge of others' presence in computer-mediated situations (Rice, 1993; Walther, 1992). Although social presence was originally conceptualized around active and consistently engaged communication (Rice, 1993; Walther, 1992), Lerner and Tetlock (1999) empirically demonstrated that even just the presence of another who is not actively participating in ongoing communication still influences perceptions of accountability and showed that social presence improved productivity, even when group participants were anonymous. This finding provides evidence that social presence can shape perceptions of accountability in not just face-to-face interactions but in computer-mediated situations as well.

H1d: Social presence will negatively affect non-compliance intention.

In addition to the accountability features built into a security system, other situational, context-specific factors could influence a security analyst's decisions in a SOC. Researchers have suggested that SETA programs and explicit security policies could help reduce the moral disengagement used to rationalize security violations (D'Arcy et al., 2014). An employee's recognition of proper security procedures would reduce the likelihood of violating a policy. Similarly, incorporating legal counsel as part of the security process offers an extra layer of oversight, in addition to taking some of the burden of security decisions off the analyst. A SOC typically involves legal counsel, who review security responses and produce an after-report to ensure legal compliance. Each of these context-specific factors should reduce a security analyst's non-compliance intentions.

H2: Explicit policy awareness will negatively affect non-compliance intention.

H3: Legal counsel will negatively affect non-compliance intention.

Due to the complexity of analysis and the magnitude of potential negative impacts, cyber-risk management is increasingly difficult; security analysis within industrial control systems (ICSs) is illustrative of this growing problem (Pal et al., 2023). One such complexity is derived from the classic competing of protecting information security and information privacy (Crossler et al., 2013). While the security landscape has become progressively multifaceted, there are privacy considerations as well. Research has shown that users who exhibit risky usage behavior on their smartphones are also more likely to use IoT devices (Menard & Bott, 2020). This behavior pattern makes such users especially vulnerable to privacy breaches because IoT devices that collect multitudes of personal behavior data could be exploited by the malicious applications used on their mobile computing devices. For a security analyst who works for an organization that collects data from users' various IoT devices, wearables, and smartphones/tablets, a security threat that simultaneously affects both organizational assets and consumers' private information is increasingly plausible. Additionally, while the organization imposes corporate policies that dictate how to protect organizational information, there are also certain privacy laws that need to be considered for protecting consumer data. The GDPR extends beyond national borders and protects its citizens privacy wherever they may use a digital system. In the US, laws, e.g., Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) would stipulate that a forensic investigator/system should only retrieve data pertinent to an investigation and ensure that evidence-gathering does not infringe upon health or educational data.

These increasing demands on security analysts align well with cybernetic theory (Singh et al., 2023), which posits that people evaluate demands based on their ability to reduce or enhance discrepancies (Edwards, 1992; Stich et al., 2019). The increasing and opposing demands of maintaining security of an organization while also ensuring privacy of consumer data would represent a discrepancy-enhancing scenario. These factors are manifested in our research as threat severity, threat probability and data sensitivity. Threat severity is related to how severe the imminent information security threat is deemed to be. Threat probability represents the likelihood of the threat becoming realized, as reported by the security system. Data sensitivity refers to the level of private data at risk from a security incident. If a threat is severe and probable enough, a security analyst may be inclined to violate an information privacy policy to engage in discrepancy-reducing behavior. Conversely, if the data being violated is highly sensitive, the analyst would be more inclined to follow the data privacy policy.

H4: Threat severity will positively affect non-compliance intention.

H5: Threat probability will positively affect non-compliance intention.

H6: Data sensitivity will negatively affect non-compliance intention.

Security-Related Stress

Security-related stress (SRS) as "a form of psychological stress…caused by internal or external security-related demands appraised as taxing one's cognitive resources or abilities" (D'Arcy et al., 2014, p. 288). SRS is modeled as a second-order construct consisting of three stress-related perceptions: overload, complexity, and uncertainty due to security-based implementations. Overload occurs when security requirements increase an employee's workload. Complexity occurs when security requirements are demanding for employees to understand or learn. Uncertainty occurs when employees cannot cope with constant changes or updates to security requirements. Users affected by SRS will ascribe negative attributes to security requirements, such as time wasted, excessive effort, or frustration. In a scenario-based survey, the findings showed that SRS negatively influenced the intention to violate security policy. Users coped with SRS through moral disengagement, rationalizing their actions by positively reconstruing the violation, downplaying its consequences, and devaluing the impact on the organization.

Security researchers have increasingly studied SRS since its initial inception, demonstrating several ways that SRS hinders an organization's overall security profile. Among workers, overload and invasion of privacy both contribute to SRS; however, prior security knowledge and perceived security threats positively influence employees' attitudes toward security compliance, mitigating SRS (Lee et al., 2016). Although awareness measures, like PMT-based security appeals, should generally ease SRS, fear-induced messaging without corresponding coping recommendations will induce stress (Warkentin et al., 2016). In some instances, security measures can actually elicit maladaptive behaviors due to insiders' lived security experiences, which produce counterproductive security-related beliefs (Balozian et al., 2023). These studies and others demonstrate that SRS is generally positively correlated with non-compliance behavior, as revealed by a recent meta-analysis (Aggarwal & Dhurkari, 2023). Because stress (including technostress and SRS) emerges over time (Salo et al., 2022) and can permeate various aspects of an employee's perception of the work environment (Rohwer et al., 2022), we believe SRS will exert a moderating effect in our research context. In situational moments when an analyst will need to make a decision on dealing with a security event, SRS could hinder security decisions such that SRS would positively moderate an independent variable's effect on non-compliance.

H7: Security-related stress will positively moderate the relationships between accountability features and non-compliance intention.

H8: Security-related stress will positively moderate the relationships between threat severity (a) and threat probability (b) and non-compliance intention.

H9: Security-related stress will positively moderate the relationship between data sensitivity and non-compliance intention.

Burnout

Burnout is traditionally defined as “a state of physical, emotional, and mental exhaustion that results from long-term involvement in work situations that are emotionally demanding” (Schaufeli & Greenglass, 2001, p. 501); subsequent researchers have further refined burnout as attributable to specific contexts (Kristensen et al., 2005). Although burnout can extend to several aspect of one’s life, (Listopad et al., 2021) in our research we limit our examination of burnout to work-related perceptions, as these are the most pertinent to our research context. In the workplace, demands placed on employees can increase burnout but making resources available to employees decreases burnout (Crawford et al., 2010). However, the IS research context, specifically workplace technology, offers an interesting fulcrum for work-oriented burnout, as demonstrated in the conflicting findings in past research. While introducing new information communication and technology (ICT) resources can reduce burnout, if the ICT is demanding, burnout could increase (Ninaus et al., 2021). This effect was demonstrated during the COVID-19 pandemic; workload, in combination with techno-overload, increased stress in remote workers (Ingusci et al., 2021). Technology permeability increased burnout among employees but employees’ collectivist-oriented mindset increased job satisfaction (Chang, 2023).

Burnout in is prevalent in software engineering positions (Tulili et al., 2022). Pertinent to analysts working with ICSs, industrial engineers who were more stressed at work experienced lower productivity and worsening personal and workplace relationships (Timotius & Octavius, 2022). Employees who are highly competent and engaged in their work are less likely to experience burnout or stress, but performance-driven climates are shown to increase burnout (Fastje et al., 2022). Frustration and fatigue make employees more likely to follow through on their rationalizations of ISP violations (D’Arcy & Teh, 2019). In each of the above examples, a performance-based work culture may have contributed to burnout despite the competency and engagement of employees. In information security settings, performance is paramount; failure to perform could result in catastrophic data loss or systems malfunctioning. In fact, researchers have observed risk homeostasis and security fatigue among data analysts (Bhana & Ophoff, 2023). Therefore, burnout could affect the decision making of employees operating in a human-in-the-loop capacity within an ML-based security system, such that burnout may cause employees to err on the side of performance rather than strict security policies. In our model, this influence would manifest as a positive moderating effect.

H7: Burnout will positively moderate the relationships between accountability features and non-compliance intention.

H8: Burnout will positively moderate the relationships between threat severity (a) and threat probability (b) and non-compliance intention.

H9: Burnout will positively moderate the relationship between data sensitivity and non-compliance intention.

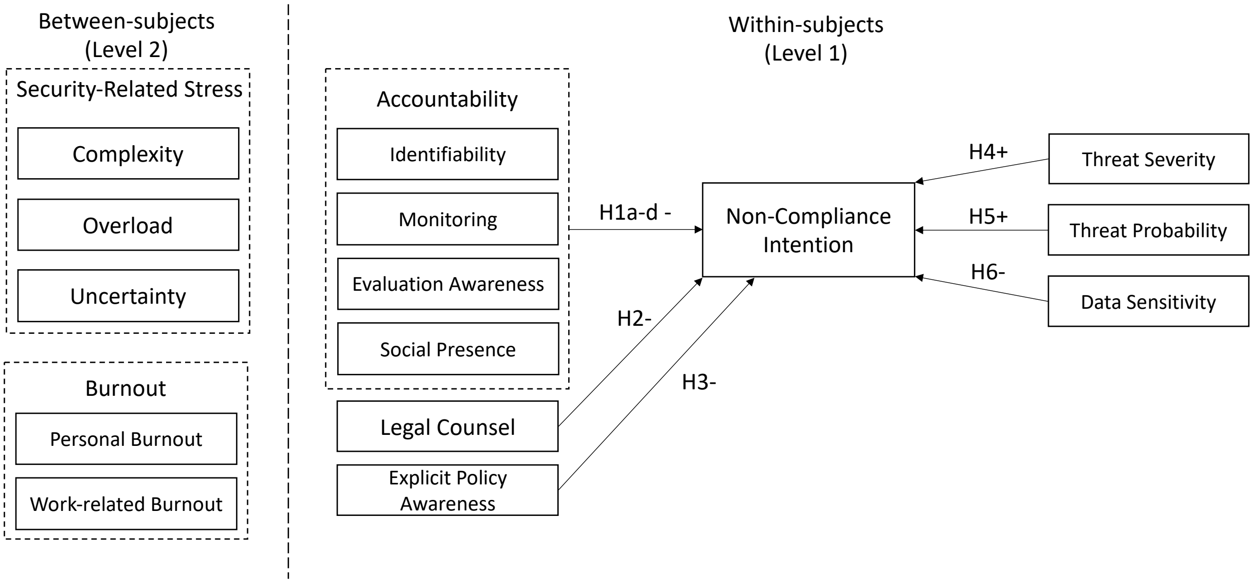

Figure 1. Research Model

METHODS

Factorial Survey Method

To examine the influence of SRS, burnout, and accountability-based system features on employees' decisions related to security and privacy, we will use a factorial survey design (Chatterjee et al., 2015; Vance et al., 2013). Within each scenario, a respondent will be shown a random combination of statements, where each statement is designed to bolster the respondent's perception of the research model's independent variables. This design will allow us to examine the individual influence and interactions of each independent variable on intention. Our model contains four independent variables representing accountability features (identifiability, monitoring, evaluation, and social presence – see Figure 1). Additionally, we are capturing several independent variables specific to the context of a potential human-in-the-loop security implementation – the sensitivity level of the data being accessed; the level of involvement of legal counsel based on security actions taken; the severity of the security threat posed to the organization; the system's confidence in its analysis presented to the human employee; and whether an explicit acknowledgment of policy awareness within the scenario impacts intention to violate. Thus, nine possible manipulation statements may be embedded in the scenario. This scenario design results in 512 possible combinations of embedded statements. For more details on the construction of our scenarios, please see Appendix A.

Sampling Frame. Scenario Contextualization, and Measurement Scales

Because we are analyzing the impact of SRS and burnout within the context of accountability features built into an ML-driven security system, the appropriate respondent for our study will be an employee who works in a similar capacity (security analyst, data analyst, human-in-the-loop, etc.). In addition, we will solicit respondents from Qualtrics, whose platform we will also use for hosting the survey instrument. Following the survey design implemented by Vance et al. (2013), our scenarios also depict situations in which the scenario character has access to critical information and decides to violate their access policy; however, in our scenario, the privacy violation occurs due to the employee attempting to maintain security in the face of an imminent threat. To measure employee burnout, we will use the Copenhagen Burnout Inventory (Kristensen et al., 2005). We will use previously validated scales for measuring the first-order SRS components complexity, overload, and uncertainty (D'Arcy et al., 2014). We will measure non-compliance intention using a single-item scale. Each construct is measured using a 5-point scale (for full measurement scales, see Appendix B).

Multilevel Modeling and Sample Size

Because we will present our respondents with multiple scenarios, each time measuring their intention to behave similarly to the scenario character, we will use multilevel modeling to assess both within-group (Level 1) and between-group (Level 2) effects. We will use Mplus as our statistical software (Muthén & Muthén, 2017). Although calculating statistical power for multilevel models is more complex than single-level statistical models, researchers can utilize Monte Carlo simulations to estimate observed statistical power under varying conditions based on Level 1 and Level 2 sample sizes, estimated intraclass correlation coefficients, and effect sizes at each level (Arend & Schäfer, 2019). To achieve statistical power necessary to confidently interpret our two-level model (assuming medium-sized Level 1 and 2 direct effects and medium-sized random slopes for cross-level effects), our sample would need at least 200 respondents, with each respondent exposed to at least nine scenarios (Arend & Schäfer, 2019), with each scenario featuring randomized high/low manipulations of the statements representing the independent variables.

POTENTIAL THEORETICAL AND PRACTICAL IMPLICATIONS

AI or ML-enhanced security countermeasures will continuously be introduced into SOC environments in the near future. Despite the touted security benefits of such systems, some of the unintended consequences of adopting such systems may include employee burnout and security-related stress. We anticipate impactful insights from our study, including how stress and burnout contribute to poor decision-making within the context of human-in-the-loop operators and AI/ML security systems. Our study is well-positioned to contribute to the cybersecurity knowledge base by offering a better understanding of the system features and environmental factors that affect SOC operators working as humans-in-the-loop.

REFERENCES

Aggarwal, A., & Dhurkari, R. K. (2023). Association between stress and information security policy non-compliance behavior: A meta-analysis. *Computers & Security*, *124*, 102991.

Arend, M. G., & Schäfer, T. (2019). Statistical power in two-level models: A tutorial based on Monte Carlo simulation. *Psychological Methods*, *24*(1), 1–19.

Balozian, P., Burns, A., & Leidner, D. E. (2023). An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures. *Journal of the Association for Information Systems*, *24*(1), 161–221.

Baumeister, R. F. (1982). A self-presentational view of social phenomena. *Psychological Bulletin*, *91*(1), 3.

Bhana, A., & Ophoff, J. (2023). Risk homeostasis and security fatigue: A case study of data specialists. *Information & Computer Security*.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & 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*, *18*, 151–164. https://doi.org/10.1057/ejis.2009.8

Chang, C. L.-H. (2023). How Does IT Influence Chinese IS/IT Users' Job Burnout?: Based on Chinese Guanxi Perspective. *Journal of Global Information Management (JGIM)*, *31*(1), 1–24.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems*, *31*(4), 49–87.

Crawford, E. R., LePine, J. A., & Rich, B. L. (2010). Linking job demands and resources to employee engagement and burnout: A theoretical extension and meta-analytic test. *Journal of Applied Psychology*, *95*(5), 834.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*(1), 90–101.

D'Arcy, J., Herath, T., & Shoss, M. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), 103151.

Edwards, J. R. (1992). A cybernetic theory of stress, coping, and well-being in organizations. *Academy of Management Review*, *17*(2), 238–274.

Fastje, F., Mesmer-Magnus, J., Guidice, R., & Andrews, M. C. (2022). Employee burnout: The dark side of performance-driven work climates. *Journal of Organizational Effectiveness: People and Performance*, *ahead-of-print*.

Geen, R. G. (1991). Social motivation. *Annual Review of Psychology*, *42*(1), 377–399.

Griffith, T. L. (1993). Monitoring and performance: A comparison of computer and supervisor monitoring. *Journal of Applied Social Psychology*, *23*(7), 549–572.

Herath, T., & Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hochwarter, W. A., Ferris, G. R., Gavin, M. B., Perrewé, P. L., Hall, A. T., & Frink, D. D. (2007). Political skill as neutralizer of felt accountability—Job tension effects on job performance ratings: A longitudinal investigation. *Organizational Behavior and Human Decision Processes*, *102*(2), 226–239.

Illman, E. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *Business Lawyer*, *73*(1), 191–198.

Ingusci, E., Signore, F., Giancaspro, M. L., Manuti, A., Molino, M., Russo, V., Zito, M., & Cortese, C. G. (2021). Workload, techno overload, and behavioral stress during COVID-19 emergency: The role of job crafting in remote workers. *Frontiers in Psychology*, *12*, 655148.

Kirsch, L. J., & Boss, S. R. (2007). The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines. *International Conference on Information Systems*, 1–18.

Kristensen, T. S., Borritz, M., Villadsen, E., & Christensen, K. B. (2005). The Copenhagen Burnout Inventory: A new tool for the assessment of burnout. *Work & Stress*, *19*(3), 192–207.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding Information Security Stress: Focusing On The Type Of Information Security Compliance Activity. *Computers & Security*, *59*, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. *Psychological Bulletin*, *125*(2), 255.

Listopad, I. W., Michaelsen, M. M., Werdecker, L., & Esch, T. (2021). Bio-psycho-socio-Spirito-cultural factors of burnout: A systematic narrative review of the literature. *Frontiers in Psychology*, *12*, 722862.

Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security*, *95*, 101856.

Muthén, L. K., & Muthén, B. O. (2017). *Mplus User's Guide* (Eighth Edition). Muthén & Muthén.

Muzumdar, P., Basyal, G. P., Vyas, P., Vyas, G., & Soni, V. (2023). An Exploratory Literature Analysis of Technostress Research in Information Systems Science. *Journal of Research in Business and Management*, *11*(1), 32–40.

Neuburger, J. (2016). Illinois Biometric Privacy Suit over Collection of Fingerprints Settled. *Proskauer*.

Ninaus, K., Diehl, S., & Terlutter, R. (2021). Employee perceptions of information and communication technologies in work life, perceived burnout, job satisfaction and the role of work-family balance. *Journal of Business Research*, *136*, 652–666.

Pal, R., Liu, P., Lu, T., & Hua, E. (2023). How Hard Is Cyber-risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs. *ACM Transactions on Cyber-Physical Systems (TCPS)*, *6*(4), 1–31.

Rice, R. E. (1993). Media appropriateness: Using social presence theory to compare traditional and new organizational media. *Human Communication Research*, *19*(4), 451–484.

Rohwer, E., Flöther, J.-C., Harth, V., & Mache, S. (2022). Overcoming the "Dark Side" of Technology—A scoping review on preventing and coping with work-related technostress. *International Journal of Environmental Research and Public Health*, *19*(6), 3625.

Salo, M., Pirkkalainen, H., Chua, C. E. H., & Koskelainen, T. (2022). Formation and mitigation of technostress in the personal use of IT. *MIS Quarterly*, *46*(2), 1073–1108.

Schaufeli, W. B., & Greenglass, E. R. (2001). Introduction to special issue on burnout and health. *Psychology & Health*, *16*(5), 501–510.

Sedikides, C., Herbst, K. C., Hardin, D. P., & Dardis, G. J. (2002). Accountability as a deterrent to self-enhancement: The search for mechanisms. *Journal of Personality and Social Psychology*, *83*(3), 592.

Singh, T., Johnston, A. C., D'Arcy, J., & Harms, P. D. (2023). Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People*.

Stich, J.-F., Tarafdar, M., Stacey, P., & Cooper, C. L. (2019). E-mail load, workload stress and desired e-mail load: A cybernetic approach. *Information Technology & People*, *32*(2), 430–452.

Timotius, E., & Octavius, G. S. (2022). Stress at the Workplace and Its Impacts on Productivity: A Systematic Review from Industrial Engineering, Management, and Medical Perspective. *Industrial Engineering & Management Systems*, *21*(2), 192–205.

Tulili, T. R., Capiluppi, A., & Rastogi, A. (2022). Burnout in software engineering: A systematic mapping study. *Information and Software Technology*, 107116.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263–289.

Walther, J. B. (1992). Interpersonal effects in computer-mediated interaction: A relational perspective. *Communication Research*, *19*(1), 52–90.

Warkentin, M., Walden, E. A., Johnston, A. C., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems*, *17*(3), 194–215.

Williams, K., Harkins, S. G., & Latané, B. (1981). Identifiability as a deterrant to social loafing: Two cheering experiments. *Journal of Personality and Social Psychology*, *40*(2), 303.

APPENDIX A

Scenario Implementation

Manipulation Statements

Identifiability Statements:

- Low - Users sign into the system using a unique user ID, composed of three random letters and three random numbers. After the login process, the user is taken straight to the security dashboard without a welcome message. The user ID is not visible anywhere on the dashboard; there is only a Log Off button in the top right-hand corner.
- High - Users sign into the system using a unique user ID, composed of first initial, last name, and a random number. The welcome screen displays the user's actual full name. The user ID is visible in the top right-hand corner of the dashboard at all times.

Monitoring Statements:

- Low - Although all system activities are logged, there is no visible indication to the user when activities in the system are recorded.
- High - The login screen warns that the user's activities in the system will be recorded. Users can click to view a history of all their activity in the system. In addition, when a user is about to perform an action in the system, a notification message warns that the current action will be logged with the user ID.

Evaluation Statements:

- Low - There is no indication that audits of user activity will be performed.
- High - All user activity in the system is comprehensively audited, according to a warning on the login screen.

Social Presence Statements:

- Low - The user works in isolation, connecting to the system remotely over an organizational VPN.
- High - The user works in a Secure Operations Center (SOC) among other security analysts. The SOC has 5-10 analysts onsite at all times.

Explicit Policy Awareness Statements:

- Low - Because Jordan believes further exploration of customer data is not a violation of the organization's customer privacy policy, Jordan
- High - Although Jordan believes further exploration of customer data may be a violation of the organization's customer privacy policy, Jordan

Legal Counsel Statements:

- Low - The human expert in this system can take any action as deemed necessary, with no consultation with a member of the organizational legal team required.
- High - According to organizational policy, any action taken by a human expert that reveals a customer's personally identifiable information must be submitted to a member of the legal compliance team after it was executed.

Data Sensitivity Statements:

- Low - anonymized customer interaction behaviors
- High - highly detailed personal customer information, including the customer's social security number, email, cell phone number, and home address

Threat Severity Statements:

- Low - activity flagged as possible malware, but no other organizational systems are reporting problems
- High - rapidly propagating malware that is taking multiple critical systems offline

Threat Probability Values:

- Low – 75%
- Medium – 85%
- High – 95%

Base Scenario (first paragraph remains static for all scenarios)

Jordan is a data analyst at Roadrunner Financial, a national bank and investment broker with millions of customers. Although it has adopted numerous digital technologies, Roadrunner has made a pledge to its customers that it will protect their private information no matter what. Jordan is employed as a human expert within the organization’s security operations and is tasked with using the organization’s security dashboard, which uses machine learning to provide information that supports security decisions. Jordan interprets monitors the dashboard's output for potential further action and feeds inputs back into the system after validating them. Through this system, the human expert has access to anonymized networking packet data, allowing the expert to assess overall network performance while keeping personally identifiable information private.

[Identifiability Statement] [Monitoring Awareness Statement] [Evaluation Awareness Statement] [Social Presence Statement] In the dashboard, Jordan notices [Threat Severity Statement]. The system tells Jordan that it is [Threat Probability Value] % confident in its analysis. The activity appears to be deriving from a customer account. Jordan is given the option to further analyze the customer’s information, which includes [Data Sensitivity Statement].

[Legal Counsel Statement] [Explicit Policy Awareness Statement] decides to further explore the customer’s information and feed the data back into the machine learning system as inputs.

Example Scenario with all low manipulations

Users sign into the system using a unique user ID, composed of three random letters and three random numbers. After the login process, the user is taken straight to the security dashboard without a welcome message. The user ID is not visible anywhere on the dashboard; there is only a Log Off button in the top right-hand corner. Although all system activities are logged, there is no visible indication to the user when activities in the system are recorded. There is no indication that audits of user activity will be performed. The user works in isolation, connecting to the system remotely over an organizational VPN. In the dashboard, Jordan notices activity flagged as possible malware, but no other organizational systems are reporting problems. The system tells Jordan that it is 75% confident in its analysis. The activity appears to be deriving from a customer account. Jordan is given the option to further analyze the customer’s information, which includes anonymized customer interaction behaviors.

The human expert in this system can take any action as deemed necessary, with no consultation with a member of the organizational legal team required. Because Jordan believes further exploration of customer data is not a violation of the organization’s customer privacy policy, Jordan decides to further explore the customer’s information and feed the data back into the machine learning system as inputs.

Example scenario with all high manipulations

Users sign into the system using a unique user ID, composed of first initial, last name, and a random number. The welcome screen displays the user's actual full name. The user ID is visible in the top right-hand corner of the dashboard at all times. The login screen warns that the user's activities in the system will be recorded. Users can click to view a history of all their activity in the system. In addition, when a user is about to perform an action in the system, a notification message warns that the current action will be logged with the user ID. All user activity in the system is comprehensively audited, according to a warning on the login screen. The user works in a Secure Operations Center (SOC) among other security analysts. The SOC has 5-10 analysts onsite at all times. In the dashboard, Jordan notices rapidly propagating malware that is taking multiple critical systems offline. The system tells Jordan that it is 95% confident in its analysis. The activity appears to be deriving from a customer account. Jordan is given the option to further analyze the customer's information, which includes highly detailed personal customer information, including the customer's social security number, email, cell phone number, and home address.

According to organizational policy, any action taken by a human expert that reveals a customer's personally identifiable information must be submitted to a member of the legal compliance team after it was executed. Although Jordan believes further exploration of customer data may be a violation of the organization's customer privacy policy, Jordan decides to further explore the customer's information and feed the data back into the machine learning system as inputs.

APPENDIX B

Measurement Scales

Non-compliance Intention

- For this item, please indicate the likelihood you would have behaved in the same way as Jordan. (Highly unlikely, Unlikely, Somewhat likely, Likely, Highly likely)

Copenhagen Burnout Inventory (Kristensen et al., 2005)

Personal Burnout

- How often do you feel tired? [1]
- How often are you physically exhausted? [1]
- How often are you emotionally exhausted? [1]
- How often do you think: "I can't take it anymore?" [1]
- How often do you feel worn out? [1]
- How often do you feel weak and susceptible to illness? [1]

Work-related Burnout

- Do you feel worn out at the end of the working day? [1]
- Are you exhausted in the morning at the thought of another day at work? [1]
- Do you feel that every working hour is tiring for you? [1]
- Do you have enough energy for family and friends during leisure time? [1]
- Is your work emotionally exhausting? [2]
- Does your work frustrate you? [2]
- Do you feel burnt out because of your work? [2]
  1 = responses are Never/Almost Never, Seldom, Sometimes, Often, Always
  2 = responses are To a very low degree, To a low degree, Somewhat, To a high degree, To a very high degree

Security-Related Stress (D'Arcy et al., 2014)

(All SRS scales are measured using fully-anchored 5-point Likert scales)

Overload

- I am forced by information security policies and procedures to do more work than I can handle.
- My organization's information security policies and procedures hinder my very tight time schedules.
- I have a higher workload due to increased information security requirements.
- I am forced to change my work habits to adapt to my organization's information security requirements.

Complexity

- I find that new employees often know more about information security than I do.
- I do not know enough about information security to comply with my organization’s policies in this area.
- I often find it difficult to understand my organization’s information security policies.
- It takes me a while to understand my organization’s information security policies and procedures.
- I sometimes do not have time to comply with my organization’s information security policies.

Uncertainty

- There are constant changes in information security policies and procedures in my organization.
- There are frequent upgrades to information security procedures in my organization.
- There are always new information security requirements in my job.
- There are constant changes in security-related technologies in my organization.