

Walking the Tightrope: The Role of Social Appraisal in Unethical but Pro-organizational Security Behavior after A Data Breach

Early stage paper

Sumin Kim

Mississippi State University
sk2013@msstate.edu

Merrill Warkentin

Mississippi State University
m.warkentin@msstate.edu

ABSTRACT

This research conceptualizes and explores employees' unethical but pro-organizational behavior in the information security context, specifically examining how employees may engage in deviant security behaviors to benefit their organization after a data breach. This study challenges the traditional focus on self-benefitting information security policy violations. By integrating protection motivation theory and the person-situation interactionist framework, this study investigates how individuals' appraisals and their interactions with social appraisal influence unethical but pro-organizational security behavior. This paper provides a theoretical contribution to protection motivation theory by exploring the role of social appraisal and juxtaposing it with individuals' appraisal. Additionally, we contribute to the information security literature by addressing the previously underexplored phenomenon of unethical but pro-organizational security behavior.

Keywords

Unethical but pro-organizational security behavior, data breach, information security.

INTRODUCTION

When a company experiences a data breach, the company and its employees may assess how to take measures to minimize the damage to the company, its clients, and its customers. After a data breach, companies can face financial loss, reputational damage, and lawsuits. Because of its serious damage to the companies, many companies increase their investments in cybersecurity and implementing Security Education, Training, and Awareness (SETA) programs for their employees. Insiders are frequently identified as the weakest link in information security (Warkentin and Willison 2009). However, information security literature has focused on insiders' behavior *before* rather than *after* data breaches. Data breach response strategies are crucial to minimize the damage to both company and customers, to secure the systems and fix vulnerabilities, and to prevent additional data loss (Federal Trade Commission 2021). As immediate response and mitigation is important after data breach, it is also important to explore employees' behavioral response as it can significantly impact the effectiveness of the company's response.

Employees' information security behavior is broadly categorized as information security policy compliance and non-compliance. This information security policy compliance behavior is further categorized as in-role security behavior, which is complying with formal security policy, and extra-role security behavior, which is beyond what is required in the security policy stated and job description. Information security policy non-compliance behavior is categorized based on their underlying intentions, ranging from passive to volitional to intentional, and from non-malicious to malicious. It is important to recognize that these categories are not clear-cut but rather exist on a continuum (Willison & Warkentin, 2013). Focusing solely on these categorizations may blind us to other types of security behaviors.

A considerable amount of research has been devoted to investigating violations of, or non-compliance with, information security policies (Cram et al. 2019). However, this body of work often overlooks the nuanced category of deviant security behaviors. Traditionally, the assumption in information security research has been that such deviations are primarily self-serving, grounded in greed or revenge, for example. Yet, evidence suggests that employees may engage in these intentional violation behaviors not out of self-interest, but rather to benefit their organization, their team, or its members (Mishra et al. 2022). These actions, and the motivations behind them, remain underexplored. This oversight is critical; in practice, pro-organizational intentions can drive employees towards unethical security practices, potentially resulting in adverse outcomes for both stakeholders and the organization over time. Therefore, this research raises question:

RQ1. How do pro-organizational intentions influence employees to engage in deviant security behaviors?

To answer this question, we are informed by protection motivation theory (PMT), which explain how individuals appraise the given threat (i.e. is this threatening to me? Do I have resources to mitigate this threat?). When employees perceive security-related threats to their organization, they may sometimes be likely to engage in protective behaviors against the threat (e.g. a data breach) to minimize the damage and protect their companies' reputation and benefits. When individuals perceive the threat as noxious and the probability of occurrence of the threat as plausible, but they believe that they have the resources to mitigate the threat, they are generally more likely to engage in coping behavior to change the threatful situation (Rogers 1975; Scherer et al. 2001). In the information security discipline, PMT has been widely used to explain employees' protective behavior against information security threats.

PMT was adopted from healthcare research, which is grounded on individuals' health threats (Johnston and Warkentin 2010). However, PMT's boundary condition of the threat's "personal relevance" has limited meaning in the information security context because the information belongs to the organization and may not be personally relevant. Furthermore, the organizational contexts involve salient social interactions. In this context, it is important to consider not only how individuals perceive a given threat, but how their coworkers may perceive that threat. Social learning theory posits that individuals learn through observing others' values, attitudes, and behaviors (Bandura 1977). Therefore, if individuals observe their coworkers treating data breaches as severe threats toward the company's reputation or reacting to threats with unethical but pro-organizational security behavior (UPSB), they are also likely to engage in such behavior. Therefore, the second research question is:

RQ2. How do others' perception toward information security threats affect individuals' UPSB behavior?

To answer the second research question, we draw on the *person-situation interactionist framework*. The recent person-situation debate recognizes that both person and situation are influential in determining a person's behavior. According to the interactionist, an employee's ethical behavior is determined by the cues in the environment and individuals who interact with the given environment (Graham et al. 2015; Trevino 1986). By following the interactionist's view, this study also considers both personal and situational factors. Although previous literature has explored the person and situation factors that motivate employees to engage in unethical but pro-organizational behavior (UPB), this behavior and its motivations have not been thoroughly examined in the context of information security. This leads to another interesting question.

What results when self appraisal and others' appraisal align or contrast? For example, when a data breach happens to the employer, an employee might think the consequences of the data breach would be very serious. However, such perception might be changed after s/he observes her/his coworkers are not worried about the consequences of the data breach. Conversely, when an employee perceives that the consequences of the data breach would be serious and she observes her coworkers perceive it the same way, her threat perception would be strengthened. This leads to the following research question:

RQ3. How do individuals react when their perceptions align with or differ from others' perceptions?

The remainder of the paper is as follows. First, the literature review on relevant topics, along with hypotheses, is presented. Next, the method to test the hypothesized model is discussed. Finally, the paper concludes with a discussion and implications.

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

Unethical but Pro-Organizational Security Behavior

UPB has garnered significant attention within the management discipline due to its paradoxical nature. Traditionally, deviant workplace behavior has been predominantly viewed through the lens of self-benefiting actions, where employees engage in misconduct to achieve personal gains at the expense of organizational goals. However, recent research has shifted focus to acknowledge that deviant behaviors can also be driven by intentions to benefit the group or organization, even if such actions violate ethical standards. This emerging perspective on UPB is crucial for understanding the complex motivations behind employee behavior in organizational settings.

UPB is defined as actions that contravene societal values, laws, or norms but are intended to benefit the organization or its members (Umpress et al. 2010). These behaviors, while aimed at advancing organizational interests, ultimately result in societal harm. The concept of UPB challenges the conventional dichotomy of policy compliance versus violation behavior by introducing a scenario where employees may engage in misconduct with ostensibly good intentions—supporting the organization or its goals.

Willison and Warkentin (2013) classified internal employee security policy violation behaviors into three categories along the continuum: (a) passive, non-volitional noncompliance, (b) volitional (but not malicious) noncompliance, and (c) intentional, malicious (harmful) computer abuse. Organizations have implemented various measures, such as SETA programs and disciplinary actions, to mitigate these behaviors. However, these initiatives may fall short if employees rationalize their deviant security actions as beneficial to their organization.

For example, employees might engage in selective disclosure of the firm's security posture while concealing vulnerabilities, especially before mergers and acquisitions (M&A) (Lowe 2019). Companies may also resort to victim-blaming, attributing data breaches to consumers or third parties to deflect liability (Jones 2024; Newman and Greenberg 2024; Valinsky 2024). The 23andMe incident, where the company blamed reused passwords by users for a data breach affecting approximately 6.9 million individuals, illustrates this tactic (Franceschi-Bicchierai 2024).

Employees may adopt ethically questionable yet organizationally favorable security practices primarily to safeguard the company's reputation and avert financial losses. Following a data breach, employees might evaluate the perceived threat and its potential repercussions. If the threat appears serious and resources to address or mitigate it are deemed available, employees

may consider adopting measures even if these measures conflict with social norms. Such actions are distinct from purely self-serving deviant behaviors, as they are intended to benefit the organization and indirectly its members.

Despite the prevalence of these practices in real-world settings, the academic focus on UPB in information security remains limited. Understanding the factors influencing employees to engage in UPSB is crucial for developing effective organizational policies and interventions.

However, many employees would not engage in unethical security behavior for the sake of their organization, perhaps because they may appraise the same event differently.

Furthermore, what are some factors that impact employees' UPB? In the literature review on UPB, Mishra et al. (2022) suggested theories that explain UPB: social identity theory, social exchange theory, social learning theory, social cognitive theory, etc. The most compelling explanation for UPB is derived from social identity theory (Tajfel and Turner 1979) and organizational identification is the psychological antecedents of UPB in the workplace (Mishra et al. 2022). The desire of employees with high organizational identification to protect their organization may prioritize their organization's interests over ethical considerations and the well-being of those adversely affected by their actions (Mishra et al. 2022). Similar UPB research (Umphress et al. 2010) found that organizational identification positively impacts on UPB when positive reciprocity beliefs are high, and Chen et al. (2016) also confirmed a positive relationship between organizational identification and UPB.

Another theory effectively explaining UPB is social exchange theory, suggesting that employees who have a positive social exchange relationship with their employers tend to engage in UPB as a gesture of reciprocating the beneficial treatment afforded by their organization (Mishra et al. 2022; Umphress and Bingham 2011; Umphress et al. 2010). For example, positive

reciprocity beliefs (Umphress et al. 2010) were considered as boundary conditions and antecedents (Umphress and Bingham 2011) of UPB in addition to mutual-investment EORs (Wang et al. 2019), supervisors' bottom-line mentality (Babalola et al. 2021), and workplace spirituality (Zhang 2020).

Additionally, the impact of supervisors' UPB (Fehr et al. 2019) and ethical leadership (Miao et al. 2013) on UPB was explored using the social learning perspective (Mishra et al. 2022). According to social learning theory, individuals learn behaviors through observing others and the consequences of their actions. This theory suggests that employees may model their behavior after their coworkers or managers, especially when they perceive such behavior as being rewarded, punished, or unpunished.

In the workplace, employees often look to their supervisors and peers for cues on acceptable conduct. When supervisors engage in UPB and are perceived to be rewarded or not penalized for such actions, employees are likely to mimic these behaviors, believing them to be beneficial for the organization. Similarly, ethical leadership can play a critical role. Leaders who demonstrate ethical behavior set a positive example, influencing employees to follow suit. Conversely, if leaders engage in or tolerate UPB, it can normalize these behaviors within the team, encouraging employees to adopt similar actions under the belief that they are acting in the organization's best interests. This learning process highlights the importance of the organizational environment and leadership in shaping employee behavior. By understanding how social learning influences UPB, organizations can better address and mitigate these behaviors, promoting a culture of ethical vigilance.

To explain UPSB, this study integrates PMT and people-situation interactionist framework. Detailed theorization is provided in the following sections.

Protection Motivation Theory

PMT is pivotal frameworks in psychological and communication research, each offering a significant contribution to our understanding of human cognition and behavior. Specifically, PMT offers insights into how individuals process and react to various stimuli and threats. PMT was introduced by Rogers (1975) and built upon the ideas of Lazarus who is primarily known for his work on stress, coping, and emotion. It explains how people are motivated to protect themselves from perceived threats through cognitive processes, emphasizing threat assessment and coping efficacy. In information security research, PMT has been used to delineate how individuals assess information security threats through threat appraisal and evaluate their coping capacities and efficacies through coping appraisal.

Threat Appraisal

PMT has been widely used in the information security discipline to explain employees' intentions to protect against information security threats. PMT posits that individuals assess threats through two key cognitive processes: threat appraisal and coping appraisal. Threat appraisal involves evaluating the severity and vulnerability associated with a threat, which in turn influences an individual's motivation to engage in protective behaviors (Rogers, 1975).

In the context of this study, we extend the application of PMT to examine how employees respond to threats against their organization's reputation. Specifically, this research proposes that when employees perceive a threat to their organization's reputation, it may lead to unethical behavior to protect their organization. This behavior, termed UPSB, arises from the desire to protect the organization from reputational damage, even if it involves actions that contravene societal norms.

Perceived severity refers to an individual's assessment of the seriousness of a threat's potential consequences. In the case of a data breach, employees who perceive the threat as highly severe are likely to experience heightened motivation to protect the organization. This heightened motivation can lead to information security policy compliance or, in some cases, to unethical behaviors intended to mitigate the perceived threat. For example, an employee might falsify security reports or blame external parties to deflect responsibility from the organization. Therefore, we hypothesize:

Hypothesis 1. *Perceived severity of threat against the organization's reputation will have a positive impact on employees' intention to engage in UPSB.*

Perceived vulnerability reflects an individual's belief about the likelihood of experiencing the threat. When employees perceive their organization as vulnerable to a data breach, they may feel a pressing need to take action to protect the organization's reputation. This sense of urgency can lead to the adoption of UPB, especially if employees believe these actions are necessary to prevent significant harm to the organization. Thus, we hypothesize:

Hypothesis 2. *Perceived vulnerability of threat against the organization's reputation will have a positive impact on employees' intention to engage in UPSB.*

Coping Appraisal

Coping appraisal involves evaluating one's ability to deal with a threat, including assessments of self-efficacy and response efficacy. In PMT, coping appraisal determines whether individuals believe they can effectively perform the recommended protective behaviors and whether these behaviors will mitigate the threat.

Self-efficacy refers to an individual's belief in their capability to execute the actions required to manage a threat. Employees with high self-efficacy are more confident in their ability

to implement security measures, even those that may be ethically dubious. This confidence can lead to increased intentions to engage in UPSB, as employees feel capable of effectively protecting the organization. Therefore, we hypothesize:

Hypothesis 3. *Self-efficacy will have a positive impact on employees' intention to engage in UPSB.*

Response efficacy pertains to an individual's belief that the actions they take will effectively mitigate the threat. Employees who believe that their unethical actions will successfully protect the organization are more likely to engage in such behaviors. If they perceive that these actions will have a significant positive impact on the organization's security and reputation, their intention to engage in UPB will increase. Thus, we hypothesize:

Hypothesis 4. *Response efficacy will have a positive impact on employees' intention to engage in UPSB.*

Social Appraisal

PMT has traditionally focused on how individuals assess threats and their coping mechanisms, which emphasizes individuals' appraisal of stimuli or threats. When individuals face a threat, they evaluate their perception of the threat (i.e. threat appraisal) and their own resources to manage it (i.e. coping appraisal) (Rogers, 1975; Scherer et al., 2001). However, in an organizational context, employees do not operate in isolation. They interact with managers, coworkers, and organizational norms that significantly influence their behavior. Therefore, both *person* (i.e., individuals' appraisal) and *situation* (i.e., social appraisal) influence individuals' behavior. Such interplay explains why employees might behave differently when facing a specific threat in the organizational context than they might without this interaction with others.

This *person-situation interactionist framework* provides a comprehensive approach to understanding employees' security related behavior.

This social dimension introduces the concept of social appraisal, which is the individuals' evaluation of how others perceive threats and norms within the organization (Scherer et al. 2001). Social appraisal is particularly relevant in information security, where collective behavior and shared norms can impact individual actions. Social appraisal can appear in two primary ways: descriptive norms and others' threat perception. Others' threat perception pertains to how peers and superiors perceive and respond to security threats, whereas descriptive norms refer to the common behaviors and attitudes observed within a group. These social factors can profoundly impact employees' intentions to engage in behaviors that align with or deviate from organizational policies.

Others' Threat Perception. Others' threat perception involves understanding how coworkers and managers perceive the severity and vulnerability of security threats. When employees notice that their peers or superiors view a threat as significant, they may feel a heightened sense of urgency to take action, even if this action involves violating security policies for the perceived benefit of the organization. This alignment with others' threat perceptions can lead to a collective response aimed at mitigating the threat, reinforcing the justification for UPB. Therefore, we hypothesize:

Hypothesis 5a. *Others' threat perception will positively moderate the relationship between perceived severity of threat and employees' intention to engage in UPSB.*

Hypothesis 5b. *Others' threat perception will positively moderate the relationship between perceived vulnerability of threat and employees' intention to engage in UPSB.*

Descriptive Norms. Descriptive norms provide a benchmark for acceptable behavior within an organization. Social learning theory suggests that individuals learn how to behave by observing

others' behaviors and their consequences (Bandura 1977). When employees observe that their peers engage in certain behaviors, they are more likely to conform to these behaviors to fit in and gain social acceptance. In the context of information security, if employees perceive that their peers commonly engage in UPSB, they may be more inclined to adopt similar behaviors, rationalizing that such actions are normative and justified. When they observe their coworkers' engagement in UPSB. Therefore, we hypothesize:

Hypothesis 6a. *Descriptive norms will positively moderate the relationship between self-efficacy and employees' intention to engage in UPSB.*

Hypothesis 6b. *Descriptive norms will positively moderate the relationship between response efficacy and employees' intention to engage in UPSB.*

The research model is presented in Figure 1.

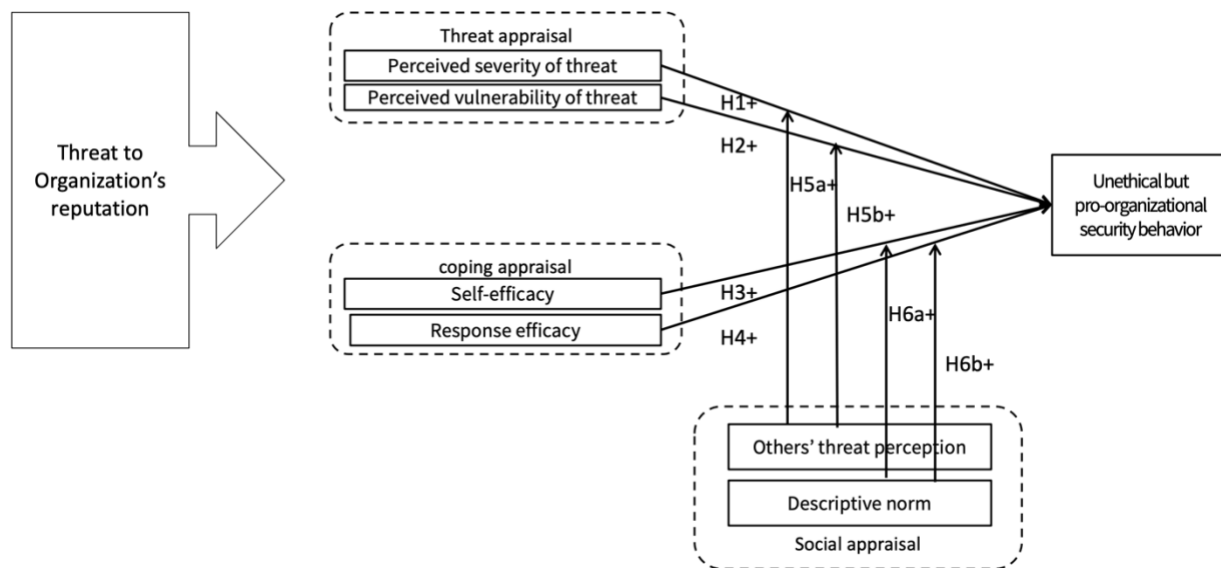


Figure 1. Hypothesized Model

PROPOSED METHOD

To test (1) the influence of threat appraisal and coping appraisal on UPSB intention and (2) the moderating role of social appraisal on said influences, this study will conduct a field experiment, employing a survey-based experimental approach to rigorously test the proposed hypotheses. This method was chosen to establish strong causal inferences and mitigate social desirability bias—a critical consideration given the focus on UPSB. The survey-based experiment addresses social desirability bias by placing participants in hypothetical scenarios rather than asking about their real-life behavior, which has been applied extensively in the extant security behavior literature. To address the potential challenge of limited realism often associated with experimental research, we assessed participants' perceived realism of the scenarios.

Experimental Design and Procedure.

A 2 (perceived threat high vs low) x 3 (others' threat perception absent vs high vs low) x 3 (descriptive norm absent vs high vs low) factorial design will be employed to examine the role of threat appraisal and social appraisal (i.e. perceived threat by others and descriptive norm) impact employees' UPSB. The experimental design is presented in Table 1.

Others' threat perception Descriptive norm	Perceived threat high			Perceived threat low		
	Absent	High	Low	Absent	High	Low
Absent	H*A*A	H*A*H	H*A*L	L*A*A	L*A*H	L*A*L
High	H*H*A	H*H*H	H*H*L	L*H*A	L*H*H	L*H*L
Low	H*L*A	H*L*H	H*L*L	L*L*A	L*L*H	L*L*L

Table 1. Experimental Design

Participants will be randomly assigned to three of the eighteen experimental conditions.

In the treatment group scenarios, participants are asked to read an announcement from their

manager describing the current data breach [high threat vs low threat] and to also read a fictitious conversation between two fellow employees about the data breach with social appraisal [absent vs high vs low]. Then, they are asked to answer survey questions, including a realism check and manipulation check of the scenarios, as well as measurement items for perceptions and intention.

Experimental Stimuli

We created a manager's announcement about a recent data breach which mentioned its possible threatful consequences to the company's benefits and reputation. This announcement is manipulated with high threat and low threat, aiming to manipulate individuals' threat perception. For high threat treatment, the manager emphasizes the severity and vulnerability of the threat. For low threat treatment, the manager mentions the severity and vulnerability of the threat with neutral tone.

Next, a conversation between two coworkers is presented to manipulate social appraisal. Social appraisal encompasses others' threat perception and descriptive norms. Others' threat perception and descriptive norms are manipulated as absent, high, and low. Because we want to consider the role of social appraisals, it is important to examine whether they are absent versus present at high or low levels. In our experiment, others' threat perception was manipulated by the two co-workers' stated perceptions of the threat posed by the data breach. When others' threat perception is high, the two co-workers are seriously worried about the data breach whereas when it is low, they are not overly concerned about the data breach.

Descriptive norm is the behavior of two co-workers, talking that they engaged in UPSB when similar incidents occurred in the past. When descriptive norm is high, the two co-workers recall prioritizing and protecting the company's reputation over ethical considerations during a similar data breach happened. Conversely, when the descriptive norm is low, the two co-workers

recall prioritizing their morality and ethics over protecting company's reputation. Manipulation check items for threat perception, others' threat perception, descriptive norm are developed.

Pretest and Expert Panel Review

Before full data collection, a pretest was conducted to decide the appropriate measure for UPSB. This was a necessary step as this research is studying unexplored phenomena in the information security discipline, UPSB. To reflect on phenomena and appropriately measure them, we established three versions of UPSB scales. The pretest was conducted to decide the best scale to measure the operationalized phenomena. This pretest was conducted using undergraduate business students in April 2024 with ethics board (IRB) approval. Students were over 18 years old, and they were awarded extra credit for their participation. The IBM SPSS 28 software was used for the analysis. By comparing mean, standard deviation, Cronbach's alpha, composite reliability, and the average variance extracted from three different versions of unethical but pro-organizational security, a measure of UPSB that appropriately reflects the phenomena was identified.

Additionally, an expert panel review was conducted to assess the content validity of the scenario and measurement items. An expert panel consisting of IS faculty and PhD students was recruited. Expert panel members were asked to read the scenarios and measurement items and provided suggestions regarding the design of experiment. The scenarios and measurement items were revised based on the suggestions of expert panel members. The revised version was reviewed again to ensure content validity and face validity.

Construct Measurement

The dependent variable, UPSB intention, was determined through preliminary investigation. This variable will be assessed using a six-item scale with two dimensions:

commission and omission. The scale was adapted from the work of Umphress et al. (2010). The perceived severity of threat will be measured using a four-item scale (Posey et al. 2015).

Similarly, the perceived vulnerability of threat will be assessed using a four-item scale from Posey et al. (2015). Self-efficacy will be evaluated using a five-item scale, and response efficacy will be measured with a four-item scale, both adapted from Posey et al. (2015). A covariate, organizational identification, will be measured using a six-item scale (Mael and Ashforth 1992). To ensure the validity of the scenario-based experiment, a realism check and manipulation checks will be included.

DISCUSSION AND CONCLUSION

This research makes significant contributions to theory, research, and practice in the field of information security. First, this study advances the PMT by incorporating social aspects into its framework, thereby enriching PMT to better reflect the organizational environment.

Second, this research provides valuable insights by juxtaposing self-appraisal and social appraisal. By examining the interactions between self-appraisal and social appraisal and their influence on individuals' behaviors (i.e. UPSB), this study offers new perspectives on the complex interplay of personal and social factors in security behavior.

Moreover, this research delves into an often-overlooked phenomenon in the literature: UPSB. Although prevalent in practice, this behavior has received limited scholarly attention. By examining this grey area, the study sheds light on the nuanced and sometimes contradictory nature of actions that, while supporting organizational goals, may contravene ethical standards.

Lastly, this research contributes to practice and society by focusing on deviant security behaviors that have been neglected yet violate societal norms and values. By identifying these behaviors and their antecedents, the study provides practical guidance for organizations to

recognize and mitigate such actions. Furthermore, the findings can assist society and law enforcement agencies in understanding and addressing UPSB, ultimately promoting a more ethical and secure organizational environment.

REFERENCES

- Babalola, M.T., Mawritz, M.B., Greenbaum, R.L., Ren, S., and Garba, O.A. 2021. "Whatever It Takes: How and When Supervisor Bottom-Line Mentality Motivates Employee Contributions in the Workplace," *Journal of Management* (47:5), pp. 1134-1154.
- Bandura, A. 1977. *Social Learning Theory*. Englewood Cliffs: Prentice Hall.
- Chen, M., Chen, C.C., and Sheldon, O.J. 2016. "Relaxing Moral Reasoning to Win: How Organizational Identification Relates to Unethical Pro-Organizational Behavior," *Journal of Applied Psychology* (101:8), pp. 1082-1096.
- Cram, W.A., D'Arcy, J., and Proudfoot, J.G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525-554.
- Federal Trade Commission. 2021. "Data Breach Response: A Guide for Business." Retrieved June 20, 2024, 2024, from <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>
- Fehr, R., Welsh, D., Yam, K.C., Baer, M., Wei, W., and Vaulont, M. 2019. "The Role of Moral Decoupling in the Causes and Consequences of Unethical Pro-Organizational Behavior," *Organizational Behavior and Human Decision Processes* (153), pp. 27-40.
- Franceschi-Bicchierai, L. 2024. "23andme Tells Victims It's Their Fault That Their Data Was Breached." Retrieved April 7, 2024, from <https://techcrunch.com/2024/01/03/23andme-tells-victims-its-their-fault-that-their-data-was-breached/>
- Graham, K.A., Ziegert, J.C., and Capitano, J. 2015. "The Effect of Leadership Style, Framing, and Promotion Regulatory Focus on Unethical Pro-Organizational Behavior," *Journal of Business Ethics* (126), pp. 423-436.
- Johnston, A.C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.
- Jones, C. 2024. "Infosec Experts Divided over 23andme's 'Victim-Blaming' Stance on Data Breach." Retrieved April 7, 2024, from https://www.theregister.com/2024/01/04/23andme_victim_blaming_breach/
- Lowe, S. 2019. "Don't Buy a Breach: Ten Cybersecurity Red Flags to Look for During M&a Due Diligence." Retrieved April 7th, 2024, from <https://www.forbes.com/sites/forbestechcouncil/2019/02/12/dont-buy-a-breach-ten-cybersecurity-red-flags-to-look-for-during-ma-due-diligence/?sh=789b7ef4406e>
- Mael, F., and Ashforth, B.E. 1992. "Alumni and Their Alma Mater: A Partial Test of the Reformulated Model of Organizational Identification," *Journal of organizational Behavior* (13:2), pp. 103-123.
- Miao, Q., Newman, A., Yu, J., and Xu, L. 2013. "The Relationship between Ethical Leadership and Unethical Pro-Organizational Behavior: Linear or Curvilinear Effects?," *Journal of Business Ethics* (116), pp. 641-653.

- Mishra, M., Ghosh, K., and Sharma, D. 2022. "Unethical Pro-Organizational Behavior: A Systematic Review and Future Research Agenda," *Journal of Business Ethics* (179), pp. 63-87.
- Newman, L.H., and Greenberg, A. 2024. "Security News This Week: 23andme Blames Users for Recent Data Breach as It's Hit with Lawsuits." Retrieved April 7, 2024, from <https://www.wired.com/story/23andme-blames-users-data-breach-security-roundup/>
- Posey, C., Roberts, T.L., and Lowry, P.B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.
- Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91), pp. 93-114.
- Scherer, K.R., Schorr, A., and Johnstone, T. 2001. *Appraisal Processes in Emotion: Theory, Methods, Research*. New York: Oxford University Press.
- Tajfel, H., and Turner, J.C. 1979. "An Integrative Theory of Intergroup Conflict," in *Organizational Identity: A Reader*. New York: Oxford University Press, pp. 56-65.
- Trevino, L.K. 1986. "Ethical Decision Making in Organizations: A Person-Situation Interactionist Model," *Academy of Management Review* (11:3), pp. 601-617.
- Umphress, E.E., and Bingham, J.B. 2011. "When Employees Do Bad Things for Good Reasons: Examining Unethical Pro-Organizational Behaviors," *Organization Science* (22:3), pp. 621-640.
- Umphress, E.E., Bingham, J.B., and Mitchell, M.S. 2010. "Unethical Behavior in the Name of the Company: The Moderating Effect of Organizational Identification and Positive Reciprocity Beliefs on Unethical Pro-Organizational Behavior," *Journal of Applied Psychology* (95:4), pp. 769-780.
- Valinsky, J. 2024. "About 13,000 Home Security Customers Were Shown Someone Else's Home." Retrieved April 7th, 2024, from <https://www.cnn.com/2024/02/20/tech/wyze-breach-camera/index.html>
- Wang, T., Long, L., Zhang, Y., and He, W. 2019. "A Social Exchange Perspective of Employee–Organization Relationships and Employee Unethical Pro-Organizational Behavior: The Moderating Role of Individual Moral Identity," *Journal of Business Ethics* (159), pp. 473-489.
- Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.
- Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.
- Zhang, S. 2020. "Workplace Spirituality and Unethical Pro-Organizational Behavior: The Mediating Effect of Job Satisfaction," *Journal of Business Ethics* (161:3), pp. 687-705.