

Measuring Organization's Ability to Deter Insider Threat Through Situational Crime Prevention

Early stage paper

Tripti Singh

University of Alabama in
Huntsville
tripti.singh@uah.edu

Andrew S. Miller

University of Georgia
asmiller@uga.edu

Allen C. Johnston

University of Alabama
acjohnston5@ua.edu

Merrill Warkentin

Mississippi State University
m.warkentin@msstate.edu

ABSTRACT

Situational crime prevention (SCP) programs implement opportunity-reducing situational techniques that target specific insider threats, impacting the immediate environment via design, management, or manipulation. Deliberate insider threats are a form of workplace deviance that share characteristics with general criminal acts. This research-in-progress paper leverages SCP's opportunity-reducing techniques and provides a scale that organizations can employ to prevent or reduce insider threats. These five techniques are: increasing the required efforts to execute the crime, increasing the risk, reducing provocation, reducing reward, and removing excuses. We develop and present measurement scales for these opportunity-reducing techniques and test their utility in information security through five empirical studies, the last of which is in progress. Our primary contributions include developing and validating SCP's opportunity-reducing techniques scale in the context of information security, which increases researchers' understanding of this important phenomenon and offers managers a new tool to address this threat.

Keywords

Situational crime prevention, insider threat, prevention, deterrence, information security

INTRODUCTION

Organizations rely on the trust they place in their insiders – such as employees, internal contractors, temporary workers, and board members – to aid them in their business operations (Sharma and Warkentin 2019; Warkentin and Willison 2009). Insiders are anyone with access, privilege, and knowledge about an organization’s information systems (Anti and Vartiainen 2024). To ensure the business fulfills its strategic goals and operations, organizations provide their insiders with the information, access, and resources to complete their work professionally. This exchange is not solely transactional, but is instead a fundamental aspect of the business. However, employers’ trust in insiders may be misguided when insiders compromise the organization’s integrity, operations, and information security (Burns et al. 2019). Insider threats—defined as an “organizational member who is a ‘trusted agent’ within the firewall” (Warkentin and Willison 2009, p. 102)—pose significant risk. categorized insider threats on a continuum from passive, non-volitional noncompliance to intentional malicious computer abuse that may include sabotage, data theft, fraud, embezzlement, etc.

In response to the need to mitigate insider threats, existing information security studies based on protection motivation theory (PMT) and fear appeals emphasize the potential consequences of malicious actions and deter individuals from engaging in malicious acts (Boss et al. 2015; Johnston et al. 2015). In addition, deterrence approaches, informed by General Deterrence Theory (GDT), assert that implementing certain, severe, and swift countermeasures can reduce insider’s illicit or inappropriate behaviors (Cheng et al. 2013; D’Arcy et al. 2009; Herath and Rao 2009; Johnston et al. 2015; Straub and Welke 1998). While PMT and GDT provide great insight into why people do or do not commit information security policy violations, they do not fully inform the processes “left of bang” (Willison and Warkentin 2013) in which employees are motivated to engage in

deviant behavior and form the specific original intention. In addition, traditional security measures focus on remediation and detection approaches *after* insider incidents, which have proven insufficient to fully address these threats (Cram et al. 2019; Cram et al. 2017). Prior literature suggests that organizations can experience greater benefits by investing more in deterrence and prevention strategies than detection and remediation efforts after an event has transpired (Straub & Welke, 1998; Willison & Warkentin, 2013).

Situational Crime Prevention (SCP) provides a robust framework that proactively addresses insider threats by focusing on strategies for the very development of the desire to commit malicious acts within an organization (Beebe and Rao 2005; Clarke 1995; Ho et al. 2022; Jeong and Zo 2021; Willison and Siponen 2009). SCP focuses on opportunity-reducing techniques for designing, managing, and manipulating organizations' information security environments, making illicit or inappropriate behavior less rewarding, riskier, and more difficult (Padayachee 2016). Implementing SCP's opportunity-reducing techniques can significantly improve an organization's ability to safeguard its digital assets and maintain secure environments, which is essential for minimizing risk and achieving long-term organizational resilience. However, doing so requires a delicate balance between implementing SCP techniques and maintaining security without compromising employee morale (Jeong and Zo 2021).

To address this balance, a reliable method for measuring SCP factors is required. So, with this balance in mind, we seek to establish the first valid scale to assess how effectively SCP techniques achieve their goals in the workplace. With an adequate and valid quantification of these techniques, it is possible to determine their effectiveness in the target organization. With these metrics in hand, organizations will be equipped to direct efforts and resources into the most impactful techniques, while avoiding wasting resources on less impactful techniques. Measuring the effectiveness of

SCP techniques will also allow for continuous monitoring and improving an organization's security efforts. In terms of research impact, introducing the SCP scale will address a critical gap in the literature, providing a structured way to evaluate and compare the effectiveness of various SCP techniques within an organization. This achievement will aid scholars in identifying other gaps and areas for improvement in insider threat prevention.

LITERATURE REVIEW

The SCP theory, originating in criminology, focuses on reducing opportunities for crime rather than relying on prevention measures and punishment. SCP posits that criminals make rational decisions to commit crimes based on their perceived costs and benefits. Its goal is to prevent crime by manipulating the environment to increase the effort and risk of committing a crime while reducing its reward. SCP encompasses five key techniques: increasing the effort, increasing the risk, reducing the rewards, reducing provocations, and removing excuses (Clarke, 1995). Each technique has five sub-techniques, totaling 25 methods originally designed for the physical crime environment. These methods have since been adapted for the digital realm to address cybercrime challenges (Beebe and Rao 2005; Hinduja and Kooi 2013; Willison and Siponen 2009).

Effort in the context of SCP relates to the energy or force required to take action (Clarke 1995). Techniques aimed at increasing effort include target hardening, controlling exits, segregating duties, offsite data storage, and employing antivirus software (Padayachee 2016). Increasing risk involves enhancing the likelihood that criminal activities will be detected and punished. SCP suggests that higher detection risks reduce the likelihood of malicious actions, as perpetrators face greater chances of facing consequences (Clarke and Weisburd 1994; Cornish and Clarke 2003). Techniques to increase risk include reducing anonymity, enhancing formal surveillance, and using intrusion detection systems (Willison and Siponen 2009).

Reward in SCP refers to the benefits gained from an action, which may be monetary, tangible, or intangible (Clarke 1995). Techniques to reduce rewards include concealing or removing targets, denying benefits, and using digital signatures (Willison and Siponen 2009). Provocation involves actions that prompt a reactive response. SCP advocates for reducing provocations or removing noxious stimuli from the environment. Techniques to achieve this may include diminishing frustration and emotional arousal, as well as neutralizing peer pressure (Padayachee 2016). Lastly, removing excuses focuses on eliminating justifications for criminal acts. Techniques within this category include posting clear instructions and enforcing compliance (Hinduja and Kooi 2013; Willison and Siponen 2009).

Although developed in criminology, these SCP techniques have been adapted and applied to the context of information security (Beebe and Rao 2005; Ho et al. 2022; Padayachee 2016; Willison 2006; Willison and Siponen 2009). For example, Willison (2006) examined why employees commit information security policy violations and guided them on selecting effective safeguards to improve prevention programs. Padayachee (2016) conducted an exploratory evaluation of information security controls designed to reduce opportunities for insider threats. Willison and Siponen (2009) explored strategies to decrease employee violations using SCP principles, highlighting how SCP can inform and enhance information security practices. Beebe and Rao (2005) applied SCP to the information security context, offering new perspectives on enhancing IS security by reducing the rewards associated with criminal actions. Despite SCP's relevance to information security, current literature lacks a tool for assessing the effectiveness of SCP techniques within an organization. Hence, this paper addresses this gap by developing and empirically validating a scale to measure the effectiveness of techniques organizations can deploy to prevent insider threats. The following section discusses the development of this scale.

DEVELOPMENT AND VALIDATION OF A SCALE FOR SCP

Guided by prior literature, we developed an SCP scale to measure various opportunity-reducing techniques, following the methodologies outlined by (Churchill Jr 1979; MacKenzie et al. 2011; Moore and Benbasat 1991). Table 1 outlines the steps and their application across multiple studies. In study 1, we defined the domain of the scale, generated an initial set of items for each opportunity-reducing technique, and assessed content validity. In study 2, we established the factor structure of five SCP techniques and evaluated their validity. In study 3, we performed validity testing of the SCP techniques. In study 4, we validated these newly developed scales for these five SCP techniques and established their dimensionality. Study 5, currently in progress, aims to demonstrate the predictive validity of these SCP techniques within a nomological network. The following section provides a detailed discussion of these studies.

Study 1

The first step in developing SCP measures was to define the scale's domain through a literature review, following the guidance of Churchill Jr (1979). We reviewed SCP literature across information security and criminology, the latter being where SCP theory originated (Clarke 1995; Cornish and Clarke 2003; Ho et al. 2022; Willison and Siponen 2009). This ensured that definitions of the five opportunity-reducing techniques, along with the items subsequently developed, adequately encompassed the theoretical depth and breadth of the constructs (MacKenzie et al. 2011). Initially, we created four to six items for every SCP technique, carefully avoiding double-barreled items and ambiguous, unfamiliar terms to maintain simplicity and precision in each item.

Steps	Implementation
Conceptualization and Development of Measures	Study 1
1. Develop a conceptual definition of the SCP techniques	Round 1 Sample: Seven IS professionals adept in information security
2. Generate items to represent the five SCP techniques	Round 2 Sample: Nine IS professionals adept in information security
3. Assess the content validity of the items	
Model specification	Study 2
4. Formally specify the measurement model	Sample: 350 working professionals
Scale evaluation and refinement	Study 3
5. Collect data to conduct pretest	Sample: 148 working professionals
6. Scale purification and refinement	
7. Assess scale validity	
Validation	Study 4
8. Gather data from a new sample and reexamine the scale properties	Sample: 410 working professionals
9. Cross-validation and establishing predictive validity of SCP scale through nomological net	Study 5 Work in Progress

Note: Adapted from (Churchill Jr 1979; MacKenzie et al. 2011; Moore and Benbasat 1991)

Table 1: SCP Scale Development Process

We conducted two rounds of card-sorting to establish inter-rater reliability in mapping items of SCP techniques. Seven information security professionals participated in the first round, using the provided item descriptions and definitions of SCP techniques to allocate items to the most appropriate technique. Following established guidelines (MacKenzie et al. 2011; Moore and Benbasat 1991; Petter et al. 2007), we calculated inter-rater reliability using Fleiss' Kappa¹. The

¹ Fleiss Kappa is same as Cohen's kappa, but it allows computation of inter rater reliability of k -coders (MacKenzie et al. 2011)

initial Fleiss Kappa score was 0.198, indicating a slight level of agreement among raters (Landis and Koch 1977), with an overall placement ratio of items within the target SCP technique at 78% (see Table 2). After revising and removing items that failed to align with the five SCP techniques, we conducted a second card-sorting with nine IS professionals. This time, the Fleiss' Kappa score improved to 0.671, suggesting significant agreement among raters (Landis and Koch 1977), and the overall placement ratio of items within the target SCP technique increased to 97.15%. Following this successful validation, we proceeded to the first round of testing of the SCP scale, as discussed in Study 2.

Study 2

Study 2 defined the measurement model to outline the expected relationships between the items and their respective SCP technique (MacKenzie et al. 2011). We assessed the factor structure of the SCP scale using Exploratory Factor Analysis (EFA). Data were collected from 350 working professionals through a market research firm. We excluded 30 responses due to either incorrect answers to attention checks or participants being under the age of 18 years. Responses were gathered using a five-point Likert scale, ranging from strongly disagree (1) to strongly agree (5). The final sample consisted of 158 males and 164 females.

We employed Principal Component Analysis (PCA) with varimax rotation using SPSS v28 (Moore and Benbasat 1991). This approach yielded a two-factor solution (results not shown) with eigenvalues exceeding one, explaining 54.63% of the variance in the dataset. In the resulting two-factor model, the items related to increasing risk, removing excuses, and reducing rewards converged into a single factor. In contrast, items related to reducing provocation and increasing effort converged into a second factor. Given that the SCP scale in this research is grounded in extensive prior SCP research and is intended to capture specific conceptual meanings as a measure

of construct validity, these preliminary results indicate a potential lack of discriminant validity. This suggests the need for further revision and refinement to accurately represent the intended five-factor model, corresponding to the five opportunity-reducing techniques of SCP (Clarke 1995; Cornish and Clarke 2003; Ho et al. 2022; Willison and Siponen 2009).

SCP Techniques	Item Placement Ratio Round 1 (%)	Item Placement Ratio Round 2 (%)
Increase the risk	97.12	100
Increase the effort	71.43	97.78
Remove excuse	78.57	94.44
Reduce provocation	75	97.22
Reduce reward	67.86	96.29
Overall Placement	77.99	97.15

Table 2. Placement Ratio of Items Within Target SCP Technique

To revise the scale, we implemented several steps: 1) we revised ambiguous items that had similar meaning, 2) we removed items with low factor loadings (below 0.5), and 3) we ensured that each SCP technique had at least three or more items. Two information security professionals reviewed the revised items to verify their accuracy and validity. In Study 3, we retested these refined items using a newly collected dataset to assess the improvements in the scale's structure and validity.

Study 3 and 4

In Studies 3 and 4, we further refined and validated the SCP scale. The revised scale's items are available in Appendix A. For Study 3, we collected new data from a market research firm with a sample size of 148 participants to establish the factor structure for the five SCP techniques. The demographic breakdown of the dataset included a majority of participants (81%) holding some

level of college education, including associate's and bachelor's degrees, and 5.4% possessing a professional degree. The gender distribution was 59% male and 41% female. Regarding employment, 87.8% of the participants worked in the private sectors (both for-profit and nonprofit), government organizations employed 7.4%, and 4.8% were self-employed either in their incorporated or nonincorporated businesses.

In Study 3, we used PCA to generate factor loadings and assess cross-loadings. All factor loadings on the substantive techniques were above 0.70, indicating sufficient convergent validity (Field 2013; Fornell and Larcker 1981). We also used the same dataset to establish convergent and discriminant validity through the Average Variance Extracted (AVE) method, following the guidelines set by (Gefen et al. 2000). Each item's factor loading exceeded its cross-loading on any other technique as detailed in Table 3. The AVE for each technique, shown in Table 4, was above 0.50 and exceeded its correlation with other techniques, confirming an adequate level of both convergent and discriminant validity (Fornell and Larcker 1981; Gefen et al. 2000). Additionally, the internal consistency reliability, Cronbach's alpha of the measures surpassed the established threshold (Moore and Benbasat 1991; Nunnally 1978). Consequently, the scale was revised based on these findings, establishing validity and reliability.

N= 148			SCP Techniques				
	Mean	Standard Deviation	Reduce provocation	Reduce reward	Increase the risk	Remove excuse	Increase the effort
Provo1	4.25	0.961	0.966	-0.068	-0.001	0.088	0.089
Provo2	4.24	0.980	0.965	-0.061	0.045	0.056	0.104
Provo3	4.35	0.954	0.945	-0.056	0.031	0.063	0.133
Provo4	4.25	0.996	0.943	-0.016	0.029	0.048	0.052
Reward1	2.99	1.267	-0.073	0.946	0.039	0.076	0.091
Reward2	3.07	1.265	-0.059	0.934	0.034	0.148	0.110
Reward3	3.07	1.289	-0.034	0.946	0.057	0.087	0.100
Reward4	3.05	1.308	-0.036	0.948	0.019	0.092	0.109
Risk1	3.55	1.157	0.030	0.027	0.931	0.154	0.201
Risk2	3.64	1.184	0.023	0.049	0.915	0.160	0.204
Risk3	3.55	1.168	0.038	0.065	0.945	0.126	0.164
Risk4	3.42	1.184	0.013	0.007	0.847	0.215	0.174
Excuse1	3.49	1.169	0.090	0.125	0.177	0.865	0.268
Excuse2	3.47	1.181	0.086	0.136	0.215	0.870	0.246
Excuse3	3.51	1.221	0.043	0.072	0.172	0.889	0.227
Excuse4	3.56	1.156	0.064	0.122	0.140	0.890	0.245
Eff1	3.82	1.199	0.089	0.177	0.343	0.197	0.800
Eff2	3.89	1.120	0.118	0.105	0.199	0.354	0.848
Eff3	3.97	1.103	0.157	0.119	0.195	0.348	0.842
Eff4	4.00	1.069	0.110	0.112	0.179	0.230	0.873

Principal component analysis (PCA) with varimax rotation; reduce provocation (Provo); reduce the reward (Reward), increase the risk (Risk); remove excuse (Excuse); increase the effort (Eff)

Table 3. Results of Principle Component Analysis

SCP Techniques	Cronbach's Alpha	CR	AVE	Reduce provocation	Reduce the reward	Increase the risk	Remove excuse	Increase the effort
Reduce Provocation	0.959	0.974	0.903	0.951				
Reduce the reward	0.969	0.969	0.886	-0.094	0.942			
Increase the risk	0.959	0.950	0.905	0.082	0.118	0.951		
Remove excuse	0.955	0.955	0.842	0.172	0.261	0.395	0.918	
Increase the effort	0.949	0.969	0.886	0.249	0.267	0.459	0.637	0.910

Composite Reliability (CR); Average Variance Extracted (AVE); The bold values on the diagonals are the square root of AVE

Table 4. Test for Validity and Reliability

In Study 4, we continued to assess the scale by establishing the dimensionality of the five techniques through model comparison tests. We collected new data from 413 working professionals knowledgeable about their organization's information security policies and procedures. Using AMOS v28, we specified a measurement model and conducted a series of Confirmatory Factor Analyses (CFA). The demographic profile of the sample included 20% holding a two-year degree and 54% possessing a bachelor's or professional degree. The gender distribution was 43% male and 57% female. Regarding employment, 76.8% of the participants were employed in private (for-profit or nonprofit) organizations, 11.6% in government organizations, 10.1% were self-employed in their incorporated or nonincorporated businesses, and 1.5% worked in family businesses.

We estimated three models to establish the dimensionality of our scale: (1) Model 1, a first-order factor model of SCP scale, which accounts for the variance among all twenty items across the five SCP techniques; (2) Model 2, a freely correlated first-order model where twenty items are grouped into the five SCP techniques—reduce provocation, reduce reward, increase risk, remove

excuses, and increase effort; and (3) Model 3, a second-order reflective model of SCP. Table 5 presents each item's mean, standard deviation, and standardized factor loadings across these three models.

To determine the dimensionality of the technique, we compared the fit of three different models using established model fit criteria (Gefen et al. 2011; Hu and Bentler 1999). Model 1 is a unidimensional model where all items load onto a single technique. Model 2 is a first-order reflective model where items are loaded onto their respective technique. Model 3 is a second-order reflective model where five techniques are treated as individual dimensions of a second-order SCP scale. For model comparison, we utilized the χ^2/df ratio as a simplified heuristic, aiming for a ratio less than 3:1 (Gefen et al. 2000). We also considered the Adjusted Goodness of Fit Index (AGFI) and the Goodness of Fit Index (GFI), noting that these indices are biased towards sample size and tend to show better results as the sample size increases (Gefen et al. 2011). Given the drawbacks of using GFI (Sharma et al. 2005), we focused on the Comparative Fit Index (CFI), Tucker Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA), and Akaike Information Criteria (AIC) to assess our models. AIC is a relative estimator that compares models to identify the one with the lowest AIC as the preferred choice. The results of these comparisons are summarized in Table 6.

Items	Mean	S.D.	Unidimensional Model: Standardized Factor Loadings ($p<.001$)	First Order Factor Model: Standardized Factor Loadings ($p<.001$)	Second Order Factor Model: Standardized Factor Loadings ($p<.001$)
Provo1	4.20	0.963	0.445	0.913	0.913
Provo2	4.19	1.005	0.440	0.906	0.905
Provo3	4.20	0.996	0.455	0.877	0.878
Provo4	4.20	1.035	0.462	0.866	0.867
Reward1	3.39	1.219	0.413	0.807	0.807
Reward2	3.72	1.083	0.471	0.814	0.815
Reward3	3.55	1.174	0.471	0.895	0.895
Reward4	3.51	1.159	0.450	0.875	0.875
Risk1	3.81	1.098	0.816	0.915	0.915
Risk2	3.86	1.087	0.826	0.913	0.913
Risk3	3.75	1.123	0.809	0.885	0.884
Risk4	3.69	1.134	0.759	0.78	0.780
Excuse1	3.63	1.095	0.646	0.798	0.797
Excuse2	3.63	1.084	0.685	0.855	0.851
Excuse3	3.58	1.148	0.661	0.805	0.809
Excuse4	3.67	1.092	0.694	0.853	0.854
Eff1	3.92	1.107	0.691	0.736	0.734
Eff2	3.92	1.068	0.721	0.861	0.862
Eff3	3.97	1.018	0.672	0.791	0.792
Eff4	3.77	1.160	0.588	0.646	0.647

Standard Deviation (S.D.); Reduce provocation (Provo); Reduce the reward (Reward), Increase the risk (Risk); Remove excuse (Excuse); Increase the effort (Eff)

Table 5. Mean, Standard Deviation, and Standardized Factor Loadings

Table 6 indicates that Models 2 and 3 outperform Model 1 in terms of fit. Models 2 and 3 are comparable; however, Model 2 demonstrates a slightly better fit, and the AIC increases from Model 2 to Model 3. Based on this analysis, Model 2, which represents the five individual SCP techniques as individual dimensions of SCP, emerges as the best-fitted model. This finding aligns with prior literature, suggesting that the five opportunity-reducing techniques function independently within the SCP scale.

Fit Indices	Cut Off Criterion	Model 1: Unidimensional Model	Model 2: First-Order Reflective Model	Model 3: Second Order Reflective Model
χ^2/df	<3	19.134	1.784	1.915
CFI	>.90	0.512	0.98	0.976
TLI	>.90	0.455	0.976	0.973
RMSEA	<.08	0.21	0.044	0.047
AIC		3332.78	385.436	405.902

Table 6: Establishing Dimensionality of Five Opportunity Reducing Techniques

FUTURE DIRECTIONS

Subsequent to these activities, we will integrate these opportunity-reducing techniques into a nomological network to test their predictive ability. We will identify relevant constructs and delineate their relationships within this network, gather appropriate valid new data, and analyze the relationships using structural equation modeling to validate the model. This process will help us assess the efficacy and interconnectivity of the SCP techniques within a broader theoretical framework. The process will reveal new avenues for understanding prediction, as well as new pathways for further research.

CONCLUSION

This research-in-progress study develops an assessment tool to measure an organization's ability to prevent insider threats through proactive measures. By creating and validating a scale explicitly designed for the information security context, we provide a scale that employers can use to mitigate insiders' intentions to act against the organization.

The empirical validation of this scale for SCP's opportunity-reducing techniques underscores their practicality and relevance and significantly contributes to research focused on insider threat mitigation. Our results offer valuable insights for both practitioners and researchers. Furthermore, this scale advances theoretical knowledge in crime prevention, ensuring that mitigation efforts are effective. Our work also enriches academic discourse by extending the applications of SCP. Specifically, we develop actionable and reliable scales that can be utilized and expanded in future research to explore insider threat mitigation further.

Appendix A: Final Items for SCP Scale

Opportunity Reducing Techniques	Definition	Conceptual Domain	Source	Items
Reduce Provocations	The perceived causes or catalysts of humans committing policy violations.	Criminal Justice	(Clarke 1995; Willison and Siponen 2009)	Provo1: My organization is fair towards employees. Provo 2: My organization treats employees fairly. Provo 3: My organization treats employees appropriately. Provo4: My organization treats its employees equitably.
Reduce Rewards	The benefits of committing a policy violation, including both monetary and internal benefits	Criminal Justice	(Clarke 1995; Clarke and Weisburd 1994; Ekblom and Tilley 2000)	Reward1: My organization is careful to hide the real value of its digital assets from its employees. Reward2: My organization protects the real value of its digital assets from its employees. Reward 3: My organization takes precautions to conceal the real value of its digital assets from its employees. Reward4: My organization takes steps to obfuscate the real value of its digital assets to its employees.
Increase Risks	The downsides of committing a policy violation, including both formal and informal punishments	Criminal Justice	(Clarke 1995; Clarke and Weisburd 1994; Ekblom and Tilley 2000)	Risk 1: My organization punishes offenders for breaking its rules. Risk 2: My organization penalizes offenders for breaking its rules. Risk 3: My organization punishes offenders for not following its rules. Risk 4: My organization sanctions violators of its rules
Remove Excuse	The ability of people to rationalize policy violations	Criminal Justice	(Clarke 1995; Willison and Siponen 2009)	Excuse 1: My organization has reduced the number of reasons that employees could give for violating its policies. Excuse 2: My organization has minimized the justifications employees can give for violating its policies. Excuse 3: My organization has decreased the possibility for employees to give explanations for violating its policies. Excuse 4: My organization has limited the excuses employees could give for violating its policies.
Increase Effort	The amount of energy required to commit a policy violation	Criminal Justice	(Clarke 1995)	Effort 1: My organization has taken steps to increase the effort required by its employees to violate its policies. Effort 2: My organization has taken measures to make it more difficult for its employees to violate its policies. Effort 3: My organization has taken initiatives to make it harder for its employees to violate its policies. Effort 4: My organization has put in place obstacles for its employees to violate its policies.

REFERENCES

- Anti, E., and Vartiainen, T. 2024. "Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review," *Communications of the Association for Information Systems* (55), pp. 1-36.
- Beebe, N. L., and Rao, V. S. 2005. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security," *Proceedings of the 2005 SoftWars Conference, Las Vegas, NV*, pp. 1-18.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837-864.
- Burns, A. J., Roberts, T. L., Posey, C., and Lowry, P. B. 2019. "The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking," *Information Systems Research* (30:4), pp. 1228-1247.
- Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. "Understanding the Violation of Is Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory," *Computers & Security* (39), pp. 447-459.
- Churchill Jr, G. A. 1979. "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research* (16:1), pp. 64-73.
- Clarke, R. V. 1995. "Situational Crime Prevention," *Crime and Justice* (19), pp. 91-150.
- Clarke, R. V., and Weisburd, D. 1994. "Diffusion of Crime Control Benefits: Observations on the Reverse of Displacement," *Crime Prevention Studies* (2:1), pp. 165-184.
- Cornish, D. B., and Clarke, R. V. 2003. "Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention," *Crime Prevention Studies* (16), pp. 41-96.
- 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.
- Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605-641.
- 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* (20:1), pp. 79-98.
- Eckblom, P., and Tilley, N. 2000. "Going Equipped," *The British Journal of Criminology* (40:3), pp. 376-398.
- Field, A. 2013. *Discovering Statistics Using Ibm Spss Statistics*, (4 ed.). London: Sage.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.
- Gefen, D., Rigdon, E. E., and Straub, D. 2011. "An Update and Extension to Sem Guidelines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.
- Gefen, D., Straub, D., and Boudreau, M.-C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the ACM* (4:7), pp. 1-77.
- Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

- Hinduja, S., and Kooi, B. 2013. "Curtailling Cyber and Information Security Vulnerabilities through Situational Crime Prevention," *Security Journal* (26), pp. 383-402.
- Ho, H., Ko, R., and Mazerolle, L. 2022. "Situational Crime Prevention (Scp) Techniques to Prevent and Control Cybercrimes: A Focused Systematic Review," *Computers & Security* (115), p. 102611.
- Hu, L. t., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1-55.
- Jeong, M., and Zo, H. 2021. "Preventing Insider Threats to Enhance Organizational Security: The Role of Opportunity-Reducing Techniques," *Telematics and Informatics* (63), p. 101670.
- Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework : Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.
- Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), pp. 159-174.
- MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in Mis and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293-334.
- Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.
- Nunnally, J. 1978. *Psychometric Theory*, (2 ed.). New York, NY: McGraw-Hill.
- Padayachee, K. 2016. "An Assessment of Opportunity-Reducing Techniques in Information Security: An Insider Threat Perspective," *Decision Support Systems* (92), pp. 47-56.
- Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.
- Sharma, S., Mukherjee, S., Kumar, A., and Dillon, W. R. 2005. "A Simulation Study to Investigate the Use of Cutoff Values for Assessing Model Fit in Covariance Structure Models," *Journal of Business Research* (58:7), pp. 935-943.
- Sharma, S., and Warkentin, M. 2019. "Do I Really Belong?: Impact of Employment Status on Information Security Policy Compliance," *Computers & Security* (87), p. 101397.
- Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.
- 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. 2006. "Understanding the Perpetration of Employee Computer Crime in the Organisational Context," *Information and Organization* (16:4), pp. 304-324.
- Willison, R., and Siponen, M. 2009. "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention," *Communications of the ACM* (52:9), pp. 133-137.
- Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.