Anger or Fear? Effects of Discrete Emotions on Deviant Security Behavior

Research in Progress

Feng Xu

Xi'an Jiaotong University & The University of New Mexico

fxu@unm.edu

Xin Luo

The University of New Mexico

xinluo@unm.edu

Carol Hsu

Tongji University

carolhsu@tongji.edu.cn

Abstract

Deterrence theory has received considerable attention in recent years. However, scholars have begun to call for research beyond the deterrence approach on security behaviors, and argue that the theory of emotion should not be omitted from information systems security decision making [15, 81]. In this research, we examine and distinguish effects of anger and fear on perceived costs of sanctions and deviant security behavior. A research model is developed based on deterrence theory and cognitive appraisal theory of emotion. We propose to design a scenario of introducing a new security monitoring system, to analyze the interplays of anger, fear, perceived certainty, perceived severity of sanctions and deviant security behavior. The results will have important implications for comprehensively understanding employees' deviant security behavior.

1. Introduction

According to the recent Intel Security Report [14], more than 43% of security breaches are caused by insider employees. For example, intellectual property theft which is caused by current and former employees costs US companies $250 billion per year [65]. The insider threat is regarded as one of the largest threats to organizations [75, 81]. To reduce the insider threat, organizations have taken efforts to develop and implement stringent monitoring and control activities, information security policies (ISPs), and sanctions to deter security threat behaviors. Based on general deterrence theory (GDT), extant studies have found that security countermeasures increase employees' perceived certainty and severity of sanctions [35, 72], which are negatively associated with deviant security

behavior, such as IT misuse or computer abuse [24, 39, 56].

Prior research focuses largely on compliant behaviors versus security policies for employees [3, 67, 75, 76, 81]. In essence, those studies attempted to examine factors which can maximize the deterrence effect and reduce employees' noncompliance behaviors. Yet findings of the literature are rather mixed and ambiguous. Although security countermeasures are found to decrease employees' security threat behaviors [21, 24], these security efforts may also increase security threat behaviors [52, 57]. For example, several studies have indicated that the increased severity of sanctions negatively influence employees' compliance intention [38, 39].

Recent studies suggest that organizations need an extended security action cycle to understand offenders' thought processes [80, 81], and find that other organizational or individual factors might have a significant effect on IS security behaviors [79]. Willison and Warkentin [81] point out that phenomena beyond the security action cycle has rarely been studied by IS researchers and in particular, "examining the relationship between emotions and deterrence would represent a new stream of research for the IS security field" (p.10). For example, continual enhancements to security countermeasures can be stressful and disruptive to employees' work routines [23]. In the organization, an event which is appraised as stressful by employees would induce negative emotions which may lead to deviant behaviors [7, 8]. Therefore, there is a pressing need to integrate emotional factors and cognitive factors to further study IS security behaviors [81].

In this paper, we design a scenario of introducing a new security monitoring system to investigate employee responses to stressful events. Based on this, we try to examine the deviant security behavior of employees in organizations. Deviance refers to

HICSS

"voluntary behavior of organizational members that violates significant organizational norms, and in so doing, threatens the well-being of the organization and/or its members" [59]. To advance this line of research, we propose to integrate general deterrence theory and negative emotional reactions (i.e., anger vs. fear) in predicting employees' deviant security behavior in organizations. We aim to empirically validate and distinguish the effect of anger and fear on perceived costs of sanctions and deviant security behavior.

Drawing on deterrence theory [72] and cognitive appraisal theory of emotion [33], we develop a framework in an effort to examine interplays of employees' emotions and organizational sanctions vis-à-vis deviant security behavior. We conjecture that both negative emotions (i.e., anger and fear) and perceived sanctions impact deviant security behavior. In addition, we argue that negative emotions influence employees' rational evaluations towards security countermeasures in organizations. That is, we posit that anger and fear have a contradicting impact on perceived certainty and severity of sanctions. Furthermore, we predict that negative emotion moderates the relationship between sanctions on deviant security behavior. In essence, we assume that the effect of sanctions decreases with a high level of anger and the effect of sanctions increases with a high level of fear.

In the following section, we review related literature and develop a theoretical model. Then, we describe our proposed methodology and expected findings. Finally, we present the contribution and discuss future research.

2. Literature Review

2.1. IS Security Behaviors

In general, IS security behaviors refer to "behaviors of employees in using organizational information systems, and such behavior may have security implications" [36]. There are many examples of IS security behaviors, such as compliance or noncompliance with IS security policy [13, 17, 39, 52, 58], computer abuse [43, 53], and IT misuse [24], etc.

Organizations that identify factors influencing employees' IS security behaviors gain a strategic advantage by improving overall security [2, 38, 70]. Recent IS security research has devoted considerable efforts to investigating factors affecting employees' security behaviors through a plethora of theoretical lens, including General Deterrence Theory [17, 24, 39, 41, 71, 72], Protection Motivation Theory [2, 9, 19, 39,

47, 67], Rational Choice Theory [13, 41], Reactance and Justice Theory [52, 53, 57, 77], Accountability Theory [75, 76], Theory of Reasoned Action [37, 67], Cognitive Evaluation Theory [67], Coping Theory [23], Compliance Theory [17], Neutralization Theory [68], and Principal Agent Theory [38].

A significant number of IS security research has investigated the effectiveness of deterrence on employee security behaviors (see Table 1). For example, D'Arcy, Hovav and Galletta [24] predict that perceived certainty and severity of sanctions negatively influence IS misuse behavior. However, other studies argue that perceived severity of punishment negatively impact employee security policy compliance intention [38, 39]. Hu, Xu, Dinev and Ling [41] and Siponen and Vance [67] point out that perceived certainty and severity of sanctions have no significant impact on the intention of security policy violation. The perceived costs of sanctions have an ambivalent conclusion on employee security behaviors.

In criminology, prior literature emphasizes the role of situational and emotional variables. Criminological scholars suggest that omitting the effect of emotion from the decision making may lead to inconsistent and incomplete results [15, 29, 81]. In the IS literature, the effect of emotions has received increasing attention [83]. For example, Zhang and Li [84] suggest that perceived affective quality positively influences perceived usefulness and perceived ease of use. Deng and Poole [26] note that the design of webpage enhances users' positive emotions and facilitates subsequent psychological state and behaviors. Hwang and Kim [42] point out that enjoyment and anxiety mediate the relationship between perceived web quality and e-trust. Most recently, Yin, Bond and Zhang [82] examine the importance of discrete emotions on online review. They compare the different effects of anxiety and anger on perceived helpfulness of online review.

In the context of IS security, some studies began to explore the effect of emotion on security behaviors have attempted to investigate the phenomena such as emotion and computer abuse [43] and emotion coping and threat avoidance behaviors [49]. In particular, Kim, Park and Baskerville [43] suggest that abuse-positive affect positively influences abuse intention. Liang and Xue [49] point out that employees would focus more on emotion-focused coping strategy if they consider that the situation cannot be controlled. However, there is a paucity of empirical research studying the mechanism of emotions and IS security behaviors. In order to advance this research, this study is attempting to investigate interaction effects of discrete emotions (anger vs fear) and perceived certainty and severity of

sanctions on deviant security behavior, particularly in organizational settings.

Table 1. Literature Review of the Relationship between Deterrence and Security Behaviors

Author	Theory	Variable	Conclusion
Straub [71]	General Deterrence Theory	Investment in Security Countermeasures; Computer Abuse	Investment in security countermeasures is negatively associated with computer abuse.
D'Arcy, Hovav and Galletta [24]	General Deterrence Theory	Perceived Certainty; Perceived Severity; IS Misuse Intention	Perceived severity negatively influence IS misuse intention.
Lee, Lee and Yoo [46]	General Deterrence Theory; Social Control Theory	Security Policy; Insiders' Abuse	Security policy has no significant effect on insiders' abuse.
Siponen and Vance [68]	General Deterrence Theory; Neutralization Theory	Formal Sanctions; Informal Sanctions; IS Security Policy Violation Intention	Formal sanctions and informal sanctions have no significant impact on IS security policy violation intention.
Hu, Xu, Dinev and Ling [41]	General Deterrence Theory; Rational Choice Theory	Certainty of Sanction; Severity of Sanction; Celerity of Sanction; IS Security Policy Violation Intention	Certainty, severity, celerity of sanctions have no significant effect on intention to commit policy violations.
Herath and Rao [38]	Deterrence Theory	Severity of Penalty; Certainty of Detection; IS Security Policy Compliance	The certainty of detection is positively and the perceived severity of penalty is negatively related to IS security policy compliance.
Herath and Rao [39]	Protection Motivation Theory; Deterrence Theory	Severity of Punishment; Detection Certainty; IS Security Policy Violation Intention	The certainty of detection positively and punishment severity negatively affect IS security policy compliance.

2.2. Nature of Emotion

Emotion is one specific type of state affect, which presents affective experiences [78]. Compared with trait affect, state affect influences cognition with different patterns and mechanisms [34]. The induction of emotion has specific targets, whereas mood is an affective state which is generalized and lower intense [32].

There are two prominent approaches to characterize emotions. Dimensional theories assume that valence and arousal are important dimensions to capture emotions [62]. Emotion in general influences perceived costs and benefits of crimes [11, 51]. For example, negative emotions in general lead to cautious behaviors no matter whether emotion is anger or fear. However, the dimensional view of emotions has been challenged [69]. There are many emotions that cannot be captured by valence and arousal [28]. For example, although anger and fear are similar on the dimensions of valence, they lead to different behaviors [12].

Other works on emotion have concentrated on cognitive judgment under different emotions [64, 69]. This theory argues that different interpretations of situations lead to different emotions [31, 61]. For example, employees monitored by security countermeasures might interpret the event as punishment which may lead to fear or as the loss of control which may result in anger. Under different emotional states, individuals view threats of sanction differently [86]. For example, when individuals experience anger, they will not consider future punishments of their behaviors and focus on current emotional states. However, when individuals are fearful, they may be more afraid of future punishments.

2.3. Anger and Fear

Based on the appraisal dimensions of emotion, anger and fear are similar in pleasantness appraisal but they differ considerably in the appraisal of certainty [30, 69]. For instance, anger arises from stressful events which are appraised as certain (i.e., individuals are clear of what happened and can predict what may happen in the future). However, fear arises from stressful events which are appraised as uncertain (i.e., individuals cannot predict what will happen) [73].

In support of appraisal view, studies in criminology literature have explored the effect of anger and fear on individual offending decisions. For example, Lerner and Keltner [48] suggest that fearful individuals assess risky situations negatively and are more likely to reduce risky decision making. Conversely, angry individuals are more certain of risky situations and are more likely to take risk seeking decision making. In

addition, prior research suggests that feelings of fear prevent offenders from intended crimes [12, 20]. The effect of fear on offending decisions increases the effectiveness of deterrence policies and intervention. However, prior research has shown that anger reduces the effectiveness of sanctions [4-6, 15, 85] and is more likely to lead to offending behaviors [12, 27, 55]. Therefore, anger and fear have different effects on sanctions and security behaviors.
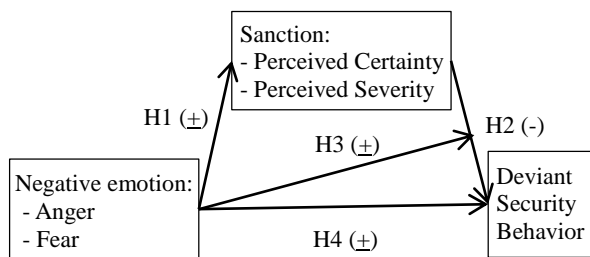
3. Research Model

Figure 1. An Integrated Emotion and GDT Model

Damasio [25] suggests that high (or low) levels of emotion can lead individuals to make irrational decisions, which are not in their best interests. When individuals experience intense emotion, they usually irrationally think and inappropriately evaluate costs and benefits [86]. This observation is consistent with the issue of bounded rationality [16, 66]. Bouffard, Exum and Paternoster [10] note that emotional states could be important factors influencing rational decision making. Individuals experiencing high emotional intensity will irrationally assess perceived costs and benefits. For example, intense emotional states may cause individuals to focus on how to cope with emotions and ignore concerns which normally inhibit behaviors. Based on deterrence theory and cognitive appraisal theory of emotion, we integrate emotions and deterrence to predict employee security behaviors. The model is depicted in Figure 1.

Prior research notes that different emotions have different impact on behaviors [48]. Anger and fear differs in the dimension of certainty. Lerner and Keltner [48] suggest that individuals experiencing fear would negatively appraise the situation and this uncertain emotion would lead to more cautious decision making. In other words, fearful individuals would be more likely to reduce risky behaviors. Conversely, individuals experiencing anger are certain of what is happening and emotion may cause quick and heuristic decision making. Prior criminological research indicates that anger reduces and fear increases

perceived costs [4, 5, 85] and those emotions lead to different behaviors [55].

In IS security context, based on appraisal tendencies, individuals experiencing anger appraise the stressful situation quickly and are more likely to lead to decreased cost perceptions. In contrast, individuals experiencing fear appraise the stressful situation carefully and are more likely to increase perceived costs of sanctions.

Therefore, we propose that anger negatively and fear positively influences individual perceived certainty and severity of sanctions.

H1a: Anger will be negatively associated with perceived certainty of sanctions.

H1b: Anger will be negatively associated with perceived severity of sanctions.

H1c: Fear will be positively associated with perceived certainty of sanctions.

H1d: Fear will be positively associated with perceived severity of sanctions.

General Deterrence Theory predicts that certainty and severity of sanctions deter individuals from illicit act [35]. In this study, according to D'Arcy, Hovav and Galletta [21], we refer "certainty of sanctions to the probability of being published, and severity of sanctions to the degree of punishment" associated with deviant security behavior. Prior deterrence research shows that sanctions negatively impact individual criminal and deviant behaviors [54]. For example, perceived certainty and severity of sanctions are negatively related to employee intention to engage in deviant behaviors [18, 40, 54].

The IS security literature has found that perceived certainty and severity of sanctions negatively influence IT deviant behaviors [22, 24, 39]. For example, Straub [71] points out that security countermeasure investment is negatively associated with computer abuse. D'Arcy, Hovav and Galletta [21] predict that perceived severity of sanctions negatively influences IS misuse intention. Herath and Rao [38] and Herath and Rao [39] suggest that the detection certainty has a positive relationship with IS security policy compliance intention. Therefore, we predict that perceived certainty and severity of sanctions are negatively associated with employee deviant security behavior.

H2a: Perceived certainty of sanctions will be negatively associated with employee deviant security behavior.

H2b: Perceived severity of sanctions will be negatively associated with employee deviant security behavior.

In addition, prior studies found support for the moderating effect of emotions on decision making [15, 27]. For example, Loewenstein [50] suggests that

emotions influence offending behaviors and the level of influence is proportionate to the emotion level. Therefore, individuals experiencing strong emotions will behave contrary to their rational considerations. Carmichael and Piquero [15] conclude that anger moderates the relationship between cognitive variables and offending behaviors. The results show that anger positively influences the effect of perceived thrills on assault intentions, while it negatively influences the effect of sanctions on assault intentions. Therefore, under a high level of anger, sanctions inhibit aggressive behaviors. Exum [27] suggests that although anger does not lead to aggressive intentions independently, it moderates the relationship between alcohol and aggression. The result shows that an intoxicated group in the anger-provoking situation reports significant higher aggressions than those in the no-anger situation.

Therefore, in the IS security context, we posit that security countermeasures may have no effect on employee deviant security behavior when individuals are under higher anger, For example, anger is more likely to influence the cognitive performance consequences of employee behaviors. Individuals experiencing anger are more likely to take actions contrary to their self-interest. In contrast, individuals who are under fear are more likely to overestimate costs of their behaviors. Under high fear, the effect of security countermeasures on security behaviors would be enhanced. Boss, Galletta, Lowry, Moody and Polak [9] point out that fear appeals would be a good supplement to IS security policy. Organizations can use fear appeals to prevent users from violating security policies. Therefore, we propose that anger negatively moderates the effect of perceived certainty, severity of sanctions on deviant security behavior and fear positively moderates this relationship.

H3a: Anger will negatively moderate the effect of perceived certainty of sanctions on employee deviant security behavior.

H3b: Anger will negatively moderate the effect of perceived severity of sanctions on employee deviant security behavior.

H3c: Fear will positively moderate the effect of perceived certainty of sanctions on employee deviant security behavior.

H3d: Fear will positively moderate the effect of perceived severity of sanctions on employee deviant security behavior.

Loewenstein [50] proposes that state emotion directly influences behaviors. Negative affect induced by stressful events is more likely to lead to negative behaviors [7, 8]. For example, Lee and Allen [45] estimate the direct and positive relationship between negative affect and deviant behaviors in the workplace..

According to the perspective of "appraisal tendency", Lerner and Keltner [48] find that fear and anger have different effects on behaviors because they interpret events or situations differently. Individuals experiencing anger exhibit more risk seeking behaviors. For example, Bouffard [12] suggests that anger has a direct and positive effect on offending behaviors. Rodell and Judge [60] note that anger positively mediates the relationship between hindrance stressors and counterproductive behaviors. In contrast, fearful individuals give more negative assessments of risky behaviors, and would lead to less risky choices [63]. For instance, Boss, Galletta, Lowry, Moody and Polak [9] predict that fear negatively influences anti-malware software use intention.

Therefore, we propose that employees experiencing anger are more likely to increase deviant behaviors such as purposely violating security policies. In contrast, employees experiencing fear would like to reduce deviant security behaviors.

H4a: Anger will be positively associated with employee deviant security behavior.

H4b: Fear will be negatively associated with employee deviant security behavior.

4. Proposed Research Method

We propose to employ the scenario-based factorial survey to test the research model. We select the scenario-based method for several reasons.

First, Klepper and Nagin [44] point out that scenario-based method is useful for employee behaviors because it incorporates details of the situation. Scenario-based method ensures that respondents' decision making is almost close to the reality and keeps the uniformity of contextual details [1]. Second, scenario-based method provides an indirect way to measure employee responses to stressful events and deviant security behaviors, which are difficult to measure directly [74].. Therefore, the scenario-based method is used widely in IS security research [24, 41, 68, 75, 76].

According to scenarios designed by Lowry and Moody [52], Siponen and Vance [68] and Vance, Lowry and Eggett [75], we expect to design scenarios to analyze employees responses to the introduction of new security monitor system. Below is an example of the scenario.

Management has decided to introduce a new computer-monitoring system to look for and identify people who may be breaking company policy. The new system will continually monitor and trace all

employees' computer and network use. All employees will be checked for computer-rule violations by managers. Managers have discretion concerning how to discipline employees who are caught violating computer policy. All employees must follow and adhere to it immediately with no compliant, dispute, and questions asked.

The procedures include two phases. In the first phase, each subject is provided scenarios corresponding to introducing a new security monitoring system and will be asked to read the scenarios. Scenarios are regarded as an unintimidating way to react to sensitive issues [54]. In the second phase, each subject will be asked to complete an online questionnaire which measures anger and fear, perceived certainty, perceived severity, and deviant security behaviors. Each subject will be asked to provide demographic information.

The proposed data collection plan will be implemented in summer 2016. We plan to send email invitations to work professionals for an online survey. A total of 300 datasets will be solicited. We will use survey instrument for data collection. Scales for perceived certainty and perceived severity are each adapted from Peace, Galletta and Thong [56] and D'Arcy, Hovav and Galletta [24]. Anger and fear are measured from Bouffard [12].

5. Expected Findings

Based on the above analysis, we expect to deeply investigate interplays between emotions and sanctions vis-à-vis deviant security behavior. We hope to unveil several interesting findings.

First, we expect that negative emotions (anger and fear) have direct influences on deviant security behavior. Specially, anger has a negative effect on deviant security behavior and fear has a positive effect on deviant security behavior. It indicates that different emotions have a unique effect on IS security behaviors.

Second, we expect that negative emotions have an indirect effect on deviant security behavior, partially mediated by perceived certainty and severity of sanctions. Emotion can alter employees' costs perceptions, then influences their security behaviors. Specially, anger decreases their perceived certainty and severity of sanctions whereas fear increases their perception of sanctions.

Third, we expect that negative emotions moderate the effect of perceived certainty, severity of sanctions on deviant security behavior. Specially, under a high emotional state of anger, perceived certainty and severity of sanctions have less impact on deviant security behavior. In contrast, under a high emotional

state of fear, perceived certainty and severity of sanctions have higher impact on deviant security behavior.

6. Expected Contribution and Future Work

This study integrates deterrence theory and cognitive appraisal theory of emotion. The theoretical marriage will significantly contribute to IS security research.

First, we provide a more complete model to understand employees' deviant security behavior by integrating emotional and cognitive factors. Willison and Warkentin [81] put forward that "the fact that phenomena which exist temporally prior to deterrencee have rarely been addressed by IS researchers" (p.5). Among their suggested research directions, this study particularly echoes their call for additional studies "examining the relationship between emotions and deterrence would represent a new stream of research for the IS security field" (p.10).

Second, we examine and distinguish the direct effect of discrete emotions (anger and fear) on IS deviant security behavior. This helps to understand the underlying mechanism of different types of emotion and is instrumental to future IT security research. The different effect of anger and fear on employee cognition and security behaviors will support the cognitive appraisal theory of emotion [64, 69].

Third, we estimate the moderating effect of discrete emotions (i.e., anger and fear) on deviant security behavior. This new path may help address the inconsistent conclusion between deterrence variables and security behaviors. In this context, anger and fear have an ambivalent effect. This study will partially explain why perceived severity has both positive and negative effect on deviant security behaviors studied in prior research [24, 39, 56].

In essence, emotion has been recently considered as an important factor in influencing IS security behaviors [49, 81]. Future research should take more efforts to understand IS security behaviors by considering the interaction between emotions and cognitive factors. The integration of emotion in deterrence theory, as proposed in this study, would provide good guidance to organizations to better understand and control employees' security behaviors and enhance corporate security.

7. References

[1] C. S. Alexander, and H. J. Becker, "The use of vignettes in survey research", Public Opinion Quarterly, 42

(1), 1978, pp. 93-104.

[2] C. L. Anderson, and R. Agarwal, "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", MIS Quarterly, 34 (3), 2010, pp. 613-643.

[3] J. B. Barlow, M. Warkentin, D. Ormond et al., "Don't make excuses! Discouraging neutralization to reduce IT policy violation", Computers & Security, 39, 2013, pp. 145-159.

[4] R. A. Baron, "Threatened retaliation from the victim as an inhibitor of physical aggression", Journal of Research in Personality, 7 (2), 1973, pp. 103-115.

[5] R. A. Baron, "Aggression as a function of victim's pain cues, level of prior anger arousal, and exposure to an aggressive model", Journal of Personality and Social Psychology, 29 (1), 1974, pp. 117-124.

[6] R. A. Baron, "Effects of Victim's Pain Cues, Victim's Race, and Level of Prior Instigation upon Physical Aggression1", Journal of Applied Social Psychology, 9 (2), 1979, pp. 103-114.

[7] R. A. Baron, "Affect and organizational behavior: When and why feeling good (or bad) matters", Social Psychology in Organizations: Advances in Theory and Research, 1993, pp. 63-88.

[8] L. Berkowitz, "Affective aggression: The role of stress, pain, and negative affect," Human Aggression: Theories, Research, and Implications for Social Policy., R. G. Geen and E. Donnerstein, eds., pp. 49-72, San Diego, CA, US: Academic Press, 1998.

[9] S. R. Boss, D. F. Galletta, P. B. Lowry et al., "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", MIS Quarterly, 39 (4), 2015, pp. 837-864.

[10] J. Bouffard, M. L. Exum, and R. Paternoster, "Whither the beast? The role of emotions in a rational choice theory of crime," Of Crime and Criminality: The Use of Theory in Everyday Life, S. Simpson, ed., pp. 159-178, Thousand Oaks, CA: Pine Forge, 2000.

[11] J. A. Bouffard, "The influence of emotion on rational decision making in sexual aggression", Journal of Criminal Justice, 30 (2), 2002, pp. 121-134.

[12] J. A. Bouffard, "Examining the direct and indirect effects of fear and anger on criminal decision making among known offenders", International Journal of Offender Therapy and Comparative Criminology, 59 (13), 2014, pp. 1385-1408.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS Quarterly, 34 (3), 2010, pp. 523-548.

[14] A. Carman, "Study: Internal employees account for 43 percent of data loss," SC Magazine, 2015.

[15] S. Carmichael, and A. R. Piquero, "Sanctions, perceived anger, and criminal offending", Journal of Quantitative Criminology, 20 (4), 2004, pp. 371-393.

[16] J. S. Carroll, "Compliance with the law: A decision-making approach to taxpaying", Law and Human Behavior, 11 (4), 1987, pp. 319-335.

[17] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?", Journal of Management Information Systems, 29 (3), 2012, pp. 157-188.

[18] C. A. Cole, "Deterrence and consumer fraud", Journal of Retailing, 65 (1), 1989, pp. 107-120.

[19] R. Crossler, and F. Bélanger, "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument", ACM SIGMIS Database, 45 (4), 2014, pp. 51-71.

[20] M. Cusson, "Situational deterrence: Fear during the criminal event," Crime Prevention Studies, R. Clarke, ed., pp. 55-68, NY: Criminal Justice Press, 1993.

[21] J. D'Arcy, and S. Devaraj, "Employee misuse of information technology resources: testing a contemporary deterrence model", Decision Sciences, 43 (6), 2012, pp. 1091-1124.

[22] J. D'Arcy, and T. Herath, "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", European Journal of Information Systems, 20 (6), 2011, pp. 643-658.

[23] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding employee responses to stressful information security requirements: a coping perspective", Journal of Management Information Systems, 31 (2), 2014, pp. 285-318.

[24] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", Information Systems Research, 20 (1), 2009, pp. 79-98.

[25] A. R. Damasio, Descartes'error: emotion, reason, and the human brain, New York: Putnam, 1994.

[26] L. Deng, and M. S. Poole, "Affect in web interfaces: a study of the impacts of web page visual complexity and order", MIS Quarterly, 34 (4), 2010, pp. 711-730.

[27] M. Exum, "The Application and Robustness of the Rational Choice Perspective in the Study of Intoxicated and Angry Intentions to Aggress*", Criminology, 40 (4), 2002, pp. 933-966.

[28] J. R. Fontaine, K. R. Scherer, E. B. Roesch et al., "The world of emotions is not two-dimensional", Psychological Science, 18 (12), 2007, pp. 1050-1057.

[29] C. E. Frazier, and T. Meisenhelder, "Exploratory notes on criminality and emotional ambivalence", Qualitative Sociology, 8 (3), 1985, pp. 266-284.

[30] N. H. Frijda, "Recognition of emotion", Advances in Experimental Social Psychology, 4, 1969, pp. 167-223.

[31] N. H. Frijda, The Emotions, Cambridge, England: Cambridge University Press., 1986.

[32] N. H. Frijda, "Varieties of affect: Emotions and episodes, moods, and sentiments," The nature of emotions: Fundamental questions by P. Ekman & R. Davison, pp. 197-202, New York: Oxford University Press, 1994.

[33] N. H. Frijda, P. Kuipers, and E. Ter Schure, "Relations among emotion, appraisal, and emotional action readiness", Journal of Personality and Social Psychology, 57 (2), 1989, pp. 212-228.

[34] J. M. George, "State or trait: Effects of positive mood on prosocial behaviors at work", Journal of Applied Psychology, 76 (2), 1991, pp. 299-307.

[35] J. P. Gibbs, Crime, punishment, and deterrence: Elsevier New York, 1975.

[36] K. H. Guo, "Security-related behavior in using information systems in the workplace: A review and synthesis", Computers & Security, 32, 2013, pp. 242-251.

[37] K. H. Guo, Y. Yuan, N. P. Archer et al., "Understanding

nonmalicious security violations in the workplace: a composite behavior model", Journal of Management Information Systems, 28 (2), 2011, pp. 203-236.

[38] T. Herath, and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", Decision Support Systems, 47 (2), 2009, pp. 154-165.

[39] T. Herath, and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations", European Journal of Information Systems, 18 (2), 2009, pp. 106-125.

[40] R. C. Hollinger, and J. P. Clark, "Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft", Social Forces, 62 (2), 1983, pp. 398-418.

[41] Q. Hu, Z. Xu, T. Dinev et al., "Does deterrence work in reducing information security policy abuse by employees?", Communications of the ACM, 54 (6), 2011, pp. 54-60.

[42] Y. Hwang, and D. J. Kim, "Customer self-service systems: The effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust", Decision Support Systems, 43 (3), 2007, pp. 746-760.

[43] J. J. Kim, E. H. E. Park, and R. L. Baskerville, "A model of emotion and computer abuse", Information & Management, 53 (1), 2016, pp. 91-108.

[44] S. Klepper, and D. Nagin, "The deterrent effect of perceived certainty and severity of punishment revisited*", Criminology, 27 (4), 1989, pp. 721-746.

[45] K. Lee, and N. J. Allen, "Organizational citizenship behavior and workplace deviance: the role of affect and cognitions", Journal of Applied Psychology, 87 (1), 2002, pp. 131.

[46] S. M. Lee, S.-G. Lee, and S. Yoo, "An integrative model of computer abuse based on social control and general deterrence theories", Information & Management, 41 (6), 2004, pp. 707-718.

[47] Y. Lee, and K. R. Larsen, "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software", European Journal of Information Systems, 18 (2), 2009, pp. 177-187.

[48] J. S. Lerner, and D. Keltner, "Fear, anger, and risk", Journal of Personality and Social Psychology, 81 (1), 2001, pp. 146-159.

[49] H. Liang, and Y. Xue, "Avoidance of information technology threats: a theoretical perspective", MIS Quarterly, 33 (1), 2009, pp. 71-90.

[50] G. Loewenstein, "Out of control: Visceral influences on behavior", Organizational Behavior and Human Decision Processes, 65 (3), 1996, pp. 272-292.

[51] G. Loewenstein, and J. S. Lerner, "The role of affect in decision making", Handbook of Affective Science, 2003, pp. 619-642.

[52] P. B. Lowry, and G. D. Moody, "Proposing the control‐reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies", Information Systems Journal, 25 (5), 2015, pp. 433-463.

[53] P. B. Lowry, C. Posey, R. B. J. Bennett et al., "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational

trust", Information Systems Journal, 25 (3), 2015, pp. 193-273.

[54] D. S. Nagin, and G. Pogarsky, "Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence*", Criminology, 39 (4), 2001, pp. 865-892.

[55] R. W. Novaco, "Anger dysregulation: Driver of violent offending", Journal of Forensic Psychiatry & Psychology, 22 (5), 2011, pp. 650-668.

[56] A. G. Peace, D. F. Galletta, and J. Y. Thong, "Software piracy in the workplace: A model and empirical test", Journal of Management Information Systems, 20 (1), 2003, pp. 153-177.

[57] C. Posey, B. Bennett, T. Roberts et al., "When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse", Journal of Information System Security, 7 (1), 2011, pp. 24-47.

[58] P. Puhakainen, and M. Siponen, "Improving employees' compliance through information systems security training: an action research study", MIS Quarterly, 34 (4), 2010, pp. 757-778.

[59] S. L. Robinson, and R. J. Bennett, "A typology of deviant workplace behaviors: A multidimensional scaling study", Academy of Management Journal, 38 (2), 1995, pp. 555-572.

[60] J. B. Rodell, and T. A. Judge, "Can "good" stressors spark "bad" behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors", Journal of Applied Psychology, 94 (6), 2009, pp. 1438.

[61] I. J. Roseman, "Cognitive determinants of emotion: A structural theory", Review of Personality & Social Psychology, 5, 1984, pp. 11-36.

[62] J. A. Russell, M. Lewicka, and T. Niit, "A Cross-Cultural Study of a Circumplex Model of Affect", Journal of Personality and Social Psychology 57 (5), 1989, pp. 848-856.

[63] R. J. Rydell, D. M. Mackie, A. T. Maitner et al., "Arousal, processing, and risk taking: Consequences of intergroup anger", Personality and Social Psychology Bulletin, 34 (8), 2008, pp. 1141-1152.

[64] K. R. Scherer, A. Schorr, and T. Johnstone, Appraisal processes in emotion: Theory, methods, research: Oxford University Press, 2001.

[65] E. D. Shaw, and H. V. Stock, "Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall", White Paper, Symantec, Mountain View, CA, 2011.

[66] H. A. Simon, Models of man, New York: Wiley, 1957.

[67] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study", Information & Management, 51 (2), 2014, pp. 217-224.

[68] M. Siponen, and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations", MIS Quarterly, 34 (3), 2010, pp. 487-502.

[69] C. A. Smith, and P. C. Ellsworth, "Patterns of cognitive appraisal in emotion", Journal of Personality and Social Psychology, 48 (4), 1985, pp. 813-838.

[70] J. M. Stanton, K. R. Stam, P. Mastrangelo *et al.*, "Analysis of end user security behaviors", Computers & Security, 24 (2), 2005, pp. 124-133.

[71] D. W. Straub, "Effective IS security: An empirical study", Information Systems Research, 1 (3), 1990, pp. 255-276.

[72] D. W. Straub, and R. J. Welke, "Coping with systems risk: security planning models for management decision making", MIS Quarterly, 22 (4), 1998, pp. 441-469.

[73] L. Z. Tiedens, and S. Linton, "Judgment under emotional certainty and uncertainty: the effects of specific emotions on information processing", Journal of Personality and Social Psychology, 81 (6), 2001, pp. 973-988.

[74] L. K. Trevino, "Experimental approaches to studying ethical-unethical behavior in organizations", Business Ethics Quarterly, 2 (2), 1992, pp. 121-136.

[75] A. Vance, P. B. Lowry, and D. Eggett, "Using accountability to reduce access policy violations in information systems", Journal of Management Information Systems, 29 (4), 2013, pp. 263-290.

[76] A. Vance, P. B. Lowry, and D. Eggett, "Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations", MIS Quarterly, 39 (2), 2015, pp. 345-366.

[77] J. D. Wall, P. Palvia, and P. B. Lowry, "Control-related motivations and information security policy compliance: The role of autonomy and efficacy", Journal of Information Privacy and Security, 9 (4), 2013, pp. 52-79.

[78] D. Watson, L. A. Clark, and A. Tellegen, "Development and validation of brief measures of positive and negative affect: the PANAS scales", Journal of Personality and Social Psychology, 54 (6), 1988, pp. 1063-1070.

[79] R. Willison, "Understanding the perpetration of employee computer crime in the organisational context", Information and Organization, 16 (4), 2006, pp. 304-324.

[80] R. Willison, and M. Warkentin, "The expanded security action cycle: a temporal analysis 'Left of Bang'.", Proceedings of the The Dewald Roode Workshop on Information Systems Security Research, IFIP WG8, 11, 2010.

[81] R. Willison, and M. Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse", MIS Quarterly, 37 (1), 2013, pp. 1-20.

[82] D. Yin, S. Bond, and H. Zhang, "Anxious or angry? Effects of discrete emotions on the perceived helpfulness of online reviews", MIS Quarterly, 38 (2), 2014, pp. 539-560.

[83] P. Zhang, "The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the ICT Context", MIS Quarterly, 37 (1), 2013, pp. 247-274.

[84] P. Zhang, and N. Li, "The importance of affective quality", Communications of the ACM, 48 (9), 2005, pp. 105-108.

[85] D. Zillmann, Hostility and aggression, NJ: Lawrence Erlbaum Associates, 1979.

[86] F. E. Zimring, G. Hawkins, and J. Vorenberg, Deterrence: The legal threat in crime control: University of Chicago Press Chicago, 1973.