Taking it out on *IT*: A Mechanistic Model of Abusive Supervision and Computer Abuse

Alaa Nehme
Iowa State University
anehme@iastate.edu

Joey F. George
Iowa State University
jfgeorge@iastate.edu

Abstract

One salient issue in organizational information security is computer abuse. Drawing on the management literature, we identify abusive supervision as a potential factor that affects the latter. As such, this paper proposes a model that formulates why subordinates commit computer abuse in response to abusive supervision. The model focuses on the mechanism of displacing aggression in retaliating against the organization. Drawing upon neutralization and deterrence theories and grounded in appraisal theory, the model offers several propositions. Most notably, the model identifies an interplay among the relevant appraisals, the emotion of anger, neutralization, deterrence and computer abuse. The model also incorporates two conditional moderators, including supervisor's organization embodiment and controllability. The specific propositions and implications are discussed.

1. Introduction

Organizational information security has been a growing concern for professionals and scholars. One particular salient issue in protecting organizational information assets is the "insider threat" [8, 53]. Although underreported, employee computer abuse has been shown to largely attribute to internal security incidents by different industry reports [54]. Previous research has extensively examined the phenomenon of *unintentional* noncompliance with information security policies (ISPs). However, the *intentional* violations of security policies and *volitional (and malicious)* misuse of information resources remain understudied with some exceptions (e.g., [10, 26, 54]), and thus call for more attention [8, 53]. In this paper, we use "computer abuse" as an umbrella term for organizational deviant actions related to both employees' intentional violations of ISPs (e.g., copying files to a USB while being aware that it is a policy violation) and malicious computer misuse (e.g., data theft/corruption/leakage).

This paper proposes a behavioral model of employee computer abuse as a reactive response to abusive supervision. The model's core tenets draw upon the management and organizational behavior literatures that examine organizational deviant behavior as a function of abusive supervision [46, 47, 50]. Further, the model draws on neutralization theory [45] and considers the emotion of anger to formulate the underlying mechanism of the proposed relationship between abusive supervision and computer abuse. Also, the model draws on deterrence theory [17, 44] to inquire into the role of sanctions with respect to the formulated underlying mechanism. We use appraisal theory as the organizing theoretical framework for developing the proposed model and hence derive the model's respective propositions.

In developing the aforementioned model, this paper sets forth a theoretical account of why employees commit computer abuse in response to appraisals of abusive supervision. As such, the model and its derived propositions represent a response to the call by Willison and Warkentin [53] to address the following understudied information security areas: (1) organizational injustice as an underlying factor of computer abuse, (2) emotions' influence on deterring computer abuse through sanctions, and (3) specific rationalizations as an outcome of certain events. Further, the model identifies two prominent conditions in the form of moderators that are useful to future information security research in explaining computer abuse as an outcome of perceived interpersonal or interactional injustice in organizations (e.g., abusive supervision): (1) supervisor's embodiment of the organization, and (2) controllability over information resources.

2. Related Literature, Research Opportunities and the Present Paper

2.1. Information Security

URI: https://hdl.handle.net/10125/64265
978-0-9981331-3-3

To explain computer abuse and unintentional ISP noncompliance, much of the previous research has applied deterrence theory, which posits that the intention to commit crime is negatively influenced by the perceived severity and certainty of sanctions (for a comprehensive review, see [52]). However, this research has had inconsistent findings [9, 53]. Some scholars argue that the nature of the motive (i.e., expressive vs. instrumental)[1] behind computer abuse may determine whether sanctions are effective in deterring the behavior [53]. Expressive crimes involve emotions (e.g., rage, anger) that may moderate the relations between sanctions and computer abuse [53]. The question pertaining to how or why emotions influence the "expected" deterrent effects of sanctions remains underexplored. Others argue that the effectiveness of deterrence against computer abuse is contingent upon variables such as moral beliefs, self-control and employee position [9]. This paper addresses the argument related to expressive motives. The focus is on the behavior of committing computer abuse as an expressive illicit behavior to retaliate against the organization. This focus aligns with the scope of the paper and the abusive supervision literature it extends.

Also, in an effort to explain why employees engage in computer abuse, some research has applied neutralization theory (e.g., [43, 54]), which posits that offenders rationalize their deviant behavior through neutralization techniques. These techniques have been found to be positively related to the intentions of violating ISPs and to override the effects of sanctions on the latter [43]. However, the root causes of engaging in specific rationalizations, or neutralization techniques, have not been addressed in the information security literature [53]. This paper identifies specific factors that may relate to the specific neutralization technique of 'denial of the victim,' where the "victim" is the organization.

Lastly, new explanatory variables that have been identified and appear to be useful in explaining the engagement of employees and insiders in computer abuse relate to the perceptions of organizational injustice and fairness [53]. Recent information security studies have shown that perceived distributive injustice and perceived procedural injustice are positively related to intentions of committing computer abuse [54], and that counterfactual reasoning components of unfairness elicit computer abuse [26]. Similar to [18], this paper focuses on one form of interpersonal injustice, abusive supervision. The extant literature has not proposed nor examined the mechanism underlying the relationship between abusive supervision and computer abuse and how it interacts with deterrence.

In sum, while the literature has recently started to examine intentional computer abuse, some issues remain unaddressed. First, the mechanism through which perceived organizational interactional/interpersonal injustice, specifically 'abusive supervision', induces computer abuse has not been formulated. Second, factors that underlie different neutralization techniques have also not been formally identified. Third, how specific emotions in a specific given situation influence the deterrence of computer abuse have also not been formulated. This paper develops a theoretical model that addresses these issues collectively.

2.2. Abusive Supervision and Workplace Deviance

Introduced to the management literature by Tepper [46], the construct of abusive supervision refers to "subordinates' perceptions of the extent to which supervisors engage in *the sustained display of hostile verbal and nonverbal behaviors, excluding physical contact*" [46]. Example behaviors of abusive supervision are "speaking rudely to subordinates to elicit desired task performance," "publicly belittling subordinates in order to hurt their feelings," and invading their privacy [46]. Three important features of the definition must be highlighted [47]. These features distinguish 'abusive supervision' from other aggression-related constructs such as petty tyranny, supervisor undermining and workplace bullying. First, "abusive supervision" reflects subordinates' subjective perceptions of the supervisor's behavior (i.e., "abusive supervision" refers to "*perceived* abusive supervision"). Second, the construct refers to *sustained* behavior, as opposed to incidental occurrences. Third, the intentional purposes of abusive behavior may not be related to causing harm but to other objectives such as eliciting high performance [47].

A multitude of studies has examined the construct's antecedents and consequences, with a greater focus on the latter [50]. Antecedents of abusive supervision relate to social learning (e.g., trickle-down effects, familial/workplace role models and organization norms), identity threats (e.g., supervisor's and subordinates' characteristics) and self-regulation impairment (e.g., work stress, pressure and fatigue) [50]. Consequences of perceived abusive supervision (on the part of the subordinates) include but are not limited to psychological strain [49], lower self-esteem

[1] An instrumental crime is a means to an end (e.g., stealing to acquire money). An expressive crime is in itself an end.

[6, 51], lower levels of performance [19], lower levels of creativity and innovation, weaker organizational commitment, higher intentions to quit, and diminished organizational citizenship behavior [55]. Most related to this paper is workplace employee deviance as an outcome, or consequence, of perceived abusive supervision.

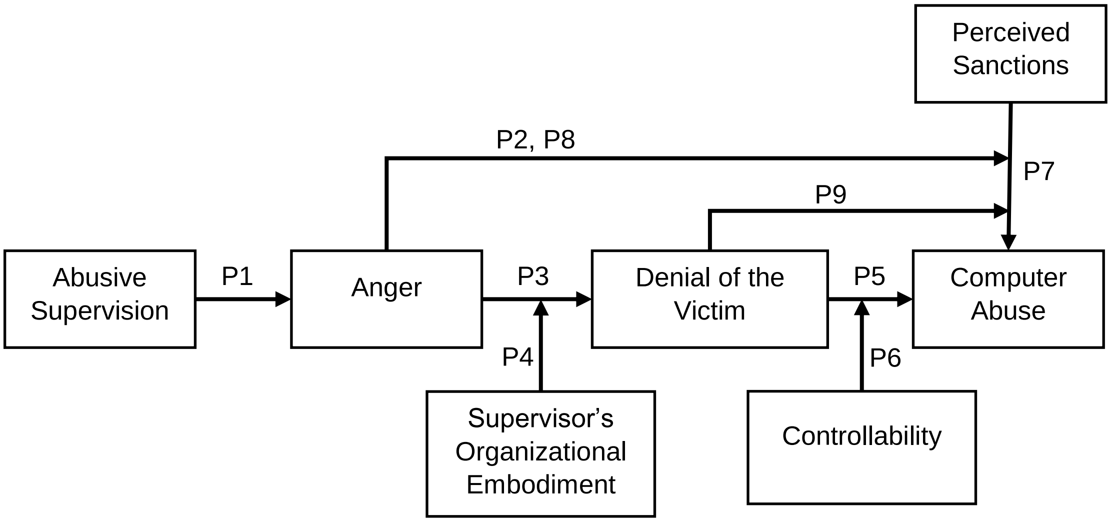

Figure 1. Proposed Model

Workplace deviance refers to the "voluntary behavior that violates significant organizational norms and in so doing threatens the well-being of organization, its members, or both" [37]. Previous studies have shown a positive relation between abusive supervision and employee workplace deviance directed against supervisors, coworkers, and the organization (e.g., [30, 48]). Workplace employee deviance may be classified either as interpersonal or organizational [37]. Interpersonal deviance comprises deviant actions taken against individuals in the organization (e.g., bullying, sexual harassment, verbal abuse, etc.). Interpersonal deviance takes two forms: deviant behavior directed toward supervisors and deviant behavior directed toward co-workers. On the other hand, organizational deviance relates to deviant actions taken against the organization. These actions may include intentionally arriving to work late, engaging in counterproductive behaviors, abusing organizational resources, stealing, etc. As an outcome of abusive supervision, deviant behaviors that concern violating information security policies and abusing computer/information resources have not been addressed.

While the literature on abusive supervision has examined different deviant behaviors as an outcome of the latter, one overlooked behavior is computer abuse. Given the pervasiveness and availability of information technology resources to employees in organizations, this creates a gap in the literature. This paper aims to fill the gap, and as such proposes a behavioral model of computer abuse as an outcome of abusive supervision with its underlying mechanisms and conditions.

3. Model Development and Propositions

Figure 1 illustrates our model and propositions. The premises of our model draw upon the management literature that examines organizational deviant behavior as an outcome of abusive supervision. As such, we propose an indirect relationship between the two. The model also draws on theories previously applied in the behavioral information security literature. These theories include deterrence theory and neutralization theory. We use appraisal theory as the organizing theoretical framework to build our model and elicit the relevant propositions.

3.1. Theoretical Framework: Appraisal Theory

Appraisal theory does not refer to one particular theory, but to a set of theories that address the relationships among the appraisals related to a stimulus, the emotional response, motivation or action tendencies and the elicited behavior. Appraisal theories of emotion provide a theoretical perspective that identifies the appraisal of a distinct event or stimulus along with the outcome emotion [22, 23, 39]. According to appraisal theory, individuals undertake cognitive appraisal processes when they face disturbance, or a threatening stressor from the external environment [16, 23]. These appraisals elicit an emotional response that in turn elicit certain behavioral actions in response to the stimulus

[22, 40]. These actions are typically congruent with the underlying implicit goal and action tendency of the situation.

Appraisal theory posits that individuals engage in two consecutive processes: primary appraisal and secondary appraisal [16]. Primary appraisals initially concern the relevance of the event. If the event is perceived as irrelevant to the individual, he/she does not further engage in further processing. Else, if the event is perceived as relevant and positive, then it arouses positive emotions. Otherwise, if the event is perceived as relevant and negative, or threatening, it is likely to arouse negative emotions. Secondary appraisals follow primary appraisals that induce positive or negative emotions [15, 16, 22]. Secondary appraisals involve evaluating the certainty of the perceived event. Further, they involve appraising coping potential, or situational control (i.e., the ability or potential to effectively cope with or respond to the perceived threat) [16]. Also, blaming or assigning responsibility to a specific person or party in case of a negative event is a form of secondary appraisal.

Appraisal theory has been widely used in different research contexts. In information security, one widely used theoretical model (e.g., [5, 35]) that is based on appraisal theory, and takes into account cognitive appraisals, the emotion of fear, motivation and the elicited protective behavior is PMT - protection motivation theory [14, 38].

3.2. Primary Appraisal and Emotion: Abusive Supervision and Anger

In alignment with appraisal theories, specifically the transactional theory of stress [23, 25], abusive supervision may be viewed as an external stressor that elicits negative thoughts and emotions [36]. Emotions are experienced by individuals as adaptive responses to appraisals about stressors in the environment. Previous research suggests that recipients of abusive supervision are likely to experience high levels of anger, psychological distress and other negative emotions [13, 31, 46, 49].

Anger is an approach-based negatively-valenced emotion that arises in response to a negative event and when individuals attribute responsibility for that event to someone else [13]. Appraisal theorists of emotion describe anger as an outcome of appraisals related to goal relevance, blaming a specific agent and sensing high situational control, or coping potential [22, 39]. Further, anger is believed to be an outcome of perceived injustice or unfairness [22, 40]. It is also viewed to have a motivational orientation, through which individuals cope with the appraised disturbance, or negative events, by taking certain behavioral actions. The cornerstones to *perceived* abusive supervision as defined by Tepper [46] are assigning responsibility to the supervisor and being certain about its reoccurrence. Thus, it aligns with anger's underpinnings. In line with previous studies, we propose:

Proposition 1. Perceptions of abusive supervision will induce anger.

3.3. Emotion and Coping Behavior: Anger and Computer Abuse

Angry employees will seek to cope with the stressor. According to appraisal theories and coping theory [24], individuals either cope with stress through problem-solving coping responses or emotion-focused coping responses. While, the former allows individuals to directly cope with the stressor (i.e., control the danger), the latter allows individuals to regulate their negative feelings (i.e., control and cope with their emotions). Thus, angry subordinates would ideally cope with the stressor (i.e., the supervisor) through taking deviant actions toward the supervisor, as suggested by the literature [49]. However, subordinates may adopt emotion-focused coping mechanisms to cope with their anger. These include directing their anger at someone or something else.

Previous research has shown that individuals often displace their aggression onto targets other than the source of stress, and thus emotionally cope with the stressor. Studies have suggested that displacing aggression explains organizational deviant behavior as a consequence of abusive supervision (e.g., [30]). The theory of displaced aggression [11] suggests that individuals who become frustrated may displace their aggression on entities other than the source of abuse (i.e., the supervisor). The two reasons that attribute to displacing aggression are the unavailability of the abuser and the fear of retaliation from the harm-doer, or abuser. These constraints redirect retaliation on less powerful and more available targets. This aligns with appraisal and coping theories that suggest that when coping potential is low (for example, in this case, coping potential may be low due to fearing that the supervisor may further retaliate from the subordinate), the preferred route of coping with the stressor becomes emotion-focused, as opposed to problem-solving oriented. Thus, displacing aggression on information resources, which are more available to subordinates and less powerful is more likely to happen. In line with previous studies that have shown that anger mediates the relationship between perceived abusive supervision and counterproductive work behavior (e.g., [13, 42]), we propose:

Proposition 2. Anger will induce computer abuse.

3.4. Emotion and Coping Response: Anger and Neutralization

3.4.1. Neutralization theory. Neutralization theory [45] has been used to examine a wide array of criminal behaviors (e.g., tax evasion and piracy) and organizational deviant behaviors. Most notably, it has been applied in the organizational information security context to explain/predict employees' violations of information security policies (e.g., [43, 54]).

Neutralization theory posits that delinquents justify their deviant behavior by applying techniques of neutralization, which ultimately neutralize any feelings of guilt and shame that arise with the committed deviant act [45]. Techniques of neutralization are rationalizations that enable offenders to neutralize social norms and protect themselves from self-blame and others' blame. These techniques originally include denial of the victim, denial of injury, denial of responsibility, condemnation of the condemners and the appeal to higher loyalties [45]. Over time, scholars have also proposed additional techniques such as the defense of the necessity [29] and the metaphor of the ledger [21].

This paper's concern is the 'denial of the victim' (DoV) neutralization technique [45]. Simply put, this technique reflects the notion that the victim deserves the harm, or the consequences of the deviant action. For example, "a production-line worker may view his or her act of theft as a rightful form of retaliation for being overlooked for a promotion" [54]. Our focus on a subset of techniques is consistent with prior research (in both the criminology and information security literatures) that have also done so since "certain techniques of neutralization would appear to be better suited to particular deviant acts" [45]. In this paper, we focus on DoV since it suits the mechanism between abusive supervision and the deviant behavior under study (i.e., computer abuse).

3.4.2. Anger and denial of the victim. According to Lazarus [23], negative emotions elicit rationalizations related to the disturbance in the environment. Since subordinates' anger is being redirected toward the organization instead of the supervisor (from proposition 2) through displaced aggression, then the most logical rationalization technique subordinates will follow is that "the organization deserves the harm." A rationalization technique that normalizes illicit and harmful behavior through the offender's justification of that behavior based on his/her given situation is the 'denial of the victim' neutralization technique. Hence, analogous to the disgruntled worker who was overlooked for promotion and thus justified his/her theft as a rightful retaliatory action, the abused subordinate would justify his/her abuse of computer resources as a rightful retaliatory act against the organization. Since this is an expressive illicit behavior and since anger induces approach-based action tendencies which align with the concept of 'denial of the victim,' we posit that anger elicits DoV. Note that in this case, "victim" refers to the organization and not the supervisor.[2] This is consistent with previous information security research that suggests a relationship between stress and moral disengagement [10], given that the theory of moral disengagement [3, 4] overlaps with neutralization theory as noted in earlier research [52, 53].

Proposition 3. Anger will induce denial of the victim (i.e., organization).

3.5. Secondary Appraisal: Supervisor's Organizational Embodiment as a Moderator

After undergoing primary appraisal and experiencing emotion, individuals undergo secondary appraisal, which include holding a party accountable or responsible for the harm. When subordinates perceive that the supervisor embodies the organization, they will be more likely to hold the organization accountable for the abusive supervision.

Supervisor's Organizational Embodiment (SOE) refers to the extent to which an employee identifies his/her supervisor with the organization [12], and represents the extent to which subordinates perceive their social exchange relationships with their supervisors reflective of the social exchange relationships with their organizations [27]. In other words, high perceptions of SOE imply that employees experience the treatment received from the supervisor as treatment received from the organization. Also, high SOE implies that the employee views the supervisor to have shared characteristics with the organization. As such, perceptions of high SOE engender a generalization of the subordinates' exchange relationship with their supervisor to the organization [12].

"SOE has important socioemotional and instrumental consequences for employees" [12]. When subordinates have a(n) favorable (unfavorable) exchange relationship with their supervisor along with high perceptions of SOE, they are more (less) likely to

[2] Had we formally formulated a problem-focused coping behavior in the model (i.e., supervisor-directed deviance), "denial of the victim" as in denial of the supervisor could have been proposed as a mediator between abusive supervision and supervisor-directed deviance. However, the focus of this model is emotion-focused coping and displaced aggression.

be instrumentally involved with the organization and have higher (lower) levels of subjective well-being [12]. SOE helps address the social exchange source-target (i.e., supervisor-organization) misalignment, and thus explains negative (positive) actions taken toward the organization (i.e., target) in response to the supervisor's mistreatment (favorable treatment) [27]. Previous studies have shown that SOE plays a prominent role in aligning abusive supervision with subordinates' negative behavior against organizations (e.g., [27, 41]). Recall that denial of the organization as the victim is the proposed rationalization technique that will be used by subordinates to justify their deviant behavior against the organization. Also, since anger is redirected toward the organization through this rationalization technique as a form of displaced aggression, we theorize that when subordinates generalize abusive supervision to the organization, anger will have a more profound effect on the subordinate's belief that the organization deserves harm.

Proposition 4. The relation between anger and denial of the victim will be stronger when subordinates' perceptions of SOE are high.

3.6. Coping Response and Behavior: Denial of the Victim and Computer Abuse

As previously discussed, neutralization takes place to rationalize illicit behavior. In this paper's context, it is expected that neutralization is positively related to computer abuse. Previous information security studies have found neutralization techniques (and the similar construct of moral disengagement) to be significant predictors of ISP noncompliance [10, 43]. As discussed previously, our model's neutralization technique of interest is denial of the victim. Thus, we propose the following:

Proposition 5. Denial of the victim will induce computer abuse.

3.7. Secondary Appraisal: Controllability as a Moderator

Controllability, one separable component of perceived behavioral control, refers to the individual's judgment about the *availability of resources* and *opportunities* to perform a certain behavior [1, 33]. While self-efficacy, the other component of PBC, reflects personality factors, controllability reflects factors pertaining to the external environment and resources [33]. In the context of computer abuse, controllability describes employees' perceptions of whether information resources are available for them to abuse, and whether they have opportunities to violate information security policies.

Recall that the theory of displaced aggression [11] attributes displacing aggression on a target other than the source to that target's availability and limited powerfulness. Thus, we theorize that when individuals have higher controllability over information resources, then denial of the victim will have a more pronounced effect on computer abuse.

Proposition 6. At high levels of perceived controllability over organizational information resources, the relation between denial of the victim and computer abuse is stronger.

3.8. Anger, Neutralization and Deterrence

3.8.1. Deterrence theory. Deterrence theory has been extensively used in the information security literature [9, 20, 43, 44, 52, 54]. The theory proposes that high levels of certainty, severity and celerity of sanctions deter offenders from committing crime [17]. In the organizational information security context, the theory postulates that employees are less likely to commit computer abuse when sanctions are severe and certain. The theory has also been extended to include informal sanctions and related components, such as shame [32, 34]. In this paper, the term "sanctions" compiles both formal and informal sanctions. In alignment with the previous information security literature, we propose that:

Proposition 7. Perceived sanctions will reduce computer abuse.

3.8.2. Anger and denial of the victim as moderators. As mentioned earlier, organizational computer abuse as an outcome of abused supervision is an expressive offense, and it aims to fulfill the subordinate's objective of retaliating against the organization. Criminologists suggest that the negative emotions (e.g., anger, rage, etc.) involved in "expressive-based crimes" alleviate the deterrent effects of sanctions on the criminal offense (see [53]). Previous findings in the criminology literature have asserted the suggested moderation (e.g., [7]). We theorize that the moderation holds in the computer abuse context.

Proposition 8. At high levels of anger, perceived sanctions will have a weaker relationship with computer abuse.

Similarly, we posit that the 'denial of the victim' neutralization technique alleviates the effect of sanctions on computer abuse. In fact, the substance of neutralization theory is that rationalization techniques negate internal norms, social control and feeling of guilt and shame, and thus delinquents justify their actions.

Thus, it is expected that neutralization alleviates sanctions involving norms and social control (i.e., formal sanctions) and guilt and shame (i.e., informal sanctions). Also, information security research has shown that the effects of sanctions on ISP noncompliance fade when neutralization is applied by employees [43]. Thus, we propose:

Proposition 9. At high levels of denial of the victim (i.e., organization), perceived sanctions will have a weaker relationship with computer abuse.

4. Discussion and Implications

Computer abuse is a form of organizational deviant behavior that represents a severe threat to organizations. The organizational behavior literature has shown that abusive supervision prompts organizational deviant behavior among other outcomes. As such, one may infer that abuse supervision may also engender computer abuse. Abusive supervision is a salient stressor that may be encountered by employees in the organization. Tepper [50] estimates the percentage of abused subordinates to be 10%. This paper's purpose was to propose a theoretical model that explains why abusive supervision may engender computer abuse. We focused on the displaced aggression mechanism which aligns with emotion-focused coping from coping theory. To develop our model, we mainly drew on deterrence theory, neutralization theory and the abusive supervision literature, and we used appraisal theory as the infrastructure. Our model offers several theoretical implications.

First, the model identifies abusive supervision as a potential source of computer abuse. Second, our model takes into account the expressive nature of committing computer abuse, and thus identifies the moderating effects of anger and neutralization on the relation between sanctions and the illicit behavior. Testing these identified paths may explain the mixed results of deterrence studies in the security literature. Third, the model identifies a particular neutralization technique (i.e., denial of the victim) that is specific to a particular event (i.e., abusive supervision).

Fourth, implicit to our model are two conditional expectations represented in the form of moderations through the constructs of supervisor's organizational embodiment (SOE) and controllability. The first condition states that anger is directed toward the organization only if subordinates perceive that concord exists between the supervisor and the organization. Contingent upon the first condition, the second condition states that subordinates commit computer abuse as a form of organizational deviance only if they have high controllability over computer/IS resources. We believe that in testing our model, or a similar one, including these moderators is imperative as they may unveil two different relationships between the high controllability (or SOE) and low controllability (or SOE) groups of empirical observations.

5. Conclusion

We present a model of why employees commit computer abuse in response to perceived abusive supervision with a focus on the mechanism of displaced aggression. This is an early step toward understanding displacing aggression onto information assets in the organization. A natural next step would be to empirically test our propositions. Also, the proposed model may be expanded to account for alternative underlying mechanisms of the relationship between computer abuse as an outcome of abusive supervision. For example, the construct of affective organizational commitment [2, 28] may be incorporated into the model as a mediator between abusive supervision and computer abuse. We hope that this paper catalyzes additional research into the area.

6. References

[1] Ajzen, I., "Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1", *Journal of applied social psychology 32*(4), 2002, pp. 665–683.

[2] Allen, N.J., and J.P. Meyer, "The measurement and antecedents of affective, continuance and normative commitment to the organization", *Journal of occupational psychology 63*(1), 1990, pp. 1–18.

[3] Bandura, A., "Moral disengagement in the perpetration of inhumanities", *Personality and social psychology review 3*(3), 1999, pp. 193–209.

[4] Bandura, A., "Selective moral disengagement in the exercise of moral agency", *Journal of moral education 31*(2), 2002, pp. 101–119.

[5] Boss, S.R., D.F. Galletta, P.B. Lowry, G.D. Moody, and P. Polak, "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.

[6] Burton, J.P., and J.M. Hoobler, "Subordinate self-esteem and abusive supervision", *Journal of Managerial Issues*, 2006, pp. 340–355.

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

[8] Crossler, R.E., A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for

behavioral information security research", *Computers & Security 32*, 2013, pp. 90–101.

[9] D'arcy, J., 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.

[10] D'Arcy, J., 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.

[11] Dollard, J., N.E. Miller, L.W. Doob, O.H. Mowrer, and R.R. Sears, *Frustration and aggression.*, Yale University Press, New Haven, CT, 1939.

[12] Eisenberger, R., G. Karagonlar, F. Stinglhamber, et al., "Leader–member exchange and affective organizational commitment: The contribution of supervisor's organizational embodiment.", *Journal of Applied psychology 95*(6), 2010, pp. 1085.

[13] Ferris, D.L., M. Yan, V.K. Lim, Y. Chen, and S. Fatimah, "An approach–avoidance framework of workplace aggression", *Academy of Management Journal 59*(5), 2016, pp. 1777–1800.

[14] Floyd, D.L., S. Prentice-Dunn, and R.W. Rogers, "A Meta-Analysis of Research on Protection Motivation Theory", *Journal of Applied Social Psychology 30*(2), 2000, pp. 407–429.

[15] Folkman, S., "Personal control and stress and coping processes: A theoretical analysis.", *Journal of personality and social psychology 46*(4), 1984, pp. 839.

[16] Folkman, S., R.S. Lazarus, C. Dunkel-Schetter, A. DeLongis, and R.J. Gruen, "Dynamics of a Stressful Encounter: Cognitive Appraisal, Coping, and Encounter Outcomes", 1986, pp. 12.

[17] Gibbs, J.P., *Crime, Punishment, and Deterrence.*, Elsevier, New York, 1975.

[18] Guan, B., and C. Hsu, "The Role of Abusive Supervision and Interactional Justice in Employee Information Security Policy Noncompliance Intention", *Twenty-Second Pacific Asia Conference on Information Systems*, (2018).

[19] Harris, K.J., K.M. Kacmar, and S. Zivnuska, "An investigation of abusive supervision as a predictor of performance and the meaning of work as a moderator of the relationship", *The leadership quarterly 18*(3), 2007, pp. 252–263.

[20] Herath, T., 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.

[21] Klockars, C.B., *The Professional Fence.*, The Free Press, New York, 1974.

[22] Lazarus, R.S., "Progress on a Cognitive-Motivational-Relational Theory of Emotion", *American Psychologist*, 1991, pp. 819–834.

[23] Lazarus, R.S., *Emotion and adaptation*, Oxford University Press., New York, NY, 1991.

[24] Lazarus, R.S., and S. Folkman, *Stress, appraisal, and coping*, Springer publishing company, 1984.

[25] Lazarus, R.S., and S. Folkman, "Transactional theory and research on emotions and coping", *European Journal of personality 1*(3), 1987, pp. 141–169.

[26] Lowry, P.B., C. Posey, R. (Becky) J. Bennett, and T.L. Roberts, "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.

[27] Mackey, J.D., C.P. McAllister, J.R. Brees, L. Huang, and J.E. Carson, "Perceived organizational obstruction: A mediator that addresses source–target misalignment between abusive supervision and OCBs", *Journal of Organizational Behavior 39*(10), 2018, pp. 1283–1295.

[28] Meyer, J.P., and N.J. Allen, "A three-component conceptualization of organizational commitment", *Human resource management review 1*(1), 1991, pp. 61–89.

[29] Minor, W.W., "Techniques of neutralization: A reconceptualization and empirical examination", *Journal of Research in Crime and Delinquency 18*(2), 1981, pp. 295–318.

[30] Mitchell, M.S., and M.L. Ambrose, "Abusive supervision and workplace deviance and the moderating effects of negative reciprocity beliefs.", *Journal of Applied Psychology 92*(4), 2007, pp. 1159–1168.

[31] Oh, J.K., and C.I. Farh, "An emotional process theory of how subordinates appraise, experience, and respond to abusive supervision over time", *Academy of Management Review 42*(2), 2017, pp. 207–232.

[32] Paternoster, R., and S. Simpson, "Sanction threats and appeals to morality: Testing a rational choice model of corporate crime", *Law & Soc'y Rev. 30*, 1996, pp. 549.

[33] Pavlou, P.A., and M. Fygenson, "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior", *MIS Quarterly 30*(1), 2006, pp. 115–143.

[34] Piquero, A., and S. Tibbetts, "Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending", *Justice quarterly 13*(3), 1996, pp. 481–510.

[35] Posey, C., T.L. Roberts, and P.B. Lowry, "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets", *Journal of Management Information Systems 32*(4), 2015, pp. 179–214.

[36] Restubog, S.L.D., K.L. Scott, and T.J. Zagenczyk, "When distress hits home: The role of contextual factors and psychological distress in predicting employees' responses to abusive supervision.", *Journal of Applied Psychology 96*(4), 2011, pp. 713.

[37] Robinson, S.L., and R.J. Bennet, “A Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Study”, *Academy of Management Journal 38*(2), 1995, pp. 555–572.

[38] Rogers, R.W., “A Protection Motivation Theory of Fear Appeals and Attitude Change”, *Journal of Psychology 91*(1), 1975, pp. 93–114.

[39] Roseman, I.J., “Appraisal determinants of discrete emotions”, *Cognition & Emotion 5*(3), 1991, pp. 161–200.

[40] Roseman, I.J., C. Wiest, and T.S. Swartz, “Phenomenology, behaviors, and goals differentiate discrete emotions.”, *Journal of personality and social psychology 67*(2), 1994, pp. 206.

[41] Shoss, M.K., R. Eisenberger, S.L.D. Restubog, and T.J. Zagenczyk, “Blaming the organization for abusive supervision: The roles of perceived organizational support and supervisor’s organizational embodiment.”, *Journal of Applied Psychology 98*(1), 2013, pp. 158.

[42] Simon, L.S., C. Hurst, K. Kelley, and T.A. Judge, “Understanding cycles of abuse: A multimotive approach.”, *Journal of applied psychology 100*(6), 2015, pp. 1798.

[43] Siponen, M., and A. Vance, “Neutralization: new insights into the problem of employee information systems security policy violations”, *MIS quarterly*, 2010, pp. 487–502.

[44] Straub, D.W., “Effective IS security: An empirical study”, *Information Systems Research 1*(3), 1990, pp. 255–276.

[45] Sykes, G.M., and D. Matza, “Techniques of neutralization: A theory of delinquency”, *American sociological review 22*(6), 1957, pp. 664–670.

[46] Tepper, B.J., “Consequences of Abusive Supervision”, *Academy of Management Journal 43*(2), 2000, pp. 178–190.

[47] Tepper, B.J., “Abusive supervision in work organizations: Review, synthesis, and research agenda”, *Journal of management 33*(3), 2007, pp. 261–289.

[48] Tepper, B.J., C.A. Henle, L.S. Lambert, R.A. Giacalone, and M.K. Duffy, “Abusive supervision and subordinates’ organization deviance.”, *Journal of Applied Psychology 93*(4), 2008, pp. 721–732.

[49] Tepper, B.J., S.E. Moss, D.E. Lockhart, and J.C. Carr, “Abusive supervision, upward maintenance communication, and subordinates’ psychological distress”, *Academy of Management Journal 50*(5), 2007, pp. 1169–1180.

[50] Tepper, B.J., L. Simon, and H.M. Park, “Abusive supervision”, *Annual Review of Organizational Psychology and Organizational Behavior 4*, 2017, pp. 123–152.

[51] Vogel, R.M., and M.S. Mitchell, “The motivational effects of diminished self-esteem for employees who experience abusive supervision”, *Journal of Management 43*(7), 2017, pp. 2218–2251.

[52] Willison, R., P.B. Lowry, and R. Paternoster, “A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research”, *Journal of the Association for Information Systems 19*(12), 2018, pp. 1187–1216.

[53] Willison, R., and M. Warkentin, “Beyond deterrence: An expanded view of employee computer abuse”, *MIS Quarterly 37*(1), 2013, pp. 1–20.

[54] Willison, R., M. Warkentin, and A.C. Johnston, “Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives”, *Information Systems Journal 28*(2), 2018, pp. 266–293.

[55] Zellars, K.L., B.J. Tepper, and M.K. Duffy, “Abusive supervision and subordinates’ organizational citizenship behavior.”, *Journal of applied psychology 87*(6), 2002, pp. 1068.