8-6-2011

The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions

Merrill Warkentin
Mississippi State University, m.warkentin@msstate.edu

Robert Willison
Newcastle Business School, robert.willison@northumbria.ac.uk

Allen C. Johnston
University of Alabama Birmingham, ajohnston@uab.edu

Recommended Citation

Warkentin, Merrill; Willison, Robert; and Johnston, Allen C., "The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions" (2011). *AMCIS 2011 Proceedings - All Submissions*. 318.
http://aisel.aisnet.org/amcis2011_submissions/318

The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Robert Willison
Newcastle Business School
robert.willison@northumbria.ac.uk

Allen C. Johnston
University of Alabama Birmingham
ajohnston@uab.edu

ABSTRACT

Insider computer abuse, the problem of intentional computer-related crimes by employees, is a costly problem for firms (Warkentin and Willison, 2009). To counter this threat, IT practitioners and IS researchers assess potential antecedents of and motivations for computer abuse intentions among employees. The theory of organizational justice, the techniques of neutralization, and the role of deterrence are offered as lenses for evaluating the formation of employee disgruntlement leading to computer abuse behaviors. We have evaluated the impacts of these perceived organizational injustice and neutralization on the formation of employee intention to commit computer abuse activities in violation of security policies and procedures, with additional influences of deterrence. Utilizing the factorial survey method, we have empirically evaluated the association between these antecedents.

Keywords

Computer abuse, organizational justice, neutralization, deterrence, motivation, factorial survey method

INTRODUCTION

Extensive evidence confirms that the security threat from malicious insiders remains the paramount concern to IT security managers. The UK National High Tech Crime Unit (2005) reported that 38% of financial fraud, 68% of theft of information/data, and 100% of sabotage to data or networks was committed internally. The 2006 Deloitte Global Security Survey reported that, of those organizations which experienced breaches, just under half were committed inside the company. The Pricewaterhouse Coopers/UK Department for Business Enterprise and Regulatory Reform survey (PwC/DoBERR, 2008) notes that for large organizations (250+ employees), 57% of respondents reported the cause of their worst security incident to be internal. The Global State of Information Security survey (PwC/CSO/CIO, 2008) showed that employees (former and current) formed the biggest threat for respondents. In a recent survey of IT security professionals, insider misuse and unauthorized access to information by insiders are the No. 1 and No. 2 security threats overall (Carr, 2007), ahead of malware, hackers, and other IS security threats. In the following sections, we review the extant research literature which has addressed those factors which are thought to influence and motivate insiders to form the intention to commit computer abuse.

LITERATURE REVIEW

In the following sections, we review the extant research literature which has addressed those factors which are thought to influence the decision making processes of the offender with regard to deterrence.

Intention

Researchers have combined a number of theories in order to specifically understand the formation of offender behavioral intention (Foltz, 2000; Lee and Lee, 2002; Lee et al, 2004; Workman and Gathegi, 2007). Combining GDT and the Theory of Planned Behavior, Foltz (2000), for example, examined the extent to which an organization can influence an individual's intention to undertake IS misuse and computer crime, and the levels of IS misuse and computer crime by individuals. While the data supported TPB as a suitable theory for understanding intention, Foltz found that written policies and procedures had no deterrent value as they do not influence the intention to commit IS misuse or computer crime. The study also found that policies and procedures were equally deficient with regard to deterring levels of IS misuse and computer crime by individuals.

Deterrence

In the context of computer security, the issue of deterrence has been addressed by several IS researchers, and represents, by far, the must studied area of employee computer crime. Perhaps not surprisingly, a number of scholars have employed General Deterrence Theory (GDT) for studying this phenomenon (Harrington, 1996; Hoffer and Straub, 1989; Straub, 1990; Straub, Carlson and Jones, 1992; Straub and Welke, 1998; D'Arcy and Hovav, 2007). A key aspect of GDT is the role played by sanctions (Cook, 1982), in terms of their perceived certainty and severity by the offender. If an offender perceives the certainty of being caught as high, and if he believes the associated sanctions will be severe, then the offender will be deterred (Straub, 1990). D'arcy et al. (2009), for example, examined how the perceived certainty and security of organizational sanctions, influenced IS misuse intentions. Unlike other studies, however, their research represented a departure by examining how these perceptions were influenced by user awareness of three forms of security countermeasures. These included i) user awareness of security policies, ii) security education, training, and awareness, iii) and computer monitoring. On the whole, these countermeasures were positively associated with perceived certainty and severity, though this was not the case with regard to policies and perceived certainty. In terms of the sanctions, the results revealed that perceived severity would be more effective in reducing misuse than perceived certainty.

Motivation

The issue of motivation has rarely been addressed in the IS security field (Straub, 1990; Shropshire, 2009). However, Straub (1990) examined the extent to which deterrents and rival explanations were related to levels of computer abuse. Rival explanations included motivational, environmental ("tightness of the security environment and visibility of security administrators") and preventives (physical and software security) factors. Specifically, motivational factors included system privileges, the strength of offender motivation, the extent of offender collusion and employment status. Straub assessed these factors in relation to incidents of abuse reported by survey respondents. Overall, the data indicated that deterrents (along with preventives) were effective in lowering incidents of abuse, while rival explanations were generally insignificant.

Although the existing literature has produced a firm basis for examining behavioral intention and its immediate antecedents, there are notable deficiencies, including a lack of focus on the root causes of intention. Existing theories are deficient in terms of providing a comprehensive lens for evaluating the motivation of the offender, which often starts with beliefs and perceptions borne of the interactions between the individual employee and his or her organization, its managers, and its policies and procedures (Willison and Warkentin, 2010). This is illustrated by the current paucity of research into the issue of motive and how motivational factors may be created in the organizational context. If researchers can make progress in understanding the distant antecedents of intention (original motivations further in the past), it may be possible to address the root cause and negate its eventual influence on behavioral intention. Finally, there is a surprising lack of research which has specifically focused on the offender (Warkentin and Willison, 2009). It would appear logical that a focus on the offender, and the application of appropriate theories, would provide timely insights into those factors which influence intention. To address these deficiencies, the following sections discuss two original bodies of theory which may provide further insight into those factors which may influence criminal intention – organizational justice theory and the techniques of neutralization. These theories afford consideration of phenomena which precedes deterrence and, we believe, influence intention.

ORGANIZATIONAL JUSTICE

There is currently a paucity of material focusing on the area of offender motivations in the IS security domain. One area which offers considerable research potential is the phenomenon of workplace disgruntlement (Keeney, et. al. 2005). To address the area of disgruntlement, we propose the use of an existing body of research which examines the issue of fairness within the organizational context. This body of research falls under the umbrella term 'organizational justice.' These constructs (entitled distributive, procedural, interactional, and informational justice), which relate to different organizational phenomena and influence employees' perceptions of fairness/unfairness in organizations, can assist in understanding disgruntlement and explaining how this phenomena may act as a motive and influence criminal intention (Willison and Warkentin, 2009; Willison and Warkentin, 2011). However, because we will focus on only distributive and procedural justice in this paper, and owing to space limitations, interactional and informational justice will not be discussed.

Perceptions of distributive justice or injustice constitute one psychological origin of the motivation to commit computer abuse by insiders. Seminal work in this area was undertaken by Adams (1965), who advanced a theory of equity. Adams argued that in terms of distributive justice, individuals compare the ratio of their work outputs (rewards) and inputs (contributions) to the ratio of a comparative other (e.g. a colleague). Central to this comparative process are what Adams (1965) termed 'normative expectations' which are learned through socialization in forums such as home, school and work. Crucially, Adams (1965, p. 280) observed that when the normative expectations of the person making social comparisons are violated and when he finds that his outcomes and inputs are not in balance in relation to those of others, feelings of inequity can result. These are termed here as perceptions of distributive injustice. A number of writers have noted that factors other than equity may be used for allocating resources e.g. 'equality' and 'need' (Leventhal, 1980). However, as most distributive research has focused on the organizational context, equity represents by far the most examined factor (Colquitt, 2001).

Perceptions of procedural justice or injustice are the second potential motivation of behavioral intention to commit computer abuse by organizational employees. Leventhal and his colleagues (Leventhal, 1980; Leventhal et al, 1980) first addressed procedural justice in the organizational context, by focusing on the nature of the procedures and the implications for procedural justice perceptions. Six rules were identified, which, if followed, it was argued, would lead to the development of fair procedures. As Cohen-Charash and Spector (2001, p.280) noted, these rules included: a) the consistency rule, stating that allocation procedures should be consistent across persons and over time; b) the bias suppression rule, stating that personal self-interests of decision-makers should be prevented from operating during the allocation process; c) the accuracy rule, referring to the goodness of the information used in the allocation process; d) the correctability rule, dealing with the existence of opportunities to change an unfair decision; e) the representativeness rule, stating that the needs, values, and outlooks of all the parties affected by the allocation process should be represented in the process; and f) the ethicality rule, according to which the allocation process must be compatible with fundamental moral and ethical values of the perceiver.

A considerable body of research has addressed the 'outcomes' which impact organizations as a consequence of perceptions of justice/injustice (see Nowakowski and Conlon (2005) for an extensive review of this literature). While some of the reactions can be considered relatively benign (e.g. employee withdrawal, reduced job satisfaction and declining organizational performance), other more extreme responses have included theft (Greenberg, 1990, 1993), retaliation (Skarlicki and Folger, 1997; Skarlicki et al, 1999), revenge (Bies et al, 1997; Bies and Trip, 1998), workplace violence (Greenberg and Barling, 1999) and sabotage (Ambrose et al, 2002; Giacolone et al, 1997). Within the context of computer abuse by disgruntled employees, which can be very damaging and costly to organizations, these two forms of organizational justice merit further investigation. Thus one research question in the present study is: What is the role of perceptions of organizational injustice in forming behavioral intention to commit computer abuse? Furthermore, which form of organizational injustice is potentially more influential in leading to the formation of computer abuse intentions? Is this relationship influenced by other psychological processes?

TECHNIQUES OF NEUTRALIZATION

Theory and research from the fields of criminology has indicated that individuals embody 'internalized norms' (Sykes and Matza, 1957) which can deter individuals from engaging in criminal behavior. That said, authors from the criminology field have also noted that individuals can employ 'techniques of neutralization' (Sykes and Matza, 1957) for helping to dissipate internalized norms and social censure (i.e. the 'self-deterring' mechanisms). This allows the offender to engage in a criminal act without feelings of guilt and shame. We also believe this theory provides original insights into a potential influence on criminal intention in the context of employee computer abuse.

In their seminal text, Sykes and Matza (1957) presented a theory of juvenile delinquency. They argued that delinquents show signs of commitment to the dominant social order by exhibiting feelings of guilt and shame when laws are broken. The subsequent paradoxical question addressed by them is why does delinquency occur if there is a commitment to the 'usages of conformity'? The authors argued that much delinquency is 'justified'/rationalized in a manner which negates the 'disapproval flowing from internalized norms and conforming others in the social environment'. Hence, these social controls and internalized norms, which keep in check and restrain criminal behavior, are 'neutralized', leaving the delinquent free to offend. Given this, Sykes and Matza termed these justifications 'techniques of neutralization,' which include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and the appeal to higher loyalties. So, for example, even if an individual accepts the responsibility for his deviant actions and is willing to admit that his deviant actions involve an injury or hurt, the moral indignation of self and others may be neutralized by an insistence that the injury is not wrong in light of the circumstances. The injury, it may be claimed, is not really an injury; rather, it is a form of rightful retaliation or punishment. By a subtle alchemy the delinquent moves himself into the position of an avenger and the victim is transformed into a wrong-doer (Sykes and Matza, 1957, p. 668).

As a theory, the techniques of neutralization have been readily embraced in the field of criminology to address a diverse range of deviant or criminal behavior (see Maruna and Cope, (2005) for an extensive review). Given the popularity of this theory, aside from its application, a number of researchers have advanced other techniques of neutralization which could be employed in criminal behavior. Klockars (1974), for example, introduced the 'metaphor of the ledger' (see Maruna and Copes (2005) for other examples). The metaphor of the ledger is applied as justification for violations that may be seen as acceptable owing to the many positive actions by the individual.

The techniques of neutralization have been applied to research diverse forms of criminal/deviant behavior. It is therefore no surprise to learn that these forms of behavior have recently encompassed IS related areas (Lim, 2002; Lim and Teo, 2005;

Hinduja 2007; Ingram and Hinduja, 2008; Morris and Higgins, 2009; Siponen and Vance, 2010. Siponen and Vance's (2010) study, an important contribution to the compliance literature, adds to earlier IS security work which has considered how dishonest employees may rationalize computer abuse (Harrington, 1996; Willison, 2002, 2006). In the present study, we investigate the use of (1) denial of injury, (2) denial of the victim, and (3) the metaphor of the ledger as moderators of the relationship between perceptions of organizational injustice and the formation of behavioral intention to commit computer abuse. (See Figure 1) This constitutes our second research question – what is the role of neutralization in the formation of behavioral intention?

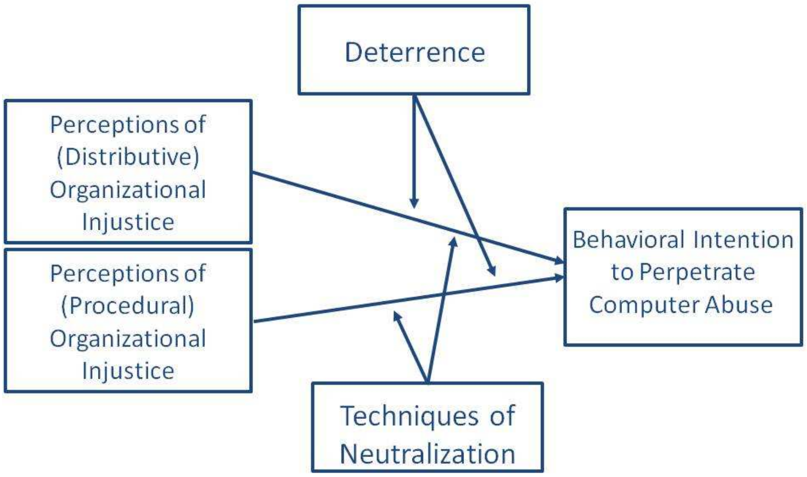

Deterrence
Perceptions of (Distributive) Organizational Injustice
Perceptions of (Procedural) Organizational Injustice
Behavioral Intention to Perpetrate Computer Abuse
Techniques of Neutralization

Figure 1. Conceptual Model

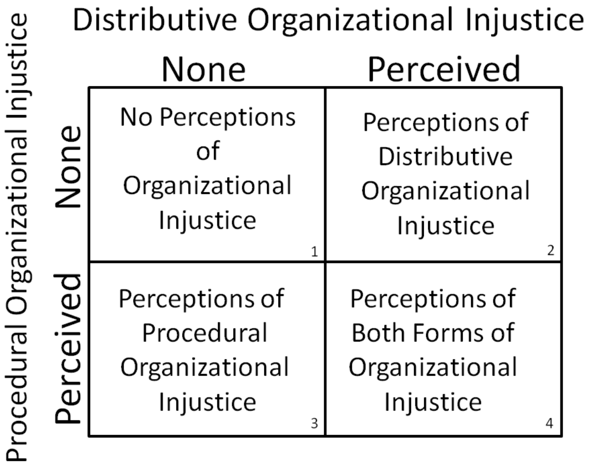
METHOD

To investigate the research questions presented above, we seek to identify a valid and operationalizable plan for measuring the relevant constructs in order to identify the salient relationships so that we may draw significant conclusions of value to both practitioners and researchers in the future. Being able to identify a large sample of actual disgruntled employees who have formed the intention to commit various acts of computer abuse would be the "holy grail" in this endeavor, but is unlikely or impossible. The establishment of a method of measuring the computer abuse intention of working professionals in the context of exposure to organizational factors that are perceived to be unjust is the immediate realistic goal. A rich tradition of using scenario analysis for such research has been established in the criminology field, and has been also applied recently within the Information Systems research community (c.f. Siponen and Vance (2010)). By asking the respondents to read a scenario and put themselves in the context of the scenario's character, the researcher can establish a reliable and valid measure for behavioral intention as it relates to various factors found in the scenario. This is because the respondents are not asked to admit to personal intentions, but rather to place themselves in the positions of scenario characters, where they are more likely to self-report a likelihood to commit a crime.

We believe the factorial survey approach, in particular, provides the best method by which to capture respondent perspectives and intentions following a scenario-driven stimulus. In general, the goal of the factorial survey approach is to reveal the social and individual structures of human decisions. By having respondents evaluate samples of scenarios (fictive descriptions or vignettes), in which several factors describing the object of interest are simultaneously manipulated, this approach has numerous advantages over conventional survey research, especially for investigating security violations (Vance, 2010). To account for the two forms of organizational justice perceptions (distributive and procedural) and the three techniques of neutralization (denial of the victim, denial of injury, and the metaphor of the ledger), a matrix of 64 potential scenario versions was developed and validated with an expert review panel for realism and clarity. In the subsequent data collection phase, following a sample random design without replacement approach (Rossi and Anderson, 1982; Jasso, 2006), a random sample of five scenarios from the potential scenario pool of 64 was selected without replacement back into the pool of 64. This random sample of scenarios is referred to as a deck and each deck was unique for each of the approximately 800 respondents invited to voluntarily participate in the study. Because the population most aligned with this research includes business professionals and managers, the sample will be drawn from working professionals throughout the US. Working professionals are more representative of the entire workforce of professionals, providing valuable insights into the entire phenomenon.

Participants were recruited by a market research organization, and were directed to a web-based survey that started with brief instructions, followed by the presentation of five scenarios, each followed by manipulation check items and a three-item reflective likert-scale measurement of behavioral intention, the latent construct. These instrument items serve as manipulation checks on the introduction of construct values embedded within the scenarios. The instrument items, adapted from Colquitt (2001) and based on Leventhal (1976), measure (and confirm) that the respondent did, in fact, perceive that the scenario's character was treated unjustly (procedural or distributional injustice or both). Example scenarios and selected items are presented in the Appendix as illustration, however space restrictions prevent their complete listing of all 64. Finally, demographic information is acquired from each respondent.

Note that the scenarios cover all four quadrants of the research design seen in Figure 2, and isolate each of the three techniques of neutralization under investigation, each of which will be independently evaluated (see Figure 1). Furthermore, within each quadrant, we have four versions of each to represent four combinations of moderate and high perceptions of perceived sanction certainty and perceived sanction severity (deterrence).



		Distributive Organizational Injustice	
		None	Perceived
Procedural Organizational Injustice	None	No Perceptions of Organizational Injustice 1	Perceptions of Distributive Organizational Injustice 2
	Perceived	Perceptions of Procedural Organizational Injustice 3	Perceptions of Both Forms of Organizational Injustice 4

Figure 2. Research Design – Scenario Categories

RESULTS AND DISCUSSION

Data collection is underway at the time of this writing. Results of data analysis will be presented at the conference, and we will discuss the implications of our work and its impact. Our discussion will address our study's limitations and its implications for theory and practice.

CONCLUSION

The theoretical and empirical contributions of the present study include the introduction and combination of theories related to organizational justice perceptions and techniques of neutralization as explanatory factors for the formation of motivations for insider computer abuse intentions. If practitioners and researchers can gain insights into how the relationship between organizations and their employees can lead to negative consequences, especially in the context of disgruntled employees and their actions, progress can be achieved toward reducing the costly and disruptive computer abuse events that have been documented and are the subject of considerable concern among managers. The present study seeks to offer a theoretical foundation for improved awareness of such factors and antecedents, and to provide empirical support for knowledge regarding the role of techniques of neutralization as either mediators or moderators of the primary relationship. The ultimate goal is the improvement of employee relations and the related reduction in computer abuse activity within organizations.

APPENDIX – ORGANIZATIONAL JUSTICE / NEUTRALIZATION / DETERRENCE SCENARIOS (THREE EXAMPLES)

The survey respondent was presented with instructions, then read five unique scenarios, such as the following:

Perceived Procedural Injustice, (No Perceived Distributive Injustice), Neutralization = Denial of Injury, Perceived Sanction Certainty = Low, Perceived Sanctioned Severity = High

Joe works in a large financial institution where he analyzes investment candidates for his firm. He did the same job as the other analysts who received raises, and he also believed that his work quality was as good as theirs. Last year, Joe did not get a raise, though other analysts in his firm did. Joe did not believe that the raise process was fair. He thought it would not hurt anyone for him to know who received what raise, so Joe decided to steal a supervisor's password (by looking in his desk drawer) so he could log on to the administrative server to see all the employee evaluations of all the analysts in his department. Joe believes his chances of getting caught and punished are low, but if caught, the punishment would be severe.

Perceived Distributive & Procedural Injustice (both), Neutralization = Metaphor of the Ledger, Perceived Sanction Certainty = Low, Perceived Sanctioned Severity = Low

Joe works in a large financial institution where he analyzes investment candidates for his firm. He did the same job as the other analysts who received raises, and he also believed that his work quality was as good as theirs. Last year, Joe did not get a raise, though other analysts in his firm did. Joe believed it was unfair that he did not also get a raise, and also felt that the raise process was unfair. Because Joe thought he had been a model employee for so many years, he figured it would be justified to break the rules just this one time. So Joe decided to steal a supervisor's password (by looking in his desk drawer) so he could log on to the administrative server to see all the employee evaluations of all the analysts in his department. Joe believes his chances of getting caught and punished are low, and if caught, the punishment would be minimal.

Perceived Distributive Injustice, (No Perceived Procedural Injustice), Neutralization = Denial of the Victim, Perceived Sanction Certainty = High, Perceived Sanctioned Severity = High

Joe works in a large financial institution where he analyzes investment candidates for his firm. He did the same job as the other analysts who received raises, and he also believed that his work quality was as good as theirs. Last year, Joe did not get a raise, though other analysts in his firm did. Joe did not believe this was fair. Joe decided to steal a supervisor's password (by looking in his desk drawer) so he could log on to the administrative server to see all the employee evaluations of all the analysts in his department. Joe felt justified in doing this because he felt that he was actual injured party. Joe believes his chances of getting caught and punished are high, and if caught, the punishment would be severe.

Following each scenario, the respondent viewed the manipulation check (see examples below) and the measure of the latent construct – the dependent variable, behavioral intention to commit computer abuse.

1. Did Joe feel it was fair that he didn't get the same raise as the other analysts?
2. Did Joe feel it was not very likely he would be punished for getting access to the data?
3. Did Joe think that his actions wouldn't really hurt anyone?

	SD	D	N	A	SA
In that situation, I would do the same as Joe.	1	2	3	4	5
If I were Joe, I would have also looked at the data that way.	1	2	3	4	5
I think Joe was justified under the circumstances.	1	2	3	4	5

Following the five random scenarios (selected from the set of 64), each respondent answered the demographic questions.

REFERENCES

1. Adams, J. (1965) Inequity in social exchange, in L. Berkowitz (Ed.) *Advances in Experimental Social Psychology*, vol. 2, New York, NY: Academic Press, 267-299.
2. Ambrose, M., Seabright, M., and Schminke, M. (2002) Sabotage in the workplace: The role of organizational justice, *Organizational Behavior and Human Decision Processes*, 89, 1, 947-965.
3. Bies, R., Tripp, T., and Kramer, R. (1997) At the breaking point: Cognitive and social dynamics of revenge in organizations, in R. Giacalone and J. Greenberg (Eds.) *Antisocial Behavior in Organizations*, Thousand Oaks, CA: Sage, 18-36.
4. Bies, R., and Tripp, T. (1998) Revenge in organizations: The good, the bad and the ugly," in R. Griffin, A. O'Leary-Kelly and, J. Collins (Eds.) *Dysfunctional Behavior in Organizations*, Part B: Non-Violent Dysfunctional Behavior, Stamford, CT: JAI Press, 49-68
5. Cohen-Charash, Y., and Spector, P. (2001) The role of justice in organizations: A meta-analysis, *Organizational Behavior and Human Decision Processes*, 86, 2, 278-321.
6. Colquitt, J. (2001) On the dimensionality of organizational justice: A construct validation of a measure, *Journal of Applied Psychology*, 86, 3, 386-400.
7. Cook, P. (1982) Research in criminal deterrence: Laying the groundwork, in N. Morris and M. Tonry (Eds.) *Crime and Justice: A Review of Research*, vol. 2, Chicago, IL: The University of Chicago Press, 211-268.
8. D'Arcy. J., and Hovav, A. (2009) Does one size fit all? Examining the differential effects of IS security countermeasures, *Journal of Business Ethics*, 89, 1, 59-71.
9. Foltz, C. (2000) *The impact of deterrent countermeasures upon individual intent to commit misuse: A behavioral approach*, unpublished Ph.D. dissertation, University of Arkansas.
10. Giacolone, R., Riordan, C., and Rosenfeld, P. (1997) Employee sabotage: Toward a practitioner-scholar understanding, in A. Robert and J. Greenberg (Eds.), *Antisocial Behavior in Organizations*, Thousand Oaks, CA: Sage, 109-129.
11. Greenberg, J. (1990) Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts, *Journal of Applied Psychology*, 54, 1, 81-103.
12. Greenberg, L., and Barling, J. (1999) Predicting employee aggression against coworkers, subordinates and supervisors: The roles of person behaviors and perceived workplace factors, *Journal of Organizational Behavior,* 20, 6, 897-913.
13. Harrington, S. (1996) The effects of ethics and personal denial of responsibility on computer abuse judgments and intentions, *MIS Quarterly*, 20, 3, 257-277.
14. Hinduja, S. (2007) Neutralization theory and online software piracy: An empirical analysis, *Ethics and Information Technology*, 9, 3, 187-204.
15. Hoffer, J., and Straub, D. (1989) The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review*, 30, 4, 35-43.
16. Ingram, J., and Hinduja, S. (2008) Neutralizing music piracy: An empirical examination, *Deviant Behavior*, 24, 4, 334-366.
17. Jasso, G. (2006) Factorial survey methods for studying beliefs and judgments, *Sociological Methods & Research*, 34, 3, 334-423.
18. Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. (2005) Insider threat study: Computer systems sabotage in critical infrastructure sectors. (Available at http://www.cert.org/insider_threat/insidercross.html).
19. Klockars, C. (1974) The professional fence, Free Press, New York.
20. Lee, J., and Lee, Y. (2002) A holistic model of computer abuse within organizations, *Information Management and Computer Security*, 10, 2, 57-63.
21. Lee, S., Lee, S-G., and Yoo, S. (2004) An integrative model of computer abuse based on social control and general deterrence theories, *Information and Management*, 41, 6, 707-718.
22. Leventhal, G. (1980) What should be done with equity theory? in K. Gergen, M. Greenberg, and R. Willis (Eds.) *Social Exchange: Advances in Theory and Research*, New York: Plenum, 27-55.
23. Leventhal, G., Karuza, J., and Fry, W. (1980) Beyond fairness; A theory of allocation preferences, in G. Mikula (ed.), *Justice and Social Interaction*, New York: Springer-Verlag, 167-218.

24. Lim, V. (2002) The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice, *Journal of Organizational Behavior*, 23, 5, 675-694.
25. Lim, V., and Teo, T. (2005) Prevalence, perceived seriousness, justification and regulation of cyberloafing in singapore: An exploratory study, *Information & Management*, 42, 8, 1081-1093.
26. Maruna, S. and Copes, H. (2005) What have we learned from five decades of neutralization research? in M. Tonry (Ed.) *Crime and Justice: A Review of Research*, vol. 32, Chicago: The University of Chicago Press, 221-320.
27. Mitchell, J., and Dodder, R. (1980) An examination of types of delinquency through path analysis, *Journal of Youth and Adolescence*, 9, 3, 239-248.
28. Morris, R. and Higgins, G. (2009) Neutralizing potential and self-reported digital piracy: A multi-theoretical exploration among college undergraduates, *Criminal Justice Review*, 34, 2, 173-195.
29. Nowakowski, J., and Conlon, D. (2005) Organizational justice: Looking back, looking forward, *The International Journal of Conflict Management*, 16, 1, 4-29.
30. Rossi, P.H., and Anderson, A.B. (1982) The factorial survey approach: An introduction, in P.H. Rossi and S.L. Nock (Eds.) *Measuring Social Judgments: The Factorial Survey Approach*, Beverly Hills, CA: Sage, 15-67.
31. Shropshire, J. (2009) A canonical analysis of intentional information security breaches by insiders, *Information Management and Computer Security*, 17, 4, 221-234.
32. Siponen, M. and Vance, A. (2010) Neutralization: New insights into the problem of employee information systems security policy violations, *MIS Quarterly,* 34, 3, 487-502.
33. Skarlicki, D., and Folger, R. (1997) Retaliation in the workplace: The role of distributive, procedural and interactional justice, *Journal of Applied Psychology*, 82, 3, 434-443.
34. Skarlicki, D., Folger, R., and Tesluk, P. (1999) Personality as a moderator in the relationship between fairness and retaliation, *Academy of Management Journal*, 42, 1, 100-108.
35. Straub, D. (1990) Effective IS security: An empirical study, *Information Systems Research*, 1, 3, 255-276.
36. Straub, D., Carlson, P., and Jones, E. (1992) Deterring highly motivated computer abusers: A field experiment in computer security, in G. Gable and W. Caelli (Eds.) *IT Security: The Needs for International Cooperation*, Amsterdam: Elsevier Science Publishers, 309-324
37. Straub, D., and Welke, R. (1998) Coping with systems risks: Security planning models for management decision making, *MIS Quarterly*, 22, 4, 441-469.
38. Sykes, G., and Matza, D. (1957) Techniques of neutralization: A theory of delinquency, *American Sociological Review*, 22, 6, 664-670.
39. Vance, Anthony. (2010) The factorial survey method: Applications for information security and privacy research, presentation at Dewald Roode Information Security Workshop, IFIP WG8.11/11.13, October 8-9, Bentley University, Boston, Massachusetts.
40. Warkentin, M., and Willison, R. (2009) Behavioral and policy issues in information systems security: The insider threat, *European Journal of Information Systems*, 18, 2, 101-105.
41. Willison, R. (2002) *Opportunities for computer abuse: Assessing a crime specific approach in the case of barings bank*, unpublished Ph.D. dissertation, University of London.
42. Willison, R. (2006) Understanding the perpetration of employee computer crime in the organisational context, *Information and Organization*, 16, 4, 304-324.
43. Willison, R., and Warkentin, M. (2009) Motivations for employee computer crime: Understanding and addressing workplace disgruntlement through the application of organizational justice, in Vance, A. (Ed.) *Proceedings of the 1st IFIP 8.2 Security Conference*, Capetown, South Africa.
44. Willison, R. and Warkentin, M. (2011) Extending the zone of control for addressing employee computer abuse: The extended security action cycle, *MIS Quarterly*, under 2nd review.
45. Workman, M., and Gathegi, J. (2007) Punishment and ethics deterrents: A study of insider security contravention, *Journal of the American Society for Information Science and Technology*, 58, 2, 212-222.