MIS Quarterly

RESEARCH ARTICLE

A LONGITUDINAL STUDY OF UNAUTHORIZED ACCESS ATTEMPTS ON INFORMATION SYSTEMS: THE ROLE OF OPPORTUNITY CONTEXTS

Jingguo Wang
Department of Information Systems and Operations Management, College of Business,
University of Texas at Arlington, Arlington, TX 76019 U.S.A. {jwang@uta.edu}

Zhe Shan
Department of Information Systems and Analytics, Farmer School of Business, Miami University,
Oxford, OH 45056 U.S.A. {jayshan@miamioh.edu}

Manish Gupta
Department of Management Science and Systems, School of Management,
State University of New York at Buffalo, Amherst, NY 14260 U.S.A. {mgupta3@buffalo.edu}

H. Raghav Rao
Department of Information Systems and Cyber Security, College of Business,
University of Texas at San Antonio, San Antonio, TX 78249 U.S.A. {hr.rao@utsa.edu}

Appendix A

Prior Studies of Insider Threats

Researchers have used the lens of social sciences to examine the characteristics of insider threats to understand motivation and subsequently develop appropriate organizational policies (Hunker and Probst 2011). Based on a database of insider threat cases, researchers in the CERT Insider Threat Center conducted a number of case studies to examine personal predispositions, organizational factors, and behavioral cues of malicious insiders (Cappelli et al. 2008; Cummings et al. 2012; Randazzo et al. 2004). Other researchers have also suggested various individual characteristics and organizational factors that may lead to insider threats (Costa et al. 2016; Liang et al. 2016; Magklaras and Furnell 2001, 2005; Shaw et al. 1998). Relying on those findings, predictive and analytical models have been proposed to identify malicious insiders (e.g., Band et al. 2006; Bishop et al. 2010; Maybury et al. 2005; Moore et al. 2008a; Nurse et al. 2014; Schultz 2002; Shaw et al. 1998). In particular, Gheyas and Abdallah (2016) provide a systematic literature review and meta-analysis of studies in detection and prediction of malicious insiders. Table A1 lists some example studies.

Additionally, a major stream of studies in the area of information systems examines what motivates employees to comply with or violate organizational security policies. Table A2 lists some example studies. Both Cram et al. (2018) and Teodor et al. (2014) carry out an extensive review of relevant journal articles and summarize organizational and individual factors (e.g., dispositional traits, sanctions, rewards, etc.). Most have conducted cross-sectional surveys to collect data, with the respondents' intention as the dependent variable.

Moreover, several studies have drawn upon environmental criminology and situational crime prevention (SCP) to address system risk from the offender's perspective (Willison 2006; Willison and Backhouse 2006; Willison and Siponen 2009). The fundamental premise of SCP is that crimes (cybercrimes or others) occur when a person has both motive and opportunity, so by either removing motive or denying a malicious

user an opportunity, one can help prevent crimes (Cullen and Agnew 2011). In short, SCP believes manipulating opportunities is a more promising crime prevention strategy than trying to make people less criminally inclined (Clarke 1980). Similar concepts such as problem-oriented policing and crime prevention through environmental design all seek to reduce opportunities for crime in practical ways at low social and economic cost (Cohen et al. 1980). Along this line, some conceptual frameworks have been proposed to mitigate insider threats from an opportunity-based perspective (Beebe and Rao 2005; Padayachee 2013, 2015, 2016; Willison 2006; Willison and Backhouse 2006; Willison and Siponen 2009). However, most of these discussions and investigations are conceptual or qualitative in nature. Empirical evidence through the application of environmental criminology such as multilevel criminal opportunity theory is sparse.

To help fill in the literature gap, this study empirically investigates the applicability of environmental criminology, specifically multilevel criminal opportunity theory, to explain unauthorized access attempts. We contextualize the aforementioned theory in the domain of insider threats and examine the role of opportunity contexts in driving insider threats to information systems in a financial institution.

Table A1 Example Studies in Insider Threats

Reference	Methodology	Theory	Data	Major Findings
Shaw et al. (1998)	Qualitative study	N/A	Interviews with convicted criminals	Psychological characteristics, such as computer dependency, ethical flexibility, and lack of empathy as potential indicators of a risk for destructive and potentially illegal behavior.
Straub and Welke (1998)	Qualitative study	General deterrence theory, and model of managerial decision making	Two information services Fortune 500 firms	Managers should initiate a theory-based security program that includes (1) use of a security risk planning model, (2) education in security awareness, and (3) Countermeasure Matrix analysis.
Shaw et al. (1999)	Case Study	N/A	46 cases with sufficient details from a DoD-sponsored project in 1997	Staff security awareness should be considered as sine qua non for a sound insider strategy, and describe three levels of user awareness: perception, understanding, and prediction.
Willison (2000)	Conceptual development	Situational crime prevention (SCP): Environmental criminology	N/A	Crimes (cyber crimes or others) occur when a person has both motive and opportunity—so by either removing motive or denying a malicious user an opportunity, we can help prevent crime.
Lee and Lee (2002)	Conceptual development	Theory of planned behavior, social bond theory and social learning theory	N/A	Model of computer abuse uses social criminology theories to account for why a person commits computer abuse and what factors significantly affect the computer abuse decision.
Beebe and Rao (2005)	Conceptual development	Situational crime prevention theory	NA	Situational crime prevention theory may offer new insights into improving IS security effectiveness by reducing the criminal's anticipated rewards from the crime.
Theoharidou et al. (2005)	Critical analysis	Criminology theories	800 organizations	ISO17799 follows the General Deterrence Theory. Consequently, it emphasizes on measures such as posing sanctions, reinforcing access control, and implementing training and awareness programs.
Band et al. (2006) and Moore et al. (2008b)	Analytical modeling	System dynamics	Insider IT sabotage and espionage cases	Behaviors, motivations, and personality disorders are associated with insider crimes such as antisocial or narcissistic personality.
Willison (2006); Willison and Backhouse (2006)	Case study	Routine activity theory, environmental criminology, rational choice perspective	Baring Bank case	It addresses systems risk from the offender's perspective. A model known as "crime-specific opportunity structure" is proposed. The model aids the conceptualization of the relationship between the offender, the organizational context, the requisite safeguards and the departments responsible for them.
Humphreys (2008)	Critical analysis	NA	NA	ISO/IEC 27001 can be used by different sectors and various organizations. It provides a flexible holistic approach to information security in the sense that it addresses people, process, legal and IT aspects.
Colwill (2009)	Critical analysis	Human factors and security risk management	N/A	Insider threats to information security cannot be totally eliminated but it can be assessed and managed. Human factors provide practical levers to gain a better understanding of the real risks facing organizations in today's global commercial environment.

Reference	Methodology	Theory	Data	Major Findings
Bishop et al. (2010)	Analytical modeling	Predictive analytics	N/A	Traditional cyber security audit data and psychosocial data can be integrated to predict possible insider exploits. However, certain types of errors that one expects in a predictive system can affect the usefulness of the results.
Munshi et al. (2012)	Critical analysis	Various theories used in insider threats research	Academic research and reported incidents	A holistic conceptual model is needed to encapsulate a broader perspective of the insider situation and reflect more closely empirical experiences.
Padayachee (2013), Padayachee (2015), Padayachee (2016)	Conceptual development	Rational choice theory, routine activities theory, situational crime prevention	A three-round Delphi process with 23 experts from the industry	A conceptual framework was developed to mitigate the insider threat from an opportunity-based perspective. The exploratory evaluation of opportunity-reducing techniques may inform organizations in designing controls and are situationally appropriate to mitigate insider threats.
Willison and Warkentin (2013)	Conceptual development	N/A	N/A	Extends Straub and Welke's (1998) security action cycle framework and proposes three areas for empirical investigation—techniques of neutralization (rationalization), expressive/instrumental criminal motivations, and disgruntlement as a result of perceptions of organizational injustice.
Liang et al. (2016)	Analytical modeling	Trait theory	133 real-world cases of offenders from military units, intelligence agencies, and business organizations	It validates malicious insider characteristics identified in previous research, thereby establishing a foundation for more comprehensive research in the future.

Table A2. Example Studies in Information Security

Reference	Research Question	Methodology	Theory	Independent Variables	Dependent Variables	Data	Major Findings
Abuse and Misuse of IS Resources							
Straub and Nance (1990)	1. How is computer abuse discovered in organizations? 2. How are identified computer abusers disciplined?	Field study	Deterrence theory	Abuse type, target asset, organization size, organization industry	Incident discovery: accidental discovery, normal system controls.	Victimization surveys of 1,063 randomly selected members of the Data Processing Management Association	Detection and punishment of violators reduce computer abuse.
Straub (1990)	1. Have IS security deterrents been effective in lowering computer abuse? 2. Can rival explanations explain lower incidence of computer abuse?	Survey study	Deterrence theory	Deterrents: IS security efforts, dissemination of information about penalties, guidelines for acceptable system use, policies for system use	Computer abuse: number of incidents, actual dollar loss, opportunity dollar loss	Survey collected from 1,211 randomly selected organizations	Use of IS security deterrents resulted in a decreased incidence of computer abuse. The effective deterrents increase employees' risk of getting caught .
Gopal and Sanders (1997)	How do preventive and deterrent controls to counter software piracy impact on software publisher profits?	Analytical modeling, survey study	Deterrence theory	Preventive control, deterrent control	Profitability		Policy statements prohibiting software piracy and warning of its legal consequences resulted in lower piracy intentions. Preventive controls decrease profits, but deterrent controls can potentially increase profits.
				Deterrence information, ethical index, gender, age	Club size	Questionnaires collected from 130 MBA students	
Lee et al. (2004)	How do social control theory and general deterrence theory explain computer abuse?	Survey study	Social control theory, general deterrence theory	Security awareness, physical security system, attachment, commitment, involvement, norms, self defense, etc.	Invaders' abuse, Insiders' abuse	Questionnaires to 500 MBA students and 500 middle managers in six Korean companies.	Deterrence factors influence self defense intention (SDI) and organizational factors significantly affect induction control intention (ICI).

Reference	Research Question	Methodology	Theory	Independent Variables	Dependent Variables	Data	Major Findings
D'Arcy et al. (2009)	How to develop an extended deterrence theory model to better explain the relationships between security countermeasures, sanction perceptions, and IS misuse?	Field study	Deterrence theory	User awareness, SETA program, computer monitoring	IS misuse intention	269 computer users from eight different companies	Three practices deter IS misuse: user awareness of security policies; security education, training, and awareness programs; and computer monitoring. Perceived severity of sanctions is more effective in reducing IS misuse than certainty of sanctions.
Policy Compliance							
Harrington (1996)	1. Do codes deter unethical behavior of IS employees? 2. Is the effect of codes moderated by the psychological traits of the IS employee?	Survey study	Deterrence theory	RD, Robin Hood, Rationalization, Intention, Less Damaging Judgment, Less Damaging Intention	Cracking Judgement, Cracking intention, Copy S/W Judgement, Copy S/W Intention, etc.	Questionnaire given to 219 IS employees in 9 organizations in the northeastern Ohio area	Codes of ethics applied to the organization generically did not affect employees' judgements or intentions to commit computer abuse.
Myyry et al. (2009)	What levels of moral reasoning and values explain adherence to information security rules?	Survey study	Theory of cognitive moral development; theory of motivational types of values	Preconventional reasoning, conventional reasoning, postconventional reasoning, openness to change, conversation.	Hypothetical compliance with information security policy, actual compliance with information security policy	132 respondents (clerical employees in a technical service center, or part-time master's students with work experience in Finland)	People who exhibit preconventional moral reasoning are more likely to obey the policies.
Siponen and Vance (2010)	Can neutralization theory provide a compelling explanation for IS security policy violations and offers new insight into how employees rationalize this behavior?	Field study	Neutralization theory, deterrence theory	Defense of Necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, denial of responsibility, etc.	Intention to violate IS security policy	Over 360 administrative personnel from three organizations in Finland	Employees may use neutralization techniques to minimize the perceived harm of their policy violations. This rationalizing behavior reduces the deterring effect of sanctions.
Bulgurcu et al. (2010)	1. What are the broad classes of an employee's beliefs about the overall assessment of consequences of compliance or noncompliance that influence attitude toward compliance and, in turn, intention to comply with the ISP? 2. What are an employee's beliefs about the outcomes of compliance and noncompliance that influence beliefs about the overall assessment of consequences?	Survey study	Theory of planned behavior	Information security awareness, perceived benefit of compliance, intrinsic benefit, safety of resources, rewards, perceived cost of compliance, work impediment, perceived cost of noncompliance, intrinsic cost, vulnerability of resources, sanctions, attitude, normative beliefs, self-efficacy to comply	Intention to comply	464 panel members provided by a US professional market research company	Employee's intention to comply with the information security policies is significantly influenced by attitude, normative beliefs, and self-efficacy to comply. Outcome beliefs significantly affect beliefs about overall assessment of consequences, and therefore significantly affect an employee's attitude. Furthermore, information security awareness positively affects both attitude and outcome beliefs.

Reference	Research Question	Methodology	Theory	Independent Variables	Dependent Variables	Data	Major Findings
Johnston and Warkentin (2010)	How do fear appeals modify end user behavioral intentions associated with recommended individual computer security actions?	Laboratory experiment	Protection motivation theory	Perceived threat severity, perceived threat susceptibility, response efficacy, social influence, self efficacy	Behavioral intent	275 faculty, staff, and students from multiple units at one large university	Fear appeals do impact end user behavioral intentions to comply with recommended individual acts of security, but the impact is not uniform across all end users.
Guo et al. (2011)	What factors influence end user attitudes and behavior toward organizational IS security?	Survey study	Composite behavior model (an extension to the theory of reasoned action)	Attitude toward security policy, relative advantage for job performance, perceived security risk, perceived sanctions, etc.	NMSV intention	335 computer users via both paper-based (approached at business buildings) and Web-based surveys	Utilitarian outcomes, normative outcomes, and self-identity outcomes are key determinants of end user intentions to engage in non-malicious security violation.
Xue et al. (2011), similar studies: Liang et al. (2013), Chen et al. (2012)	How does punishment affect employee compliance intention in mandatory IT settings?	Field survey	Punishment research and justice theory	Actual punishment, Punishment expectancy, Perceived justice of punishment, Satisfaction, Perceived usefulness, Perceived ease of use	Compliance intention	118 ERP users at one of China's top 500 enterprises	IT compliance intention is strongly influenced by perceived justice of punishment, which is negatively influenced by actual punishment.
D'Arcy et al. (2014)	How does employee stress caused by burdensome and ambiguous information security requirements impact employee's deliberate information security policy violations?	Survey study	Coping theory	Security-related stress: overload, complexity, uncertainty; Moral disengagement: reconstrue conduct, obscure or distort, devalue the target	ISP violation intention	539 employee users	Security-related stress engenders an emotion-focused coping response in the form of moral disengagement from ISP violations, which in turn increases one's susceptibility to this behavior.
Vance et al. (2015)	1. How can UI design artifacts increase perceptions of accountability in the users of a broad-access system? 2. Can increases in user accountability reduce intentions to violate access policies?	Design science	Accountability theory	Identifiability, expectation of evaluation, awareness of monitoring, social presence, perceived accountability	Intention to violate the access policy	114 employees with administrative access to the academic records system of a large private university	Four user-interface design artifacts were developed to raise users' accountability perceptions within systems and in turn decrease access-policy violations.
Hsu et al. (2015)	1. What are the consequences of organizational in-role and extra-role security behaviors on the effectiveness of ISPs? 2. What is the role of formal and social controls in enhancing in-role and extra-role security behaviors in organizations?	Survey study	Social control theory	Department level: extra-role behaviors, in-role behaviors	Department level: ISP effectiveness	IS managers and employees at many organizations	Extra-role behaviors are important in improving ISP effectiveness. Formal control and social control individually and interactively enhance both in- and extra-role security behaviors.
				Individual level: involvement, attachment, belief, commitment, specification, evaluation, reward, social control, formal control	Individual level: extra-role behaviors, In-role behaviors		

Appendix B

Comparison Between the Current Study and Wang et al. (2015)

Table B1 Comparison between the Current Study and Wang et al. (2015)

	Wang et al (2015)	Current Study
Research Question	What kinds of IS applications are more likely to experience unauthorized attempts?	Under what circumstances will insiders be more likely to make unauthorized attempts?
Unit of analysis	IS Application.	Employee-month.
Dependent Variables	1. The inter-arrival times of two consecutive unauthorized attempts on an application. 2. The number of unauthorized attempts on an application in a unit time.	The number of repeated unauthorized attempts an employee had in a month.
Theoretical Framework	Routine activity theory.	Multilevel criminal opportunity theory.
Hypotheses	Application characteristics that reflect value, inertia, visibility, and accessibility contributes to the victimization risk of an application.	Insiders accessing the IS applications under the contexts presenting an opportunity to exploit will be more likely to make unauthorized attempts.
Analysis Techniques	1. Survival analysis with a Weibull hazard model. 2. Count data analysis with a zero-inflated Poisson-Gamma model.	Multilevel linear regression.
Findings	The study investigates victimization risk and attack proneness associated with IS applications. It supports the empirical application of routine activity theory in understanding insider threats, and provide a picture of how different applications have different levels of exposure to such threats.	This study investigates how opportunity contexts impact employees' unauthorized access attempts on IS applications. It contextualizes multilevel criminal opportunity theory and suggests the important roles of contextual variables in leading to insider threats. Further, it shows that the results do not align with employees who might not know the systems well enough and could be making mistakes.

References

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., and Trzeciak, R. F. 2006. "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," Carnegie Mellon University Software Engineering Institute.

Beebe, N. L., and Rao, V. S. 2005. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security," in *Proceedings of the 2005 SoftWars Conference*, Las Vegas, NV, pp. 1-18.

Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., and Whalen, S. 2010. "A Risk Management Approach to the 'Insider Threat,'" in *Insider Threats in Cyber Security*, C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop (eds.), New York: Springer, pp. 115-137.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., and Willke, B. J. 2008. "Management and Education of the Risk of Insider Threat (Merit): System Dynamics Modeling of Computer System Sabotage," Carnegie Mellon University Software Engineering Institute (http://www.dtic.mil/docs/citations/ADA632604).

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

Clarke, R. V. 1980. "Situational Crime Prevention: Theory and Practice," *British Journal of Criminology* (20), pp. 136-137.

Cohen, L. E., Felson, M., and Land, K. C. 1980. "Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977; with Ex Ante Forecasts for the Mid-1980s," *American Journal of Sociology* (86:1), pp. 90-118.

Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat—Who Can You Trust These Days?," *Information Security Technical Report* (14:4), pp. 186-196.

Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., and Spooner, D. L. 2016. "An Insider Threat Indicator Ontology," CERT Center and Carnegie Mellon University Software Engineering Institute (http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf).

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2018. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605-641.

Cullen, F. T., and Agnew, R. 2011. *Criminologyical Theory: Past to Present*, Oxford, UK: Oxford University Press.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., and Trzeciak, R. 2012. "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," Carnegie Mellon University (http://www.dtic.mil/docs/citations/ADA610430).

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Gheyas, I. A., and Abdallah, A. E. 2016. "Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis," *Big Data Analytics* (1:1), Article 6.

Gopal, R. D., and Sanders, G. L. 1997. "Preventive and Deterrent Controls for Software Piracy," *Journal of Management Information Systems* (13:4), pp. 29-47.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203-236.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257-278.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Humphreys, E. 2008. "Information Security Management Standards: Compliance, Governance and Risk Management," *Information Security Technical Report* (13:4), pp. 247-255.

Hunker, J., and Probst, C. W. 2011. "Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (2:1), pp. 4-27.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security* (10:2), pp. 57-63.

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41:6), pp. 707-718.

Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring Employees' It Compliance: Carrot or Stick?," *Information Systems Research* (24:2), pp. 279-294.

Liang, N., Biros, D. P., and Luse, A. 2016. "An Empirical Validation of Malicious Insider Characteristics," *Journal of Management Information Systems* (33:2), pp. 361-392.

Magklaras, G., and Furnell, S. 2001. "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse," *Computers & Security* (21:1), pp. 62-73.

Magklaras, G. B., and Furnell, S. M. 2005. "A Preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems," *Computer & Security* (24), pp. 371-380.

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., and Longstaff, T. 2005. "Analysis and Detection of Malicious Insiders," MITRE Corp. (http://www.dtic.mil/docs/citations/ADA456356).

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. 2008a. "The "Big Picture" of Insider IT Sabotage across U.S. Critical Infrastructures," CERT Center and Carnegie Mellon University Software Engineering Institute (http://link.springer.com/chapter/10.1007/978-0-387-77322-3_3).

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. 2008b. *The "Big Picture" of Insider IT Sabotage across US Critical Infrastructures*, New York: Springer.

Munshi, A., Dell, P., and Armstrong, H. 2012. "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents," in *Proceedings of 45th Hawaii International Conference on System Science*, Los Alamitos, CA: IEEE Computer Society Press, pp. 2402-2411.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., and Creese, S. 2014. "A Critical Reflection on the Threat from Human Insiders—Its Nature, Industry Perceptions, and Detection Approaches," in *Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust*, New York: Springer, pp. 270-281.

Padayachee, K. 2013. "A Conceptual Opportunity-Based Framework to Mitigate the Insider Threat," in *Proceedings of the Information Security for South Africa 2013 Conference*, pp. 1-8.

Padayachee, K. 2015. "A Framework of Opportunity-Reducing Techniques to Mitigate the Insider Threat," in *Proceedings of the Information Security for South Africa 2015 Conference*, pp. 1-8.

Padayachee, K. 2016. "An Assessment of Opportunity-Reducing Techniques in Information Security: An Insider Threat Perspective," *Decision Support Systems* (92), pp. 47-56.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. 2004. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," U.S. Secret Service and CERT Coordination Center/Carnegie Mellon University Software Engineering Institute (http://www.secretservice.gov/ntac/its_report_040820.pdf).

Schultz, E. E. 2002. "A Framework for Understanding and Predicting Insider Attacks," *Computers & Security* (21:6), pp. 526-531.

Shaw, E., Ruby, K., and Post, J. 1998. "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," *Security Awareness Bulletin* (2:98), pp. 1-10.

Shaw, E. D., Post, J. M., and Ruby, K. G. 1999. "Inside the Mind of the Insider," *Security Management* (43:12), pp. 34-44.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.

Straub, D. W., and Welke, R. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Teodor, S., Jonas, H., Kristoffer, L., and Johan, B. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42-75.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of ISO 17799," *Computers & Security* (24:6), pp. 472-484.

Vance, A., Benjamin Lowry, P., and Eggett, D. 2015. "Increasing Accountability through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly* (39:2), pp. 346-366.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly* (39:1), pp. 91-112.

Willison, R. 2000. "Understanding and Addressing Criminal Opportunity: The Application of Situational Crime Prevention to IS Security," *Journal of Financial Crime* (7:3), pp. 201-210.

Willison, R. 2006. "Understanding the Offender/Environment Dynamic for Computer Crimes," *Information Technology & People* (19:2), pp. 170-186.

Willison, R., and Backhouse, J. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective," *European Journal of Information Systems* (15:4), pp. 403-414.

Willison, R., and Siponen, M. 2009. "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention," *Communications of the ACM* (52:9), pp. 133-137.

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

Xue, Y., Liang, H., and Wu, L. 2011. "Punishment, Justice, and Compliance in Mandatory IT Settings," *Information Systems Research* (22:2), pp. 400-414.