European Journal of Information Systems

ISSN: 0960-085X (Print) 1476-9344 (Online) Journal homepage: https://www.tandfonline.com/loi/tjis20

Behavioral and policy issues in information systems security: the insider threat

Merrill Warkentin & Robert Willison

To cite this article: Merrill Warkentin & Robert Willison (2009) Behavioral and policy issues in information systems security: the insider threat, European Journal of Information Systems, 18:2, 101-105, DOI: 10.1057/ejis.2009.12

To link to this article: https://doi.org/10.1057/ejis.2009.12

European Journal of Information Systems (2009) 18, 101–105

www.palgrave-journals.com/ejis/

GUEST EDITORIAL

Behavioral and policy issues in information systems security: the insider threat

Merrill Warkentin and
Robert Willison

European Journal of Information Systems (2009) **18,** 101–105.
doi:10.1057/ejis.2009.12

Modern global economic and political conditions, technological infrastructure, and socio-cultural developments all contribute to an increasingly turbulent and dynamic environment for organizations, which maintain information systems (IS) for use in business, government, and other domains. As our institutions (economic, political, military, legal, social) become increasingly global and inter-connected; as we rely more on automated control systems to provide us with energy and services; and as we establish internet-based mechanisms for coordinating this global interaction, we introduce greater vulnerability to our systems and processes. This increased dependence on cyberspace also inflates our vulnerability – isolation is no longer an option. Perhaps no aspect of this phenomenon is as alarming and challenging as the need to understand and address the various risks to the security of the IS on which we depend.

Security risks arise from multiple sources and motivations. In a taxonomy developed by Loch, *et al.* (1992), threats to IS security were categorized into four dimensions – those that are external (both human and non-human) and those that are internal (human and non-human). The research focus of those in engineering and computer science is predominantly on the external threats, and a plethora of artifacts have been developed to protect the organization's perimeter (e.g., intrusion detection systems, firewalls, anti-malware software, etc.). Within the MIS research tradition, there has been a significant effort to investigate human perpetrators of IS security threat, especially from those who are within the organization (behind the firewall, as it were). In the Loch, *et al.* (1992) framework, these sources of threat were further characterized by their intention (intentional *vs* accidental). Much of the focus within the behavioral research community has been on IS security policy non-compliance by employees. Such acts may be intention-based, willful, malicious violation (such as sabotage, data theft, data destruction, etc.) or they may be unintentional or accidental actions, including forgetting to change passwords, failing to log off before leaving a workstation, or careless discarding of sensitive information rather than shredding it. Warkentin (1995) expanded the taxonomy to include low-grade and high-grade threats; the latter being a purposeful individual or organization who will seek obscure vulnerabilities and inflict far greater economic damage by maintaining intrusions for the maximum long-term gain.

So risks from intentional human activity are especially dangerous, especially in a world full of new, more sophisticated hackers, spies, terrorists, and criminal organizations which are committed to coordinated global attacks on our information assets in order to achieve their goals. Some malicious individuals wish to inflict damage and loss for political reasons or for military purposes, some are seeking 'trade secrets' and proprietary corporate information, and others are seeking financial information with which to conduct fraud, identity theft, and other criminal acts. Another category of risks has arisen from new classes of

increasingly devious and effective malware capable of penetrating even the most recent perimeter defenses. These include viruses, worms, trojans, rootkits, and distributed botnet attacks.

But the greatest threat of all is the insider threat – the organizational member who is a 'trusted agent' inside the firewall (Im & Baskerville, 2005; Stanton *et al*., 2005; Willison, 2006; Willison & Backhouse, 2006). This employee or other constituent with a valid username and password regularly interacts with the information assets of the organization. Employees can initiate great harm to the confidentiality, integrity, or availability of the IS through deliberate activities (disgruntled employee or espionage) or they may introduce risk via passive non-compliance with security policies, laziness, sloppiness, poor training, or lack of motivation to vigorously protect the integrity and privacy of the sensitive information of the organization and its partners, clients, customers, and others. This has been termed the 'endpoint security problem' (Warkentin *et al*., 2004) because the individual employee is the endpoint of the IS and its network. (It is sometimes said that the greatest network security problem – the weakest link – is between the keyboard and the chair.) Insiders often have direct access to the entire network from their endpoint, and can pose a major threat. In a global survey of nearly 1400 companies in 50 countries, researchers found that awareness and personnel issues remain the 'most significant challenge to delivering successful information security initiatives' (Ernst & Young, 2008). Though social engineering often provides the path of least resistance to hackers, only 19% of respondents in this survey conduct social engineering tests of employees, but 85% reported regular tests of internet security. The insider threat has repeatedly been called the greatest threat to information security, and yet this is often overlooked in a rush to protect the perimeter with ever-increasingly sophisticated perimeter controls. Greater emphasis on hiring, training, and motivating employees to act securely will generate great payoff for the organizations that pursue this strategy.

Numerous approaches and perspectives have been used to investigate enterprise IS security management. The focus of this special issue is on the individual computer user, the workgroup, and/or the organization and its processes as they relate to the pursuit of IS security. Organizations typically develop and implement plans, policies, protocols, and procedures for ensuring the security of information resources, along with user training programs and governance structures to promote compliance with security policies and procedures (Warkentin & Johnston, 2008). Working against these efforts are dishonest employees intent on perpetrating some form of computer crime, as well as sloppy or unmotivated employees who fail to maintain a secure environment due to accidental or careless actions. What factors cause some individual users and groups to maintain compliance with security policies, whereas others accidentally or intentionally violate security rules and procedures? What motivators and inhibitors are effective in ensuring compliance or in preventing intentional actions of computer crime, hacking, espionage, or sabotage? How can compliance with security policies and procedures be achieved? What are the causes of non-compliance? What factors within the organizational context may motivate an employee to commit computer crime? How do we understand the criminal behavior of these offenders? These research questions motivated our planning for this special issue.

Researchers have investigated various antecedents of security policy compliance and non-compliance, and, not surprisingly, the theoretical foundations have been familiar ones – the technology acceptance model, organizational behavior, social influence, and so forth. We believe that, although these can be (and will continue to be) fruitful areas for understanding the motivation of individuals, we must incorporate new avenues of exploration into our repertoire. We should expand our horizons and incorporate not only new theoretical foundations, but new methodological approaches as well. We can learn from other cognitive and behavioral sciences, including criminal justice, education, ethics, and others.

The issue of compliance obviously relates to the behaviors of honest employees, who, for whatever reason, may or may not abide by an organization's security policy. However, we should not forget that with regard to IS security in the organizational context, there is another form of behavior that should be considered – the behavior of the offender. Interestingly, this is an area of research which has received far less attention from the IS security community. Yet a focus on the offender has the potential to open up original areas for future research. Traditionally, IS security countermeasures have been categorized into four types, which include deterrence, prevention, detection, and recovery (Forcht, 1994; Parker, 1998; Straub & Welke, 1998). Compliance research, therefore, involves attempts to improve 'prevention' methods. Employee behavior relating to password use would be an obvious example. If an individual is or is not compliant with a policy, his or her behavior is linked to the technical system, which aims to 'prevent' computer abuse. However, with a focus on offender behavior, it is possible to move away from this area of control. But this is dependent on the application of appropriate theories for appropriate problems. For this purpose, IS security researchers need not reinvent the wheel. Existing bodies of divergent theory enable an understanding of offender behavior, not only during perpetration, but also importantly, prior to the commission process. If these 'appropriate' theories can be drawn from, there exists the potential to fully develop an understanding of this second form of behavior and expand the range of safeguards beyond the traditional deterrence, prevention, detection and, recovery classification (Straub & Welke, 1998).

A recent paper (Willison, 2009) illustrates this point. Although research on the 'insider' threat is increasing, there currently exists a lack of insight into the problem of employee disgruntlement and how this plays a role in motivating some form of computer crime. To address this problem, Willison (2009) draws on a body of theory called Organizational Justice, which examines how different organizational phenomena can influence employees' perceptions of fairness. It is argued that through the application of this theory, a better understanding of the dynamics of disgruntlement is provided. This enables the implementation of measures which can stop the formation of, but also dissipate, pre-existing disgruntlement. Importantly, disgruntlement temporally occurs prior to behavior addressed by deterrent safeguards. Hence, through the application of Organizational Justice, this offers organizations the possibility to expand their range of safeguards. For while companies may rely heavily on controls to prevent employee computer crime, why not mitigate disgruntlement and thereby forestall initial elements of criminal behavior?

In terms of the total (expected) value of security threats to be mitigated while managing system security, one must establish the set of all possible threats, then apply a formula (see Warkentin, 1995) that summates for each threat the product of the damage to be expected, should that threat occur, and the probability of its occurrence. For example, a devastating natural disaster may wipe out a data center, but the chances of it happening in a specific location may be low, whereas the probability of inaccurate data entry may be higher, but the potential loss is far lower. Importantly, the expected value of the total cost of a malicious attack from an insider can have a far greater financial impact than countless minor acts of omission, carelessness, or oversight by well-meaning, but insufficiently trained or poorly motivated employees. Indeed, what makes the criminal insider threat so dangerous is the fact that such individuals commit crimes in the context of their workplace – the environment which provides them the targeted training and exposure to the very skills and knowledge (knowledge of accounting procedures, knowledge of security flaws, seniority and authority, computer software skills, etc.) that enable them to execute their criminal acts. Parker (1998) advocates considering 'cyber-criminals' in terms of their skills, knowledge, resources, authority, and motive. Dishonest employees very often have these attributes in abundance, and when such a threat is executed, the financial consequences can be devastating. Placing a greater research emphasis on the criminal offender would therefore appear to be a worthwhile cause. So an increased emphasis on the individual who commits the crime, rather than on the individual who merely exhibits minor non-compliance, would be warranted by the far greater financial impact. This is the major motivation for an increased analysis of this nomological net through the new lenses of sociology and criminology research, including deviant behavior research, organizational justice research, agency theory, psychological theories, organizational behavior, perceived organization support, and other theories and methods for investigating human behavior. We believe this call for research represents a viable agenda for the future.

This special issue consists of six papers, all of which consider the relationship between IS security and the behavior of employees for enforcing this function. Research of this nature is timely, for while lip service is paid to the importance of IS security, questions have been raised concerning the quality of academic research in this area. Siponen *et al.* (2008), for example, reviewed the IS security literature for the period 1990–2004, including the three main IS security journals and relevant papers found in the top 20 IS journals. Covering 1280 papers and analyzed in terms of their theories, methods and topics, the results are sobering. The application of theory is considered a key element of good research, yet no theory was cited in 1043 papers. In terms of the methods used for empirical research, the percentage of papers, which conducted field studies (0.07%), surveys (5.31%), case studies (2.65%), and action research (0.07%) proved equally deficient. Finally, although the need to consider the more social aspects of IS security has long been recognized, the topics 'security education' and 'security awareness' accounted for only two and seven papers, respectively. These figures are telling when compared with the 'maturity' of other IS sub-disciplines. Several IS studies have noted that as a discipline matures, the application of theory and the number of empirical studies increases (Farhoomand, 1987; Farhoomand & Drury, 1999; Vessey *et al.*, 2002). This is accompanied by a move from a technological to or more 'organizational' or 'managerial' focus (Culnan, 1987; Vessey *et al.*, 2002). The same, however, cannot be said for IS security.

Our first paper, by Herath and Rao, focuses on the issue of end users' compliance with information security policies. More specifically, they advance and test an integrated model that draws on General Deterrence Theory, Protection Motivation Theory, Organizational Commitment, and the Decomposed Theory of Planned Behavior. With 312 employee survey responses from 78 organizations, the study explores the intention to comply with information security policies. As one of the few empirical studies in this area, the research advances key implications for future academic studies and IS security practitioners.

In a similar vein, Myyry, Siponen, Pahnila, Vartiainen, and Vance also examine compliance, but rather than focus on intention, they address how theories of moral reasoning may provide some insight into the causes of non-compliance. A theoretical model that explains non-compliance based on moral reasoning and values is, therefore, proposed. Based on the Theory of Cognitive Moral Development by Kohlberg and the Theory of Motivational Types by Schwartz, the subsequent integrated model is largely supported by the authors' empirical findings.

Carol Hsu examines how members of a financial organization interpret the implementation of a security certification process, namely BS7799 Part 2. Using an interpretive case study methodology, Hsu draws on the concept of frame analysis to identify the disparate group interpretations held by managers, the certification team, and other employees. Through this interpretation, each group assigns different meanings to the certification process that impacts decisions concerning the related security practices. Hsu, therefore, argues that managers must first identify frame incongruence, and then intervene to ensure alignment and achieve overall security effectiveness.

Boss, Kirsch, Angermeier, Shingler, and Boss develop a model to explain employees' information security precaution-taking behavior. Their findings, based on an extensive survey, suggest that when individuals perceive security policies to be mandatory, they will be more motivated to take security precautions. And if they believe that the firm's management is reviewing their actions, they will be more likely to be in compliance. They also noted that both apathy and computer self-efficacy are important determinants of information security behaviors. Individual employees may be apathetic about compliance with security policies, but communications from managers may change their perspective. Furthermore, their interesting study suggests that the role of rewards as an incentive for employee action may not work in the security context as it does in other domains.

In our next paper, we present an interesting project that relates to the use of passwords for security authentication. Zhang, Luo, Akkaladevi, and Ziegelmayer address the problem of recalling multiple passwords from an empirical cognitive perspective. In this study, the authors recognize that users often jeopardize password secrecy in order to improve memorability. The more passwords that users possess, the harder the recall process becomes. The manuscript investigates the use of interference alleviation methods to improve multiple password recall, and suggests that a list reduction method may improve the individual cognitive process of recall.

In our final paper, Lee and Larson investigate organizational adoption of anti-malware software by small- and medium-sized business (SMB) executives. Applying Protection Motivation Theory, the authors surveyed SMB executives, and demonstrated that threat and coping appraisal successfully predicted their anti-malware software adoption intention, which led to adoption by their organization. They also determined that social influence and budgetary issues played a role in the adoption decision. Finally, vendor support was a key facilitator of anti-malware adoption, especially in IT-intensive industries.

So various factors, motivators, inhibitors, and causes of policy compliance and computer crime are addressed in these papers. These factors might be characterized as (1) those that relate to beliefs and intentions regarding security and policy compliance that actors bring with them (which may include ethics and moral reasoning) as addressed by Herath and Rao and by Myyry, Siponen, Pahnila, Vartiainen, and Vance; (2) those that address comprehension and perception properties, including cognitive processes as addressed by the Hsu paper and the Zhang, Luo, Akkaladevi, and Ziegelmayer paper; and (3) those that focus on motivational influences (or lack thereof), including the apathy, fear, and confidence characteristics, plus the threat-coping behaviors that are covered in the Boss, Kirsch, Angermeier, Shingler, and Boss paper and the Lee and Larson paper. Collectively, this excellent set of manuscripts provide an illuminating perspective on this important research domain.

We wish to thank the many reviewers who ensured a rigorous selection process and who also helped us identify opportunities to develop each manuscript through the three stages of revision. The resulting projects were significantly improved by this process. We are also indebted to Richard Baskerville for his leadership and to the staff of *EJIS* for their support throughout this process.

About the authors

Merrill Warkentin is a professor of MIS and FoB Notable Scholar in the College of Business at Mississippi State University. He holds BA, MA, and Ph.D. degrees from the University of Nebraska-Lincoln. His research, primarily in computer security management, eCommerce, and virtual teams (CMC), has appeared in such journals as *MIS Quarterly*, *Decision Sciences*, *Decision Support Systems*, *Communications of the ACM*, *Communications of the AIS*, *The DATABASE for Advances in Information Systems*, *Information Systems Journal*, *Information Resources Management Journal*, *Journal of Organizational and End User Computing*, *Journal of Global Information Management*, *Information Systems Management*, and others. Professor Warkentin is the author or editor of six books. He is serving or has served as AE for several journals, including *MIS Quarterly*, *Information Resources Management Journal*, and *The Journal of Information Systems Security*. He has held leadership positions for several international conferences, including Program Co-Chair for the IFIP TC8 International Workshop on Information Systems Security

Research, WISE2007, and WISP2009. Dr. Warkentin has advised numerous companies and organizations, has served as National Distinguished Lecturer for the Association for Computing Machinery (ACM), and has been a featured speaker at over 100 industry association meetings, executive development seminars, and academic conferences.

Robert Willison is an assistant professor in the Department of Informatics, Copenhagen Business School. He received his Ph.D. in IS from the London School of Economics and Political Science. His research focuses on IS security, with a specific interest in employee computer crime. He has published in journals including *Information and Organisation*, *European Journal of Information Systems*, and *Communications of the ACM*. He is an AE for the *European Journal of Information Systems* and is currently acting as Co-Programme Chair for the IFIP TC8 International Workshop on Information Systems Security Research.

References

CULNAN M. (1987) Mapping the intellectual structure of MIS, 1980–1985: a co-citation analysis. *MIS Quarterly* **11(3),** 341–353.

ERNST and YOUNG (2008) Moving beyond compliance: Ernst & Young's 2008 global information security survey. [WWW document] http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf (accessed 1 April 2009).

FARHOOMAND A.F. (1987) Scientific progress of management information systems. *The DATA BASE for Advances in Information Systems* **18(4),** 48–56.

FARHOOMAND A.F. and DRURY D.H. (1999) A historiographical examination of information systems. *Communications of the AIS* **1,** 1–27.

FORCHT K. (1994) *Computer Security Management*. Danvers: Boyd and Fraser.

IM G. and BASKERVILLE R. (2005) A longitudinal study of information systems threat categories: the enduring problem of human error. *The DATA BASE for Advances in Information Systems* **36(4),** 68–79.

LOCH K.D., CARR H.H. and WARKENTIN M.E. (1992) Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly* **16(2),** 173–186.

PARKER D. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley Computer Publishing, New York.

SIPONEN M., WILLISON R. and BASKERVILLE R. (2008) Power and practice in information systems security research. In *Proceedings of the International Conference on Information Systems* Paris, France, 14–17 December 2008.

STANTON J.M., STAM K.R., MASTRANGELO P. and JOLTON J. (2005) Analysis of end user security behaviors. *Computers & Security* **24(2),** 124–133.

STRAUB D. and WELKE R. (1998) Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* **22(4),** 441–469.

VESSEY I., RAMESH V. and GLASS R.L. (2002) Research in information systems: an empirical study of diversity in the discipline and its journals. *Journal of Management Information Systems* **19(2),** 129–174.

WARKENTIN M.E. (1995) Information system security and privacy. In *Emerging Information Technologies, Advances in Telematics* HANSON J, Ed), Volume 2, pp. 57–77, Ablex Publishing, Norwood, NJ.

WARKENTIN M. and JOHNSTON A.C. (2008) IT governance and organizational development for security management. In *Information Security Policies and Practices* STRAUB D, GOODMAN S and BASKERVILLE RL, Eds), pp. 46–68, M.E. Sharpe, Armonk, NY.

WARKENTIN M., DAVIS K. and BEKKERING E. (2004) Introducing the check-off password system (COPS): an advancement in user authentication methods and information security. *Journal of Organizational and End User Computing* **16(3),** 41–58.

WILLISON R. (2006) Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization* **16(4),** 304–324.

WILLISON R. (2009) Motivations for employee computer crime: understanding and addressing workplace disgruntlement through the application of organisational justice. Working Paper No.1, Copenhagen Business School, Department of Informatics.

WILLISON R. and BACKHOUSE J. (2006) Opportunities for computer abuse: considering systems risk from the offender's perspective. *European Journal of Information Systems* **15(4),** 403–414.