INDIAN INSTITUTE OF MANAGEMENT KOZHIKODE

Working Paper

IIMK/WPS/225/ITS/2018/01

February 2018

Understanding the Human, Managerial and Organizational Aspects of Information Security Management: A Literature Review

Anupriya Khan [1]
M P Sebastian [2]

[1]Research Scholar, Indian Institute of Management Kozhikode, Kerala, 673570, India, E-mail: anupriya09fpm@iimk.ac.in

[2] Professor, Indian Institute of Management Kozhikode, Kerala, 673570, India., E-mail: sebasmp@iimk.ac.in,

Abstract

This study on human, managerial and organizational aspects of information security management has three parts. First, it identifies the articles that focus on effective management of information security, employee attitude-intention-behavior, and information security policy compliance. The second part identifies the theoretical frameworks commonly used in IS security research. The third part is about analyzing and synthesizing the identified literature. This study summarizes the theories used in IS security management research with non-technical considerations. The theoretical frameworks used in IS security literature generally show a tendency towards explaining the driving factors towards information security compliance and most of them perceive employees to be the key threats to information security. The study shows that noncompliance behavior is associated with the human factors which cannot be reduced if effective management is not in place.

Keywords

Behavior, effective management, information system security, policy compliance, theory framework.

1. Introduction

Within the modern business climate, organizations confront with dramatic challenges with regard to threats to corporate data, information technology infrastructure, and personal computing. Several findings suggest that the disparity between increasing threats and organizations' responses is growing at an alarming rate (Ernst & Young, 2012). State of the art and complex technological solutions cannot ensure the effective information security transformation. It is interesting to note that most IS security research in the past were technical in nature with limited attention to the human and organizational factors. Dhillon and Torkzadeh (2006) suggest that it is essential to go beyond technical considerations and analyze the principles and values that are grounded in organizational practices, in order to maintain information systems (IS) security in organizations. Their value-focused assessment of IS security in organizations result in several fundamental objectives to maximize IS security such as enhancing management development practices, providing adequate human resource management practices, increasing trust, providing open communication, maximizing awareness, establishing ownership of information, promoting responsibility and accountability, improving authority structures, understanding personal beliefs, and understanding individual characteristics. Similar recommendations are recently provided by many other scholars who stress on analyzing IS security issues from the managerial perspective (Ernst & Young, 2012; Singh, Picot, Kranz, Gupta, & Ojha, 2013; Siponen, Mahmood, & Pahnila, 2014). Guided by these suggestions, this paper reviews the extant literature considering the role of management, the human aspects (human error, employee attitude, intention, and behavior), and the challenges of effective implementation of information security policies.

By synthesizing relevant literature on IS security, this paper aims to provide an understanding why is it important to recognize the human and organizational aspects, and the role of management toward quality information security. This study also lists the underlying theories that are frequently used to analyze IS security phenomenon from a non-technical point of view. Most of these studies (e.g., Guo, Yuan, Archer, & Connelly, 2011; Herath & Rao, 2009) perceive employee non-adherence to information security policies as a major problem for organizations and thus investigate the underlying factors that drive employee non-compliance behavior.

2. Research Methodology

This paper follows a systematic review of the relevant literature that deal with non-technical aspects of IS security management. The study has three parts. First, it identifies the articles that focus on effective management of information security, employee attitude-intention-behavior, and the information security policy compliance. The second part identifies the theoretical frameworks commonly used in IS security research. The third part is about analyzing and synthesizing the identified literature. The databases used for researching the articles include Business source complete, EBSCOhost and Google scholar (search engine). However, not all the articles are included as part of this study. The articles that are of quality and relevance are considered. Most of the non-academic articles (white papers and industry magazine articles), books and conference papers are excluded due to lack of methodological rigor.

3. Analysis of the Results

The extant literature on IS security management integrates a vast amount of studies that approach IS security from different aspects. This paper attempts to cover the major non-technical aspects of IS security management by analyzing the IS security literature with respect to the following three themes: information security from the managerial perspective, human aspects of information security management, and IS security policy compliance: the role of policy awareness and training. This section summarizes the theories used in IS security management studies with non-technical considerations.

3.1. Information security from the managerial perspective

The need of considering a managerial perspective in organizations while addressing information security issues and implementing relevant solutions is realized and given substantial amount of significance in several studies. The central argument posed by these articles is that the technological solution to an information security issue is not the ultimate solution because of the possibility of a gap between recommending a solution and implementing it. The successful implementation of any solution is contingent on the broader organizational strategies as well as the mindset of the management and the employees. Thus it becomes critical to analyze how the management deals with challenges posed by IS security.

It is evident that IS security is one of the major dimensions of the business affairs and falls into the management territory. A major challenge is to balance information security and business needs (Kayworth & Whitten, 2010). Therefore, the management including the top

management of an organization has a core responsibility towards developing and implementing an effective IS security policy (Chang & Ho, 2006). Effective information security transformation requires leadership and the commitment (Ernst & Young, 2012). Managers are expected to be fully aware of the total range of controls available so that they can select appropriate control based on the situation to minimize risks. Unfortunately, their ignorance often leads to their inability to cope with systems risk, and consequently, their action becomes less effective (Straub & Welke, 1998). So, the role of management is very crucial in IS security management as their action toward IS security is associated with the overall business demands and outcomes.

The literature has recognized top management support to have strong influence on the effective implementation of the security policy (Knapp et al., 2006; Ma, Schmidt, Herberger, & Pearson, 2009). The key factors that lead to IS security effectiveness include IS security governance program, policy, a review system and change management to address new challenges (Ezingeard & Bowen-Schrire, 2007). Without top management support all these activities may not be complete and of quality (Johnston & Hale, 2009). For example, in the study by Ernst and Young (2012), lack of top management support, ineffective leadership, lack of skilled personnel and budgetary constraints were reported to be the key hindrances to IS security effectiveness. Effective management must address these critical issues.

Apart from top management support, there exist a number of factors such as organization structure, culture, size, industry type, IT competence, environmental uncertainty, and the legal requirements that shape the implementation of IS security management (Chang & Ho, 2006; Ma et al., 2009). Organizational structure that facilitates open and efficient communication (Straub & Welke, 1998), reporting (incident reporting), and specifies the responsibility, accountability and authority is desired for better management of IS security (Ma et al., 2009). A formal organizational structure can be effective to facilitate strategic alignment between business and security objectives (Kayworth & Whitten, 2010). Even a decentralized structure supporting decision making at all levels within organizations can ensure a secure IS architecture (Pulkkinen, Naumenko, & Luostarinen, 2007).

As indicated earlier, there are at least three factors--technical, human, and organizational, that are directly linked with the effectiveness of IS security management (Werlinger, Hawkey, & Beznosov, 2009). The technical factors include the acquisition of required technologies including hardware and software, and the allocation of budgets. The human components consist of hiring, training, educating, and motivating employees so that they can assess the IS security threats, mitigate them and comply with the policies. The organizational factors deal with designing and implementing information security policy and best practices (Chang & Lin, 2007). Balancing these three factors is essential for effective IS security management.

3.2. Information security policy compliance: The role of policy awareness and training

The IS security research has identified various managerial practices that are effective in IS security management. Most studies have stressed on IS security policy development, awareness, training, and compliance. Information security policy, if effectively implemented, plays an essential role in securing the relevant data in organizations (Chang & Lin, 2007; Doherty, Anastasakis, & Fulford, 2009; Singh et al., 2013). Unfortunately, employee

noncompliance with IS security policies is a growing concern for organizations (Puhakainen & Siponen, 2010).

In many cases, employees have access to the most critical data and hence their violation of access policy is a major internal threat to the information security management (Rubenstein & Francis, 2008). Mere existence of an information security policy may not be efficacious unless employees adhere to it in practice. This is naturally possible once the employees are aware of the policy and properly trained for compliance. The information security policy awareness brings employees' attention to the need for safeguarding the relevant information assets from malicious attacks and various vulnerabilities, and the training helps them to act on it. The training helps employees avoid violating the access policies. The policy compliance thus relies on two the aspects: (i) the awareness, which is a considerably beneficial measure (Hagen, Albrechtsen, & Hovden, 2008), and (ii) training, which shapes employees' behavior (Albrechtsen & Hovden, 2010) towards policy compliance. The extant IS security research has thus suggested the need for a comprehensive policy, an awareness and training program (Hagen, Albrechtsen, & Hovden, 2008; Ma et al., 2009; Puhakainen & Siponen, 2010; Siponen, Mahmood, & Pahnila, 2014; Whitman, 2004) and security control mechanisms for IS security management. High-level managers must make employees aware, warn them of information security noncompliance, and describe why it is necessary to carry out these policies (Siponen, Mahmood, & Pahnila, 2014). In many cases, employees are not certain about their accountability though the information security policy outlines it. Hence, the accountability for information security must be explicitely stated and shared by all employees (von Solms & von Solms, 2004). The mmanagement is again responsible for these processes.

3.3. The human aspects of information security management

Human beings are one of the most critical threats in information security management in organizations. Trček, Trobec, Pavešić, and Tasič (2007) contend that human factor is of utmost importance and the interaction between of human and technical factor impacts IS security. An employee who involves in data security breach does so (i) intentionally or (ii) unintentionally.

In the first case, an insider can violate the security policy and access the organizational data with a malicious intention that results in "fraud, unauthorized disclosure, theft of intellectual property, and other abuses" (Vance, Lowry, & Eggett, 2013). Employees therefore are viewed as a major cause of most of the data breaches and information security vulnerabilities (Yeniman et al., 2011; Jaeger, 2013). Hence, it is required to look into the human aspects for effectively managing and reducing the potential threats from employees. Studies have found that employees involve in data breach possibly due to their ignorance, lack of awareness, lack of training, unauthorized access, lack of compliance, wicked intention and ineffective managerial control (Rubenstein & Francis, 2008; Vance, Lowry, & Eggett, 2013). The second case is based on human error, i.e., "non-deliberate accidental cause of poor computer and information security" by humans (Kraemer & Carayon, 2007). An example of human error could be an accidental mistake in programming that makes the computer to crash. Kraemer and Carayon (2007) found that organizational factors such as communication, security culture, and policy lead to human errors in the context of information security.

Acknowledging the importance of human factors in IS security context, a significant amount of studies investigate employees' intention to comply with information security policy (e.g., Vance, Lowry, & Eggett, 2013; Johnston & Warkentin, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Siponen & Vance, 2010; Straub & Nance, 1990; D'Arcy et al., 2009; Herath & Rao, 2009; Myyry et al., 2009). Siponen, Mahmood, and Pahnila (2014) demonstrates the perceived severity and perceived vulnerability to potential information security threats, employees' belief as to whether they can adhere to information security policies, their attitude toward complying with information security policies, and social norms to have a significant and positive effect on the employees' intention to comply with information security policies. On a similar note, Guo et al. (2011) suggests that utilitarian outcomes (relative advantage for job performance, perceived security risk), normative outcomes (workgroup norms), and self-identity outcomes (perceived identity match) are key determinants of end user intentions to engage in nonmalicious security violation. The factors that explain employee non-compliance behavior can be addressed if effective information security management is in place. As discussed in the previous section, the management must make employees aware of the situations, train them and communicate with them openly without leaving any scope for confusion to curb the access policy violations and security breaches.

Human resource management, being a part of the business management, plays a significant role in controlling and diverting employee behavior towards the security of information. An organization deals with various activities of human resources that include planning, hiring, training, monitoring, motivating, controlling and diverting human activities to ensure information security. All these activities, especially security policy awareness, training and interventions significantly influence employee intention to comply the policy and behavior indicators (Puhakainen & Siponen, 2010; Albrechtsen & Hovden, 2010). Henceforth, the role of human factor, i.e., employees are necessary and should not be neglected at any stage while exercising the risk analysis, and designing and implementing the information security policy (Werlinger, Hawkey, & Beznosov, 2009).

3.4. Theoretical framework

Table 1 summarizes the underlying theoretical concepts that are used in IS security literature. A close observation reveals that most studies focus on the intersection of human and organization factors, and finds the organizational as well as individual factors that are responsible for employees' ill intention and noncompliance behavior in the IS security context.

Author(s), Year	Underlying Theory	Description
Chang & Lin, 2007	Organizational culture	Based on various characteristics of organizational culture including cooperativeness, innovativeness, consistency and effectiveness, this paper evaluates the CIA (Confidentiality, Integrity, Accountability) principles of IS management.

Albrechtsen & Hovden, 2010	Cultural theory	The paper classifies the stakeholders' perceptions of security risks in the context of risk management using cultural theory.
Albrechtsen & Hovden, 2010	Theoretical model of the intervention	The theoretical model of the intervention shows that the intervention is expected to improve information security awareness and behavior among the intervention participants. The model emphasizes on employee participation, collective reflection, group-work and knowledge sharing at the organizational level.
Siponen, 2000a	Intrinsic Motivation, Emotivism	The article presents a framework for persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions.
Siponen, 2000b	Theory of Justice	The proposed model identifies ethical education as to improve employees' IS security behavior. Ethical principles are used to justify claim that certain IS security acts are morally favored.
Straub and Welke, 1998	Deterrence Theory; behaviorism	The findings emphasizes that IS security awareness training improves employees' compliance with security policies. The IS security training is conducted primarily to communicate severity and certainty of sanctions to the employees and review IS security policies.
Puhakainen & Siponen, 2010	Elaboration Likelihood Model (ELM); Universal Constructive Instructional Theory (UCIT)	ELM helps practitioners to understand how and why training is expected to work. Using ELM and UCIT, the paper proposes a training program and validates it through an action research project.
Siponen, Mahmood, & Pahnila, 2014	Protection Motivation Theory, the Theory of Reasoned Action, the Cognitive Evaluation Theory	The article provides a new multi-theory based model to explain employees' adherence to security policies.
Vance, Lowry, & Eggett, 2013	The theory of accountability	The paper presents a new approach for reducing access policy violations; identify four system mechanisms that heighten an individual's perception of accountability: identifiability, awareness of logging, awareness of audit, and electronic presence.
Backhouse, Hsu & Silva, 2006	Clegg's circuits of power framework	Attempts to understand the development of the first standard in information security management.
Smith et al., 2010	Clegg's circuits of power framework	Investigates IS security within government by analyzing power relationships during an IS security standards adoption and accreditation process.
Johnston & Warkentin, 2010	Protection motivation theory	Investigates the influence of fear appeals on the compliance of end users and recommends that specific individual computer security actions be enacted toward the mitigation of threats.

Bulgurcu, Cavusoglu, & Benbasat, 2010	The theory of planned behavior	Identifies the antecedents of employee compliance with the information security policy (ISP) of an organization and shows that employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply with. Also, outcome beliefs are reported to significantly affect beliefs about overall assessment of consequences and they, in turn, significantly affect an employee's attitude. Information security awareness positively affects both attitude and outcome beliefs.
Siponen & Vance, 2010	Neutralization theory	The paper understands employees' failure to comply with IS security policies and offers new insights into how employees' rationalize this behavior.
Straub & Nance, 1990	Deterrence theory	Suggests that detection and punishment of violators minimize computer abuse.
Kankanhalli et al., 2003	Deterrence theory	Analyzes whether the use of sanctions leads to enhanced IS security effectiveness and finds that deterrents, as measured in man-hours spent in security efforts, leads to better IS security effectiveness.
D'Arcy et al., 2009	Deterrence theory	Finds that IS security policies, awareness programs, and computer monitoring influence the perceived severity of formal sanctions, which leads to reduced intention to misuse IS.
Spears & Barki, 2010	User participation theories (from the systems development literature)	Indicates that user participation contributes to improved security control performance through greater awareness, greater alignment between IS security risk management and the business environment, and improved control development. While users are often considered as the weak link in IS security literature, the article suggests that users, if provided with required business knowledge, may be an important resource to IS security and contribute to more effective security measures.
Hsu, Shih, Hung, & Lowry, 2015	Social control theory	Social control can encourage both in- and extra-role security behaviors that in turn contribute to information security policy effectiveness.
Hsu, Lee, & Straub, 2012	Institutional theory, economic-based factors	Institutional factors influence the adoption and assimilation of ISM. Economics-based factors such as perceived environmental uncertainty, resource availability, competitive advantage moderate the institutional conformity pressure on information security adoption while organization capability such as top management support, IT capability, cultural acceptability influence the institutional confirmation of information security assimilation.
Herath, et al., 2014	Technology Acceptance Model, Technology threat avoidance theory	An email authentication service is designed to cope with email threats. The study shows that user intention to adopt an email security service is determined by users' perception of risk and evaluation of both internal and external coping strategies.

Lowry, Posey, Bennett, & Roberts, 2015	Fairness theory, Reactance theory, Deterrence theory	The paper shows that organizational trust can decrease reactive computer abuse, and organizational security education, training and awareness (SETA) initiatives decrease the perceptions of external control and freedom restrictions, thereby increasing organizational trust.
Herath & Rao, 2009	IS adoption theories, Protection motivation theory, Deterrence theory, and Organizational behavior	Studies the driving factors toward IS security compliance.
Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009	Theory of cognitive moral development, Theory of motivational types of values	Explains noncompliance with information security policies in terms of moral reasoning and values.
Guo, Yuan, Archer, & Connelly, 2011	The composite behavior model (extension of theory of reasoned action and theory of planned behavior)	The results suggest that utilitarian outcomes (relative advantage for job performance, perceived security risk), normative outcomes (workgroup norms), and self-identity outcomes (perceived identity match) are key determinants of end user intentions to engage in non-malicious security violation.
Liang & Xue, 2009	Technology threat avoidance theory	The theory is used to describe the threat avoidance behavior. Users are motivated to avoid malicious IT when they perceive a threat and believe that the threat is avoidable by taking safeguarding measures; if users believe that the threat cannot be fully avoided by taking safeguarding measures, they would engage in emotion-focused coping.

Table 1: Underlying theories in IS security research

4. Conclusion

The review of the extant literature on IS security management shows the important of considering managerial perspective while analyzing effectiveness of information security. As opposed to the view in which IT professionals were held responsible for IS security, a number of scholars now believe that management has core responsibility towards IS security. The literature discusses various managerial practices but mostly stress on IS security policy development and implementation. Amongst different IS security policy compliance approaches, awareness and training are considered to be the most effective. The theoretical frameworks that are mostly used in IS security literature show a tendency towards explaining the driving factors towards information security compliance. Apparently, most of them perceive employees to be the key threats to information security and hence bring forth different factors to enable organizations to make their employees adhere to the information security policies. It is also evident from the review that the three themes are interlinked, which suggests that noncompliance behavior (theme 2) is associated with the human factors

(theme 3) and cannot be reduced if effective management (theme 1) is not in place. In essence, the study advises the organizations to pay more attention to the insider threats and work toward bringing effective management including quality leadership and commitment. A limitation of this research is that publications in languages other than English could not be included.

References

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432–445.

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

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 79-98.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 293–314.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449–457.

Ernst, & Young. (2012). *Fighting to close the gap.* Retrieved from http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf

Ezingeard, J.-N., & Bowen-Schrire, M. (2007). Triggers of Change in Information Security Management Practices. *Journal of General Management, 32*(4), 53-72.

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

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 106–125.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Info Systems Journal*, 61–84.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. *Information Systems Research, 23*(3), 918–939.

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

Jaeger, J. (2013, February 5). Human Error, Not Hackers Cause Most Data Breaches. *Compliance Week*.

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-129.

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

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 139-154.

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive, 9*(3), 163-175.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2006). The Top Information Security Issues Facing Organizations: What Can Government do to Help? *Information Systems Security, 15*(4), 51-58.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics*, 143-154.

Liang, H., & Xue, Y. (2009, March). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), 71-90.

Lowry, P. B., Posey, C., Bennett, R. (., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, 193-230.

Ma, Q., Schmidt, M. B., Herberger, G., & Pearson, J. M. (2009). An integrated framework for information security management. *Review of Business, 30*(1), 58-69.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 126–139.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757-778.

Pulkkinena, M., Naumenkoa, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool. *Journal of Systems and Software, 80*(10), 1607-1620.

Rubenstein, S., & Francis, T. (2008). Are your medical records at risk? *Wall Street Journal—Eastern Edition*, D1-D2.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, 225-239.

Siponen, M. (2000a). A Conceptual Foundation for Organizational IS Security Awareness. *Information Management & Computer Security*, 31-41.

Siponen, M. (2000b). On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non Descriptive Foundations, in Information Security for Global Information Infrastructures (Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on IS Security, S. Qing and J. H. P. Eloff (eds.), Boston: Kluwer Academic Publishers, 401-410.

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

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503-522.

Straub, D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly* , 45-62.

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

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology* , 113-118.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems, 29*(4), 263-290.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*(1), 43–57.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 360–365.

Research Office

Indian Institute of Management Kozhikode

IIMK Campus P. O.,

Kozhikode, Kerala, India,

PIN - 673 570

Phone: **+91-495-2809238**

Email: research@iimk.ac.in

Web: https://iimk.ac.in/faculty/publicationmenu.php