Towards Modelling the Impact of Security Policy on Compliance

Winfred Yaokumah, Department of Information Technology, Pentecost University College, Accra, Ghana
Steven Brown, School of Business and Technology, Capella University, Minneapolis, MN, USA
Alex Ansah Dawson, School of Technology, Ghana Institute of Management and Public Administration, Accra, Ghana

ABSTRACT

This study develops a model, based on the controls present in ISO/IEC 27002 framework, to integrate the role of technical and administrative security controls. The model provides better understanding of how security policy can influence security compliance and the pathway through which this effect is generated. Data were collected from 223 IT security and management professionals. Using Partial Least Square Structural Equation Modelling (PLS-SEM) and testing hypotheses, the study finds that information security policy has significant indirect influence on information security compliance. The effect of security policy is fully mediated by security roles and responsibilities, operations security activities, and security monitoring and review activities. Security policy strongly influences operations security activities and has the greatest effect on security roles and responsibilities. Among the three mediating variables, monitoring and reviews has the most significant influence on security compliance. Conversely, the impact of security policy on compliance is not significant.

KEYWORDS


INTRODUCTION

Various threats (potential dangers exploiting system vulnerabilities) are militating against information assets as a result of vulnerabilities in information systems. Vulnerabilities are weaknesses or lack of countermeasures in the information systems themselves (Shon, 2013). Threats may be intentional or unintentional and can come from both internal and external sources. Internal (insider) threats to information security are critical issues for organizations (Baracaldo & Joshi, 2013; Wang, Gupta, & Rao, 2015). A global survey profiles the nature of data breaches in 19 organizations from 27 countries. The study covers more than 47,000 reported security incidents and 621 confirmed data breaches. The findings reveal that over 50% of the insiders who committed sabotage were formal employees, 70% of Internet Protocol address (IP) theft cases were committed by internal people intended to resign their job, and 75% of attacks were opportunists with financial motives targeting no specific individual or organization (Data Breach Investigations Report [DBIR], 2013). This report heightens the need for organizations to ensure that essential security controls are put in place and security policies are complied with.

Though several threats including browser exploits, data interception, malware, network exploits, spamming, spoofing, and theft/loss (US GAO, 2012) exist, technical (logical) controls are available to protect information systems. Technical controls such as firewalls, intrusion preventive and detection
systems, antimalware, encryption, backup and restoration mechanisms, logging, monitoring, auditing, identification and authentication mechanisms were implemented in software configurations, hardware devices, and in procedures to protect information systems. Apart from technical controls, administrative controls (such as security policies and procedures) and physical controls (such as cable locks, fencing, closed-circuit TV, and lighting) play a major role in security systems (Shon, 2013). These controls provide functionalities intended to secure information systems.

These functionalities comprise of deterrent (intended to discourage a potential attacker), preventive (intended to avoid an incident from occurring), corrective (fixes components or systems after an incident has occurred), recovery (intended to bring the environment back to regular operations), and detective (identify an incident’s activities and potential intruder) (Shon, 2013). Despite these security measures, the major threat is the members of the organization themselves who are entrusted to protect information systems (Willison & Warkentin, 2013) and are required to comply with the organization’s security measures and policies. A recent study found that insiders (current and former employees, third parties) with trusted network access represent a major threat to information security, yet many organizations fail to implement processes and technologies to address internal incidents (PWC Report, 2015).

To ensure compliance with security objectives, legal, and regulatory requirements, organizations have established security policies to guide employees’ behaviour. The information security policy contains intentions, principles, rules, and guidelines which the management wants the employees to adhere to (Sommestad et al., 2014). It provides management direction and support for information security ((ISO/IEC, 2009). It generally describes the acceptable use of computer resources, information security roles and responsibilities, the type of training that employees should have, and the consequences of security policy violation (Sommestad et al., 2015). Providing adequate security to information security requires that technical information systems security and management personnel comply with security measures. For instance, critical data may be put at risk when the technical personnel fail to follow operational procedures, perform vulnerability assessment, check security in the third party products and services, perform regular backups, properly manage user accounts, secure mobile devices that are attached to the organization’s productive networks, effectively control malware activities, protect data transfer and network services, monitor, log, and audit information systems regularly.

Ensuring compliance with information security policy remains a challenging task (D’Arcy & Greene, 2014). Although organizations have instituted information security policy and compliance programs (D’Arcy & Herath, 2011; Sommestad et al., 2014), concise models to fulfil the organization’s information security policy and compliance efforts are sparse. A major problem with security models is that there are just too many to follow. In just the ISO/IEC 27002:2013 framework, there are 14 major controls, which in itself a challenge for employees to comply with. Information security policy-compliance model for incorporating critical inter-related security measures is necessary for knowledge support in the management of information security in organizations where confidentiality, integrity, and availability are paramount.

Therefore, the purpose of this study is to model the impact of information security policy on compliance, focusing on information systems security and management personnel, to understand how the activities of these personnel can influence security compliance. A recent study found that malicious database administrators can bypass the security mechanisms and make hidden modifications to databases, which may be untraceable (Kieseberg et al., 2013). Previous literature on security policy compliance focused on end-users (non-technical users). For instance, D’Arcy and Herath (2011) employed deterrence theory; Hedström et al. (2013) applied social action theory (SAT) for management of information security; Sommestad et al. (2014) identified attitudes, intentions or actual behaviour having influence on compliance with information security policy. Also, Sommestad et al. (2015) found that anticipated regret and threat appraisal predict information security policy compliance.
14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:
www.igi-global.com/article/towards-modelling-the-impact-of-security-policy-on-compliance/160154?camid=4v1


Recommend this product to your librarian:
www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

Attribute Grammars and Their Applications
www.igi-global.com/chapter/attribute-grammars-their-applications/13584?camid=4v1a

Corporate Collapse and IT Governance within the Australian Airlines Industry
www.igi-global.com/article/corporate-collapse-governance-within-australian/44599?camid=4v1a

The Significance of Government's Role in Technology Standardization: Two Cases in the Wireless Communications Industry
DongBack Seo (2010). Teaching Cases Collection (pp. 63-73).
www.igi-global.com/article/significance-government-role-technology-standardization/40324?camid=4v1a
Information Resources Development in China
www.igi-global.com/chapter/information-resources-development-china/13848?camid=4v1a