Information Systems Security Policy Compliance: An Analysis of Management Employee Interpersonal Relationship and the Impact on Deterrence

Michael Warah Nsoh, Corpus Christ Army Depot, Corpus Christ, TX, USA
Kathleen Hargiss, Independent Researcher, Bradenton, FL, USA
Caroline Howard, HC Consulting, Oceanside, CA, USA

ABSTRACT

The article describes research conducted to assess and address some key security issues surrounding the use of information technology from employee behavioral standpoint. The aim of the study was to determine additional security measures to reduce security incidents and maximize effective use of information systems. The research is an extension of several recent empirical studies in information systems security policy behavioral compliance, which have generally found people to be a weak link in information security. A mix of theoretical frameworks resulted in a model based on the Theory of Planned Behavior (TPB), which was used to test the impact that management and employee relationship has on deterrence. Results indicate that management has a significant stake in influencing the behavior of their employees, and that the issue of employee disgruntlement nevertheless is not paramount of top management’s Information systems security challenges.

Keywords: Employee Disgruntlement, General Deterrence Theory, Information Systems Security Policy, Management Employee Interpersonal Relationship, Neutralization Theory, Theory of Planned Behavior

1. INTRODUCTION

Information Technology is a vital apparatus for strategic business planning and competitive advantage; it inherently has the potential to facilitate and expedite business processes at unprecedented levels. The wide adoption of information technology to conduct ordinary business activities has also been an attractive avenue for criminal ideations resulting in critical security concerns. In order to mitigate possible factors that can impede information security, private and

DOI: 10.4018/IJSITA.2015040102
public organizations are predisposed to three categories of security countermeasures including: Technologies, administrative procedures, and education, awareness and training programs (Chaundhry, Chaundhry, & Reese, 2012; Whitman & Mattord, 2009). A preponderance of articles in the research community continues to emphasize the point that, the lack of adherence or conformance to information security policies on the part of employees, either deliberately or inadvertently is of paramount concern (Ifinedo, 2012; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009). These facts have lead to the conclusion that, internal users of information systems in organizations constitute the weakest link of defense against information security. The focus of this study is on internal threats and its associated motivators and consequences using the theory of planned behavior, elaborated upon in greater detail in the following paragraphs.

The adoption of Information Technology to conduct daily business operations is a strategic effort and is susceptible to yielding competitive advantage and high returns on investment (Evans, 2011). This outcome can undoubtedly not be achieved without severe security commitments, primarily on the part of top management and secondarily on the part of users of information systems who are the primary custodians of sensitive and confidential information by virtue of their service to the organization and customers alike. Achieving a high level of employee commitment to the security of information systems requires an elevated sense of situational awareness and attention to specific security eventualities (Hu, Dinev, & Hart, 2012; Siponen, Mahmood, & Pahnila, 2009; Whitman, 2003). The focus of information security is increasingly on the role of people and compliance as people often constitute the greatest threat due to poor unintentional and intentional choices resulting from motivating factors that could infringe on their ability to make rational choices (Hu, Xu, Dinev, & Ling, 2011; Pahnila, Siponen, & Mahmood, 2007). Information Security has always been a call for concern for business organizations and their stakeholders alike because of the devastating and humiliating consequences that security incidents can pause to the Confidentiality; Integrity and Availability (CIA) of organizational information.

2. LITERATURE REVIEW

2.1. Information Systems Security Policy, Management Employee Interpersonal Relationship, and the Theory of General Deterrence

Information systems security management has been a challenging endeavor, especially from the perspective of impeding internally originated threats (Cheng, Li, Li, Holm, & Zhai, 2013; Ifinedo, 2012; Johnston & Warkentin, 2010; Whitman, 2003). Employee questionable behavior that is either deliberate or accidental has been a primary trepidation and a serious information security threat to organizational information systems leading to tremendous financial and reputational reparations in the order of millions of dollars (Herath & Rao, 2009b). Contemporary business organizations have therefore adopted behavioral Information Systems Security (ISS) governance as a mitigating mechanism for this Information Systems Security pandemic (Myyry et al., 2009; Siponen et al., 2009; Siponen & Vance, 2010). Research on information security policy compliance has in recent days significantly achieved new levels in response to the fact that, the information system technology community has come to the understanding that information security is increasingly a people issue (Herath & Rao, 2009; Ifinedo, 2012).

Information Systems from the vantage point of a business or public organization is best understood as a combination of technology, people, and management where people play a great role out of these three components. Hu, Dinev, and Hart (2012) conducted a study in information security policy using an individual behavioral model that they developed. Their model integrates the role of top management and organizational culture together with a fundamental social sciences
Related Content

A Technology-Focused Framework for Integrating Knowledge Management into Strategic Innovation Management
[www.igi-global.com/chapter/technology-focused-framework-integrating-knowledge/36704?camid=4v1a](www.igi-global.com/chapter/technology-focused-framework-integrating-knowledge/36704?camid=4v1a)

Supply Chain Risk Management: A Game Theoretic Analysis
[www.igi-global.com/chapter/supply-chain-risk-management/28704?camid=4v1a](www.igi-global.com/chapter/supply-chain-risk-management/28704?camid=4v1a)
The Pricing Strategy Guideline Framework for SaaS Vendors
www.igi-global.com/article/pricing-strategy-guideline-framework-saas/63005?camid=4v1a

Negotiation, Trust, and Experience Management in E-Supply Chains
www.igi-global.com/chapter/negotiation-trust-experience-management-supply/36693?camid=4v1a