ABSTRACT

Information security management is continuous process and effort in organizations. Today, information security management has been an integrative part of business process management. Therefore, business processes must include information security management. This study proposes a new research avenue and business practice - applying the Total Quality Management (TQM) practices in managing information security. We are focused on the human behavioral practices in TQM and attempt to examine how TQM behavioral practices influence the performance of information security management. Accordingly, we propose 12 hypotheses that address the causal relationship between TQM practices and organizational information security level.

KEYWORDS: Information Security, Total Quality Management (TQM), Soft Practice, Hard Practice

INTRODUCTION

Information security management is continuous process and effort that identifies and fixes security breaches and prevents from future security attacks. In organizations, information security management has been integrated in various business processes and decision making and thus managing business processes must include information security management to a certain degree. Managing information security in organizations is a complicated socio-technical task and must deal with human behavior and technical factors. Many IS researches have indicated that the greatest threat to information security comes from the insiders - employees who are ‘trusted agents’ inside the firewall (e.g., Stanton et al., 2005; Willison and Backhouse, 2006; Warkentin and Willison, 2009). Therefore, managing people’s information security behavior has become a major task during business process management.

First of all, the organization must have well-established security policy in place. Second, they must implement the policy enforcement so that all employees are aware of and follow the policy. With the established information security policy, the organization can apply various latest developed information technologies to protect information asset. In addition, the organization must train their employees’ information security management behavior and security policy
Total Quality Management (TQM) is a holistic management approach aiming to achieve long-term success in the competitive business context by doing continuous improvement in all areas in the business operations. TQM requires all employees to actively engage in products/services quality management to find and fix products/services defects from the beginning. TQM has been widely adopted in a variety of industrial sectors for several decades. Since information security management has been integrated in many business process management, TQM can be also applied to manage information security in organizations. This research explores how TQM can be applied in information security management. Particularly, we attempt to examine how to use various TQM practices or dimensional factors to effectively manage information security. Based on prior TQM studies and practices in industries, we are focused on the human behavioral dimension in TQM practices or soft practices and investigate why and how they can be applied in information security management. Three major contributions are expected in this study. First, we propose a new approach for managing information security in practice. Second, by integrating information security management in business process management, we can use TQM to manage the entire enterprise business processes easily and seamlessly. Third, we expect this study explores a new research avenue in information security management in the IS discipline.

LITERATURE REVIEW

Information security management is one of the most important research agendas in IS literature and industrial practices. It has been a key success factor in many industries. A significant bodies of studies have been conducted for information security management from both human behavioral and technical perspectives (e.g., Siponen 2005; Spears and Barki, 2010; Zafar et al., 2012; Ramachandran et al, 2013). Although there are many well-established industry standards and guidelines, information security management is continuous effort and process. This is because business processes are running on disparately distributed networks. Organizations are facing various challenges when they manage information security in compliance with industry standards and internal security policy (Dynes et al., 2007). For example, “quantifying risks is a complex task and the effort of doing so thoroughly is often hard to justify to management” (Dynes, 2007). There is no one-size-fit-all solution in information security management. The organization must make wise justifications on where their most valuable intangible assets are located and how much investment is needed to protect them. Therefore, in both industries and academia, there are many different security management standards, guidelines, best practices, and research findings. Each of them works well in a specific business context. However, these diverse management strategies and practices have cost much resources and efforts and it is hard to manage information security across business functional areas and organizational boundaries. On one hand, the organization must focus on their core business processes and well serve their customers. On the other hand, they have to deal with continuous and intensive security risks on their information assets. Both industries and academia need a unified information security management framework to address ongoing issues of information security that organizations are facing.

On the technical side, the IT industry has designed and developed various security management frameworks. For example, the Unified Threat Management (UTM) is a comprehensive technical security framework which addresses various network protection techniques including firewall, intrusion prevention, virtual private network, web gateway security, and message exchange security over network. On the human behavioral side, many studies
have been conducted on employee’s security policy compliance behavior, individual security management behavior, etc. (e.g., Dinev and Hu, 2007; Spears and Barki, 2010; Bulgurcu et al., 2010).

Total Quality Management (TQM) is a long-term management approach that requires all organizational employees to be actively involved in the improvements in business processes, quality of products/services, and the culture. According to the American Society for Quality (http://asq.org/learn-about-quality/total-quality-management/overview/overview.html), TQM is a strategic and systematic approach that is customer-focused, continual improvement, total employee involved, process-centered, system-integrated, fact-based decision making and effective communication. Organization is a socio-technical system in which human beings and technology mutually interact to make business processes happening. Management scientists consider that TQM has two distinguished types of practices or factor dimensions: soft (behavioral) dimension and hard (technical) dimension. Soft practices are focused on human behavioral management including management leadership, employee training, teamwork, employee reward and recognition, and customer satisfaction (Lewis et al., 2006a; Lewis et al., 2006b; Gadenne & Sharma, 2009). With regard to information security management, soft practices deal with various employees’ behavior on security policy compliance and enforcement. The outcomes of soft practices are hard to measure with quantitative approaches and they are the challenging issues for management (Samson and Terziovski, 1999). However, soft practices are critical to TQM success (Powell, 1995). This makes very sense in that business operations are human activities and people are decision makers and controllers of business processes. Hard practices include quality of technology, continuous improvement, process management, and information flow management (Lewis et al., 2006a; Gadenne and Sharma, 2009). Hard practices are necessary to enhance and support implementing soft practices in TQM (Lewis et al., 2006a; Vouzas and Psychogios, 2000). In the information security management, hard practices include various security hardware and software techniques such as firewall, antivirus software, security patches, etc.

Today, almost all business processes and decision makings are implemented and supported by information systems. Managing information security has become an integrative part of business process management. Therefore, adopting TQM in the information security management would help organizations better manage information security and reduce the costs and burdens related to information security during business process management. In addition, TQM would be a great tool that integrates information security management into regular business processes and decision making.

THEORETICAL DEVELOPMENT/MODEL

According to the literature review above, we propose several benefits from using TQM in information security management. First, TQM integrates information security management into the entire enterprise business process management and thus helps achieve higher management performance. Second, employees view information security as an integrative part of their workflows and thus their compliances of information security policy and police enforcement will be increased. Third, customers will feel more secure if the service providers have higher reputation on information security management and thus the customers’ satisfactions will be greatly improved.

This study applies the TQM soft practices in information security management. Zeitz et al. (1997) designed a survey instrument measuring TQM and supporting organizational culture. The instrument measures 13 dimensions of TQM and 10 dimensions of organizational culture.
We adapted the soft dimensions of Zeitz’s (1997) survey in our research model. These dimensions are management leadership, quality supervision, quality training, teamwork, customer orientation, communication, innovation, job challenge, organizational commitment, rewards, and trust. According to TQM philosophy, TQM practices positively influence the business outcomes and performances. Powell (1995) empirically examined some TQM dimensions and the findings suggest that “most features generally associated with TQM - such as quality training, process improvement, and benchmarking - do not generally produce advantage, but that certain tacit, behavioral, imperfectly imitable features - such as open culture, employee empowerment, and executive commitment - can produce advantage.” Accordingly, we propose the following hypotheses.

H1: Management leadership in information security is positively related to the organizational information security level.

H2: Management supervision in information security is positively related to the organizational information security level.

H3: Information security training is positively related to the organizational information security level.

H4: Teamwork in information security management is positively related to the organizational information security level.

H5: Customer orientation (e.g., care about customers) is positively related to the organizational information security level.

H6: Effective communication is positively related to the organizational information security level.

H7: Employee’s attitude to innovation is positively related to the organizational information security level.

H8: Job challenge (e.g., the more challenge, the more secure required) is positively related to the organizational information security level.

H9: Organizational commitment is positively related to the organizational information security level.

H10: Performance reward is positively related to the organizational information security level.

H11: Organizational trust is positively related to the organizational information security level.

These hypotheses will be examined in a survey–based quantitative study.

RESEARCH METHOD

A cross-sectional survey study will be conducted to test the hypotheses. Although a survey is a non-experimental research method, it is a means of gathering information about the characteristics, actions, or opinions of a large group of people (Pinsonneault and Kraemer 1993). Explanatory survey research can be used to answer the question of “why” and to test theory and associative relationship (Pinsonneault and Kraemer 1993; Neuman 2003). A cross-sectional survey provides a snapshot of the interested variables in a study at one particular
Apply TQM in Information Security Management

point in time. We believe that the cross-sectional survey method is appropriate for this study because we are interested in the current state of the impact of TQM dimensions on security management performance.

The survey questionnaire will be adapted from the existing published and validated survey instruments. The adapted instruments will be tested with reliability and validity, therefore we don’t need to reinvent wheel. We will administrate a survey on employees in companies across industrial sectors to increase the generalizability of findings from the study. We will solicit participations through various security forums, industrial associations, and/or social media sites. We will invite participants via email and web links. We will use Qualtrics.com to host our survey.

PLS modeling technique will be used to examine the measurement instrument and the structural model which addresses the hypotheses. PLS modeling has been used by a growing number of researchers from various disciplines. PLS places minimal restrictions on measurement scales, sample size, and residual distribution (Chin et al. 2003). Compared to covariance based SEM techniques, PLS is more suitable for explanatory studies that investigate new theories or new application of theories (Chin et al. 2003). We apply TQM principles in a new context, therefore choosing PLS as data analysis tool is appropriate in this study.

SUMMARY

Information security has become a critical part of modern business processes. Recent high profiles of security breach at Target, JPMorgan, and other Fortune 500 companies indicate that information security management is still unsatisfactory, even in large companies that spend significantly more on information security than their small/medium counterparts. Information security has real implications for business performance as reflected by the hefty costs those companies have to pay to control the damages after each security breach. It is critical for researchers and practitioners to find better way to manage information security so that customers can trust companies with their information. Since information security is more and more embedded in modern business processes, we believe that TQM principles can be well applied to manage the human behavioral side of information security. This is a new approach to managing information security. We proposes several hypotheses based on the TQM literature. To test the hypotheses we will conduct an empirical study using a survey instrument. This study can have implications for academia and practice alike. For academic research, we introduce TQM into the domain of information security management. This is the first study that applies TQM principles to the context of information security management. It also reminds practitioners that information security management needs to be addressed from the top management to every employee inside the organization. Leadership, communication, training, commitment, culture, and other TQM practices may all play roles in security management performance. This study will shed some lights on which of those practices can have significant impact on security management performance.

REFERENCES


Chin, W. W., Marcolin, B. L., and Newsted, P. R. (2003) “A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation
study and an electronic-mail emotion/adoption study”, Information Systems Research, 14 (2), pp. 189-217.


