Do Managers Understand Importance of Securing IT Resources?

Nadianatra Musa, Industrial Engineering Department, College of Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia

Vishv Malhotra, University of Tasmania, Hobart, Australia

Trevor Wilmshurst, University of Tasmania, Hobart, Australia

ABSTRACT

Information infrastructures and resources has become critical component of the modern business and non-business organizations. In turn this dependence makes these organizations vulnerable to any significant failure in their information infrastructures and resources. Literature is full of examples of the companies suffering major losses and even demise as a result of information infrastructure and resources failures. To mitigate this vulnerability the senior management and governance of the organizations needs to pay direct role and attention to protect their critical information infrastructures and resources. This paper provides some results of a study that was conducted recently to determine how the senior management of Malaysian business organizations view and control the information infrastructure and resources in their organizations to mitigate vulnerabilities to this critical component of their business organization.

Keywords: Component Interaction, Formal Component, Informal Component, IS/IT Security, Technical Component

INTRODUCTION

Even as businesses are becoming more dependent on the information technology and systems for conducting business, there continues to be a significant lack of appreciation related to securing these critical resources among the company boards and senior managers (Musa 2012). The machines, tools and techniques that were introduced by the industrial revolution several centuries ago are now well-integrated into the modern management practices. The senior management rightly can rely on the professional engineers and staff to ensure the continued operation of the business activities even as these machines and equipment fail, damage, or get stolen or vandalized – the regular preventative maintenance, spare capacities and other engineering practices.

DOI: 10.4018/IJVCSN.2015010105
provide the necessary dependability to support the organizations in a predictable manner. The management practices related to the information technology and systems that the companies install, however, are not yet so comprehensively understood and comprehensively ingrained into the governance culture of the organizations.

In the recent PhD work done by one of the authors in the context of Malaysian listed companies one of the findings is that there is a general view among the senior managements that the computer professionals supporting the information technology and systems for the organizations can deliver dependable security for this vital infrastructure. The views and attitudes of the Malaysian managers and company boards are not isolated and are to a varying degree common across the organizations elsewhere.

While the degraded status of the conventional, tangible resources is readily noticed through the reduced performance, lower output and regular inspections, the damage to information technology and systems infrastructure may go unnoticed even as it remains compromised. Professional staff in information technology section may guarantee good recovery of the systems after a noticed security incidence; however, they do not have the competence to repair all damages done to the business through such mishaps. This task of securing business value remains the responsibility of the board and senior management.

The question we pose here is: do the senior management of the companies adequately understand the importance of securing the value of information technology and system resources in their organizations? Or more fundamentally, do the boards and senior management adequately understand the risks that the information infrastructure in their business poses to the business? When committing funds for information infrastructures the managers construct business case and evaluate the cost-benefit trade-offs. Software engineering techniques have evolved to the standards where the systems can be built and deployed reliably. However, like any other resource that an organization uses in running its business, the information infrastructures need to be secured to ensure that they deliver value to the organization on a reliable and dependable basis. The senior management tends to delegate this responsibility to the computer professionals. Is this prudent?

Computer security has indeed become an essential topic in all credible university degrees related to the computers (Hawthorne, 2012). However, the topic of computer security has generally confined to well-known CIA-triad: Confidentiality, Integrity and Availability. In their recent textbook, Pfleeger and Pfleeger (Pfleeger 2012) have discussed a few more components of this security platform following the security standard ISO 7498-2 (ISO 1989). These are authentication and accountability (non-repudiation). Auditability has been added as a requirement following from the US Department of Defence (DoD 85) requirements. These six attributes certainly support and help in re-establishing the information resources that the businesses have after a security mishap; but, they cannot ensure that the resources would deliver the business value that the organization mandated when they developed the business case for investing in these resources. For example, the damage to the reputation of an organization that accidentally leaks financial or health details of its clients may be too serious and may jeopardize the continued viable existence of a corporation.

McIlwraith (McIlwraith 2006) reports that some 70% of information technology and systems related security incidences are the result of internal users’ actions or omissions; not necessarily of a malicious intent. The senior management that does not understand and visibly commit to secure the value of its information infrastructure is unlikely to receive reports on the vulnerabilities and threats when the line managers and staff become aware of them. Compromised information technology and system resources can cause significant direct loss to the business as a result of non-availability of the resources as well as from actions needed in recovering the resources and systems. In addition the business may incur indirect losses in the form of damaged reputation and
Related Content

Internet-Based Protest in European Policymaking: The Case of Digital Activism
[www.igi-global.com/article/internet-based-protest-european-policymaking/38969?camid=4v1a](www.igi-global.com/article/internet-based-protest-european-policymaking/38969?camid=4v1a)

Cultural Barriers to Organizational Social Media Adoption
Andrew Miller (2011). *Social Knowledge: Using Social Media to Know What You Know* (pp. 96-114).
[www.igi-global.com/chapter/cultural-barriers-organizational-social-media/50752?camid=4v1a](www.igi-global.com/chapter/cultural-barriers-organizational-social-media/50752?camid=4v1a)

Self-Production through the Banal and the Fictive: Self and the Relationship with the Screen
[www.igi-global.com/article/self-production-through-the-banal-and-the-fictive/152823?camid=4v1a](www.igi-global.com/article/self-production-through-the-banal-and-the-fictive/152823?camid=4v1a)
Gender Issues in the Diversity and Practice of Public Relations in the UAE
Case Study of P.R. Male Managers and Female P.R. Practitioners
www.igi-global.com/article/gender-issues-diversity-practice-public/55818?camid=4v1a