Chapter 60
Analyzing Human Factors for an Effective Information Security Management System

Reza Alavi
University of East London, UK

Hamid Jahankhani
University of East London, UK

Shareeful Islam
University of East London, UK

Ameer Al-Nemrat
University of East London, UK

ABSTRACT

Managing security is essential for organizations doing business in a globally networked environment and for organizations that are at the same time seeking to achieve their missions and goals. However, numerous technical advancements do not always produce a more secure environment. All kinds of human factors can deeply affect the management of security in an organizational context. Therefore, security is not solely a technical problem; rather, the authors need to understand human factors, which need adequate attention to achieve an effective information security management system practice. This paper identifies direct and indirect human factors that have impact on information security. These factors were analyzed through the study of two security incidents of the UK's financial organizations using the SWOT (Strength, Weaknesses, Opportunities, and Threats) technique. The study's results show that human factors are the main causes for these security incidents. Factors such as training, awareness, and security culture influence organizational strength and opportunity relating to information security. People's irrational behavior and errors are the main weaknesses highlighted in security incidents, which pose threats such as poor reputation and high costs.

INTRODUCTION

Managing information security is particularly critical and challenging for organizations that use information technology to support their business needs. Information Security Management Systems (ISMS) address all issues related to the establishment, evaluation, and maintenance of a secure information system (Tipton & Krause, 2008). Inadequate implementation of security causes serious impacts on organizations' productivity and reputation (Kraemer & Carayon, 2006; Islam et

DOI: 10.4018/978-1-4666-8111-8.ch060

al., 2011). According to the *Technical Report of Information Security Breaches 2012* by the UK Department for Business, Information & Skills, large organizations faced a 93% increase in cyberthreats (Cyberthreat, 2006). Even using the latest security techniques and protocols, most systems still face a lot of security breaches. Technological solutions to deal with issues that arise from information security are very similar globally, such as anti-virus, firewalls, and intrusion detection systems (Zhang et al., 2009). It is also argued that there is no universal, top-model framework to fulfill the requirements of ISMS (Shoemaker & Conklin, 2011). However, the real challenges are from the non-technical part of the problem, such as human and organizational issues, which need adequate attention to ensure an effective information security management system. Deloitte, in its 2006 global security report, argues that many security breaches are the result of human error or negligence resulting from weak operational practices (DeloitteReport, 2006). Yanyan in (Yanyan & Renzuo, 2008) also claims that the success of ISMS is entirely dependent on human factors. Therefore, security systems do not depend solely on preventing technical problems, but rather, they also depend on humans who use the systems and behave "a certain way" in the system environment.

Typically, human work within an organization falls into four categories: individual, team, management, and customer/interested party (Islam & Dong, 2008; Islam et al. 2010). Human factors within these categories can become uncontrollable forces. Because people have different perceptions of security, their reactions to IS procedures are diverse. Each individual has concerns, values, culture, skills, knowledge, attitude, and behavior of his or her own. These factors are highly subjective and extremely hard to measure and calculate in the design process of an ISMS. These human forces interact with technological elements in an interconnected world of so-called "secure information systems" (Herzog, 2010). People have their own unique culture, attitude, skills, knowledge, understandings, behavior, and interests that depend on the role that he or she plays within the organization. Individual interaction with computers and decisions made in regard to information security is certainly a very dynamic and complex issue. Human factors cause the greatest single issue of concern in ISMS (Jahankhani et al., 2009). Therefore, we need a comprehensive understanding of human factors and their impact on the effective implementation of information security management systems. This task is challenging, as the domain is highly subjective by nature and it is difficult to quantify all the factors into a measuring scale. There are many areas in which judgment becomes extremely difficult and hugely subjective because the study is about people and people's reactions to IS and therefore is highly personal. For instance, it would be extremely difficult to judge and evaluate people's apathy and their attitudes towards ISMS.

This paper identifies and analyzes the human factors involved in effective information security management system practice from an organizational perspective. We categorized the factors as direct and indirect. The direct factors are greatly dependent upon an individual's perception, behavior, and knowledge of IS. But the indirect factors have impact on an individual's understanding, predominantly by forces beyond people's power, such as organizational culture and policies. The identified factors have been analyzed using two real security incidents in UK financial organizations. We used the SWOT (Strength, Weaknesses, Opportunities, and Threats) analysis tool for this purpose. Our observation is that technology is not responsible for these security incidents; humans are mainly responsible for both incidents. We found certain elements that were involved in these incidents, such as errors, inadequate awareness of programmers, and lack of communication between senior management and employees. We conclude that individual security awareness, communication with the security team, and adequate and sufficient budget planning are essential besides