Applying a Security Management Mechanism to a System Development Lifecycle

Chia-ping Yu, Department of Information Management, Tamkang University, New Taipei, Taiwan
Chih-Ping Chu, Graduate Institute of Management Sciences, Tamkang University, New Taipei, Taiwan
Pin-Hui Lu, Department of Information Management, Tamkang University, New Taipei, Taiwan

ABSTRACT

This article uses qualitative research and grounded theories, to explore information security issues in the development of information systems. Its findings are: first, three security issues are identified: security plans, resources, and a security policy to implement information security mechanisms. Second, there are strong connections between security plans, resources and security policy. Third, managers implement several critical security issues across stages of system development life cycle. This article identifies the opportunities and challenges facing security management issues. Clear security policies or plans can guide software practitioners in an organization to focus on security issues, and keep controlling threats thereafter. In order to improve the quality of security management and to identify possible threats over a longer term, organizations have to monitor and manage their application service providers and security techniques.

KEYWORDS

Case Study, Grounded Theory, Information Security, System Development Lifecycle

1. INTRODUCTION

With the continuous evolution of information systems, organizations depend on them more than ever before, and the risks to information security are gradually increased. Keen (2001), and Dhillon and Backhouse (2000) suggested information security events may do serious damage to trust relationships between organizations and users in organizations which are highly dependent on information systems. Loch, Carr, and Warkentin (1992) also pointed out that information security events result not only in money losses but also have a severe impact on the competitiveness of an organization. There are a large number of issues regarding the reliability, security and standardization of information especially after the information systems are networked, facing higher risks of threats to the information system and even resulting in international conflict (Seyal, 2011). For example, the SWIFT banking system was hacked and many national central banks suffered great losses in February 2016. In April 2016, German nuclear power plants were forced to shut down because of a malicious program. WannaCryptor, a ransomware, spread all over the world in May 2017. These information security incidents usually have a negative impact on the competitive power of the organizations affected. As a result, information security is important for every industry without exception. Meanwhile, each unit of a company should re-examine the security of its own information system.

DOI: 10.4018/IJEA.2018010101

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Information is a business asset with significant value for corporations, something that must be protected properly from being attacked so as to minimize possible losses and maintain the corporation’s ongoing operations (Hall & Chapman, 2002; Schweizerische, 2013; Siponen & Willison, 2009). With the ever-changing development of technology, issues of threats and the protection of information security is also a challenge for corporations nowadays (Webb, Ahmad, Maynard, & Shanks, 2014). In general, the basic goals that information security should reach are to defend the Confidentiality, Integrity and Availability of data storage in an information system. This is the so-called “C.I.A” of information security (Schweizerische, 2013). Although digitalization means that data can be easily transmitted and accessed, yet it also makes it vulnerable to systemic risks. Systemic risks mean that computer assets such as software, hardware, data, and services are modified, destroyed, stolen or made unavailable (Straub & Welke, 1998). Meanwhile, risks and threats also bring about practical and potential losses financially, legally and prestigiously for companies (Culnan, Foxman, & Ray, 2008). Therefore, the security of information systems involves protecting the inner data of the information system so as to increase confidentiality. In addition to preventing intrusions, security can ensure the integrity of an information system and assure its availability under the premise of safety and efficacy.

Since there is now considerable compliance with information security management standards, introducing and authenticating compliance with them has become a common and convenient way to ensure information security for industries. Currently the information security management standards industries in frequent use include ISO 27001 (International Organization for Standardization 27001), COBIT (Control Objectives for Information and related Technology), TCSEC (Trusted Computer Systems Evaluation Criteria) and SAS 70 (The Statement on Auditing Standards No. 70). Take ISO 27001 for example. Its control measures, including access control, information system acquisition, development, and maintenance can enhance the safety of information system development. However, if corresponding information security programs are neglected when information systems are updated, there may be serious consequences when threats occur. It is difficult, though, to estimate the subsequent costs of recovery and the impact of a negative image on the organizations. As a result, information security issues ought to be taken into comprehensive consideration to make systems sufficiently safe when information systems are updated. To reach the goals of information security, scholars have also proposed practical approaches in their research in recent years. The three key categories are as follows:

1. Organizations should set up complete information security strategies by systems and in policies to stimulate whole awareness of information security. For instance, Kemp and Kemp (2005) think that the regulations of information security policies are the main mechanisms by which organizations can implement information security management, and are able to provide information users a set of management standards so as to maintain information security;
2. Organizations must establish entire operational procedures or control measures on the basis of execution. For example, organizations should choose the proper information facilities to build an Information Security Management System (ISMS) after making information security policies suitable for their organization (Axelrod, Bayuk, & Schutzer, 2009; Eloff & Von Solms, 2000; Vroom & Von Solms, 2004);
3. The corporations’ information security can be achieved by supplying sufficient techniques, manpower and organizational resources. Hartman, Flinn, and Beznosov (2002) emphasize that industries should make whole plans for resource allocation and safety measures with awareness of the dimension of management so as to pursue optimization of the efficacy of information security.

In the past, research regarding information system security can be classified under several types. The first type aimed at projects which had already developed and constructed information systems and examined whether the safety provided was enough to ensure information security. For instance, Dhillon and Backhouse discussed security problems of information systems in 2000. The second
Within-Culture Variation and Information Technology: An Empirical Assessment
Jennifer E. Gerow, Edith Galy, Jason Bennett Thatcher and Mark Srite (2010). *Technological Advancement in Developed and Developing Countries: Discoveries in Global Information Management* (pp. 337-364).
[www.igi-global.com/chapter/within-culture-variation-information-technology/39443?camid=4v1a](www.igi-global.com/chapter/within-culture-variation-information-technology/39443?camid=4v1a)

Improving Student Engagement in Meaningful Learning at Tertiary Level Experiences from a New Zealand Faculty of Law
[www.igi-global.com/article/improving-student-engagement-meaningful-learning/75336?camid=4v1a](www.igi-global.com/article/improving-student-engagement-meaningful-learning/75336?camid=4v1a)