The Classification of Information Assets and Risk Assessment: An Exploratory Study using the Case of C-Bank

Patrick S. Chen, Department of Information Management, Tatung University, Taipei, Taiwan

David C. Yen, School of Economics and Business, SUNY at Oneonta, Oneonta, NY, USA

Shu-Chiung Lin, Department of Information Management, Tatung University, Taipei, Taiwan

ABSTRACT

Many information systems' incidents result from inadequate protection of information assets. Assets classification and risks assessment procedures will no doubt help to identify the associated risks related to information systems for a better security control. In the banking industry, prior research and studies are rather lacking due to the nature of maintaining confidentiality. The purpose of this study is to develop an approach to classify information assets of financial institutions and also assess their corresponding risks. Delphi method was adopted and questionnaires based on the guidelines of the well-recognized standard of ISO/IEC 27001 were developed subsequently. A total of 99 information assets subject to security breaches are chosen for risks assessment and a panel of seven experts is invited to complete questionnaires. Consequently, a model for calculating the risk index is proposed according to an exponential scale ranging over 9 grades. The results reveal that three types of information assets exposed to a high level of risk warrant special protection. The experts also make some security enhancement suggestions for the assets with a risk grade $\geqq$ 6. Aiming to enrich research literature on the risks assessment of information assets in the banking industry, the results of this study can provide a valuable reference for both academia and security practitioners.

Keywords: *Assets Classification, Information Assets, Information Security, Risks Assessment*

1. INTRODUCTION

In today's information age, information technology (IT) security is becoming increasingly important since most activities that formerly took place in the work place have been changed to the cyberspace (Coles and Hodgkinson, 2008). Most companies in general and the financial institutions in particular, have deployed various information technologies and applications to carry out their operations and adopted a comprehensive security measure to protect their systems (Chen, Kataria, and Krishna, 2011). In addition, degraded security applied to protect the information

DOI: 10.4018/JGIM.2015100102

assets can lead to serious problems such as financial loss, suspended operation, and declining trust, and consequently it tends to leave the organization in high risk. For this reason, information asset security is such an important topic that deserves a special attention.

In recent years we have seen numerous occurrences of information security incidents, many of which involved with the attempts to acquire banking information for illegal profits and hence, lead to increased business risk and lost revenues (Salmela, 2008). For example, in 2008, Heartland Payment Systems in USA was hit by data security breach to disclose credit card data through malware and 94 million credit card accounts were affected (Acohido, 2009). The TJX security breach may be another compelling case to justify and support the need of information systems asset classification and risk assessment (Haggerty, 2008). The information hackers managed to have accessed the in-store kiosks, and used USB drives to load the software onto those terminals and transformed them into remote terminals that connected to TJX's intranet. Form this case, it brings forth a serious issue about the lacking of secured, physical in-site IT assets.

As information security incidents keep pouring in, information system risk assessment has been a topic of research interest (Budgen, 1992; Chen, Kataria, and Krishna, 2011; Keil, Cule, Lyytinen, and Schmidt, 1998; Yang, Shieh, and Tzeng, 2011; Chen, Lin, Li, and Shi, 2008). Classification of information assets may be regarded as the first step for a successful risk control. According to a specific publication 800-53 developed by the National Institute of Standards and Technology (NIST), the domain of risk management may begin with the categorization of information systems. But, the classification of information assets in the financial industry is seldom mentioned in the current research literature. To bridge this gap, this study attempts to develop a methodology for classifying information assets and modeling their associated risks in the financial industry based on well-defined security standards in this subject field.

To analyze information security risks, both quantitative and qualitative methods should be developed accordingly (Karabacak and Sogukpinar, 2005). This study performs an in-depth investigation to classify various information assets and conduct the assessment of the associated risks related to the assets. Useful measures that can be adopted to improve security control in handling high-risk assets are suggested to avoid the recurrence of incidents. Further, the Delphi method is employed to collect and analyze data to examine the case of a representative middle-scale domestic bank, C-Bank (use of acronym for confidentiality) with a total deposit of about US$100 billion. To lead the discussion, the computing environment of the C-Bank is introduced in Figure 1, which shows that the only entry to access the bank's intranet is via a T3 connection.

In terms of the contribution of this study, it may include, but not limit to the following 3 items.

1. Building a risk assessment methodology of information assets to systematically classify all the information assets held by the Computing Center of the C-Bank, which can be generalized for the relevant studies conducted in other financial institutions;
2. Modeling information assets associated risks to assess the risks attached to all corresponding assets to establish a list of detailed risks for future reference and investigation; and
3. Proposing the improvement measures and feasible controls for safeguarding the high-risk information assets to protect the business' competitive advantages.

The remainder of this paper is organized as follows. Section 2 addresses the information systems and security practices of the case company, C-Bank. Literature review part providing comprehensive research background knowledge and introducing the classification of information assets and related risk assessments studies in particular, are provided in Section 3. Section 4 introduces the example to be studied and the Delphi method used to investigate C-Bank, respectively. Moreover, a detailed account of the classification of information assets and the