Chapter 4
A Hybrid Asset–Based IT Risk Management Framework

Baris Cimen
https://orcid.org/0000-0002-2445-6235
Department of Management Information Systems, Bogazici University, Turkey

Meltem Mutluturk
https://orcid.org/0000-0001-5666-594X
Department of Management Information Systems, Bogazici University, Turkey

Esra Kocak
https://orcid.org/0000-0002-4808-830X
Department of Management Information Systems, Bogazici University, Turkey

Bilgin Metin
https://orcid.org/0000-0002-5828-9770
Department of Management Information Systems, Bogazici University, Turkey

ABSTRACT

Information security has become one of the most important responsibilities of all organizations due to increasing cyber threats. Attackers take advantage of systems vulnerabilities; therefore, system administrators should be aware of potential threats to take necessary actions to protect their organizations and stakeholders. At this point, a risk assessment is needed to discover possible threats for vulnerable systems of the organization and to implement strategies for the business goals. This study proposes a hybrid risk management framework using both qualitative and quantitative methods to analyze risk within organizations and reduce them with practical countermeasures. Based on this framework, case studies have been carried out considering three hypothetical companies identifying possible information security risks, and these risks have been reduced to an acceptable level by applying the proposed risk analysis methodology.

DOI: 10.4018/978-1-6684-3698-1.ch004

INTRODUCTION

Cyber-attacks have confounded information technology infrastructure of organizations and posed significant threats to their valuable information resources that have been valued as extremely important assets in cyberspace. Business managers need to be savvy to possible threats, aware of and prepared for both internal and external elements in order to manage cybersecurity risks. Hence, risk analysis procedure assists managers through evaluating possible threats or risks imposed on organizations, measuring the probability and impact of those risks and finally implementing strategies that create additional value to business operations by means of protecting their most precious information assets. Although, the most established risk analysis methodologies give great attention to technical risks, in recent, business organizations need risk analysis that incorporates social and organizational elements of complex systems with technical aspects in order to correctly evaluate and manage those risks. Within this context, the main objective of this paper is to address information risk management concepts considering possible threats and important organizational assets.

Drawing upon BS 7799 (Biery, 2006) information security risk management guidelines, in addition, by contributing additional possible threats, three hypothetical companies have been examined in terms of their business and organizational priorities. To that end, a strategic framework was proposed in order to identify critical business operations and relevant threats along with asset valuation for these three companies. Finally, a summary of evaluations and solutions were proposed to the identified threats for these companies. This study proposes a hybrid risk management framework via using both qualitative and quantitative methods to analyze risks within three hypothetical companies with the aim of incorporating social and organizational aspects alongside technical ones to overcome incompetencies of methods that previous studies did not. The remainder of the paper is structured as follows. The extant literature on cybersecurity risk analysis and management was reviewed and followed by presenting the proposed risk management framework. The paper concludes by providing a summary of the results and an overview of solutions and evaluations.

BACKGROUND

Business Impact Analysis (BIA) has been defined as the process of conducting risk and gap assessment along with the implementation of global security standards considering people, process and technology in an organization (Sikdar, 2017). Business landscape renders a need for BIA within the context of business continuity management plan as a result of the latest trends such as globalization, e-commerce, enterprise resource planning, outsourcing business operations and legal and regulatory norms (Sikdar, 2017). Moreover, companies have developed BIA programs to cope with crisis events such as technological failures, natural events and deliberate disasters (Păunescu et al., 2018). While performing BIA, it is crucial to think in an organizational context and to understand relationships and dependencies throughout the enterprise including customers, business partners, stakeholders, supply chain vendors along with legal and regulatory institutions (Sikdar, 2017). According to Bjerga and Aven (2016), BIA estimates the possible damages that an enterprise might suffer without taking into consideration recovery methods. Although BIA and risk analysis have been often treated as separate activities, they are linked to each other by basic premises such as, what can happen, what will be affected and what are the resulting effects and impact (Hiles, 2002). Within this context, risk analysis refers to the study of evaluating