Chapter 24

E-Business and Information Security Risk Management: Challenges and Potential Solutions

Stefan Fenz
Vienna University of Technology, Austria

ABSTRACT

For almost all private individuals and especially organizations, information technology (IT) including hardware, software, and data is an irreplaceable part of their everyday life/business. Thus, IT has to be protected in an adequate way to ensure that it delivers the expected services. Information security risk management (ISRM) helps to holistically protect the IT and to minimize their failure probability at reasonable costs. This chapter shows why ISRM is important for e-businesses, gives a brief overview about the ISRM history, describes current problems in ISRM, and presents novel ISRM methods as potential solutions to the stated problems. The chapter closes with an outlook on future ISRM research directions.

INTRODUCTION

Information technology including hardware, software, and data is an integral part of our everyday life and it has brought enormous benefits to almost every economic sector. Nowadays, people and especially organizations are heavily relying and dependent on information technology (Commission of the European Communities, 2006). To ensure that our world is working as expected we have to protect IT components and the data which is stored on these components. The 2007 cyber attacks on the Estonian IT infrastructure and the July 2009 attacks on governmental websites of South Korea and the US have shown how vulnerable national IT infrastructures are.
E-Business and Information Security Risk Management

Information security breaches can cause serious harm to commercial organizations and studies have shown that even the stock price of an organization can be affected by information security breaches (cf. Campbell et al., 2003). According to Gefen et al. (2004) trust is especially important in the case of e-Commerce. Mahadevan (2004) proposed a three dimensional framework for defining e-business models. Within the framework, security and trust represent significant values to buyers and sellers. Both concepts are considered major concerns in e-business. Therefore, the author argues that risk management clearly increases the value of e-business operations for buyers and sellers. Besides several other components, trust and security depend on an established and maintained IT-security program which protects hardware, software, and data. Ideally the IT-security program is based on a comprehensive information security risk analysis. In that way sellers can efficiently protect their assets to prevent income loss, and buyers can make sure that their data is processed and stored in a secure way. Forrester Research estimated the IT-security costs of organizations in 2007 to over 100 billion USD worldwide. The Verizon 2009 Data Breach Investigations Report examined 90 confirmed breaches comprising over 285 million sensitive data records (Baker et al., 2009). 87% of these breaches were considered avoidable through simple or intermediate controls. Here Information security risk management (ISRM) comes in. ISRM provides organizations tools and processes to estimate the risk level of their resources and to identify measures to mitigate the risk to an acceptable level. Although, ISRM has been used in the research and industrial field for over 30 years it is still linked to several problems. Therefore, the objectives of this chapter are: (i) to introduce the reader to ISRM, (ii) to give a brief overview about the ISRM history, (iii) to describe current problems in ISRM, (iv) to present novel ISRM methods as potential solutions to the stated problems, and (v) to provide an outlook to future research directions.

BACKGROUND

Generally risk is defined as the probability per unit time of the occurrence of a unit cost burden (Sage and White, 1980). In the information security context risk is defined as a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization (Stoneburner et al., 2002). As the security measures which are necessary to lower the risk are almost always associated with costs, organizations strive for those measures which are capable to reduce the risk to an acceptable level at the lowest possible costs. ISRM addresses exactly these issues and was defined by the National Institute of Standards and Technology (NIST) in Special Publication 800-30 as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ mission (Stoneburner et al., 2002). Information security risk management represents a crucial element in ensuring a long-term business success and numerous approaches to implementing an adequate information security risk management strategy have been proposed. Although the definition above was published in 2002 we have to keep in mind that information security risk management is not a new domain. The history of information security risk management shows that people are researching in that field for over 30 years. Standards and best-practice guidelines are available and implemented in many organizations. So why be any longer concerned about information security risk management?

It was 1975 when the U.S. National Bureau of Standards proposed the Annual Loss Expectancy (ALE) as a metric for measuring computer-related
Related Content

An Implementation of a New Type of Online Auction
[www.igi-global.com/chapter/implementation-new-type-online-auction/39501?camid=4v1a](www.igi-global.com/chapter/implementation-new-type-online-auction/39501?camid=4v1a)

E-Commerce Agents and Payment Systems
[www.igi-global.com/chapter/commerce-agents-payment-systems/9321?camid=4v1a](www.igi-global.com/chapter/commerce-agents-payment-systems/9321?camid=4v1a)

Value-Based Analysis of Mobile Tagging
[www.igi-global.com/article/value-based-analysis-mobile-tagging/50300?camid=4v1a](www.igi-global.com/article/value-based-analysis-mobile-tagging/50300?camid=4v1a)

Adoption of e-Commerce by Canadian SMEs: Defining Organizational, Environmental and Innovation Characteristics
[www.igi-global.com/chapter/adoption-commerce-canadian-smes/41192?camid=4v1a](www.igi-global.com/chapter/adoption-commerce-canadian-smes/41192?camid=4v1a)