Chapter 3
Cyber Risk Management in Banks:
Cyber Risk Insurance

İsmail Yıldırım
Hittite University, Turkey

ABSTRACT

Security vulnerabilities available in cyber security systems lead to virtual and physical damages to financial systems which in turn cause national- and individual-level security issues. Today's world is being shaped by digital technology, and cyber threats to information constitute a significant risk factor for businesses. This study explores the cyber security risks the banking system may encounter. The status of banking system, a system which includes a number of online services, in Turkey with respect to cyber security risks and the current risks are assessed and presented along with possible solutions. This study analyzes e-payment systems (online banking and e-trade/the use of debit/credit cards) and the supply chain, the backbone of the e-finance system, with respect to national cyber security risks. Nevertheless, cyber risk insurance, an emerging tool for cyber risk management, was analyzed in detail.

INTRODUCTION

Many nations introduce radical solutions against cyberattacks and make investments in such solutions. A number of nations such as the United States of America prefer to protect their critical infrastructure of cyber security on the market level, while nations such as Israel developed state-centric security strategies. Many cyber security specialists stated that it is not possible to adopt an effective defense and counteracting security regimen without cooperation with the stakeholders from the private sector, as the state services are backed by a number of private service providers and telecommunication companies (Grauman, 2012).

Cyber risk is a type of risk which includes any unexpected technical failure of the IT infrastructure of a business or any cyberattack targeting such infrastructure which leads to possible financial losses

DOI: 10.4018/978-1-5225-5927-6.ch003

and damaged brand value. Today, any commercial establishment ranging from Small- and Middle-sized Enterprises (SMEs) to international businesses face the financial consequences of the risks arising from cyber threats. As a result, a new market has emerged with the increasing interest in cyber security products.

Cyberattacks brought with them a new opportunity for insurance companies which offer their services in a highly competitive market and that want to expand their product range. Many companies have already introduced their cyber insurance products. And many more are preparing to launch their products. According to the survey by ABI Research, it is expected the global cyber risk insurance market will reach up to US$10 billion in market value by 2020. The main factors behind this growth are reported to be the increased costs associated with cyber breaches and cyberattacks, and the adoption of risk management strategies which tend to transfer the risks associated with cyber threats to insurance companies. It was further reported that the cyber risk insurance market has been growing at an annual rate of 20-30% in the USA and Europe (www.usom.gov.tr).

Cyberattacks constitute a major risk factor for both privately-owned and state-owned enterprises. Insurance companies have developed insurance packages to minimize the possible effects of cyberattacks on enterprises under the names of data recovery insurance, data protection insurance, cyber insurance, and cyber liability insurance. Cyberattacks may have adverse effects on the automation infrastructure of enterprises. However, the reach of such attacks are not limited to these systems. These cyberattacks are associated with legal, managerial, public relations, and financial consequences (Assaf, 2008).

Cyber liability insurance companies offer assurance against such cyber risks having analyzed the relevant consequences. A cyberattack may have adverse effects on the reputation and market value of an enterprise, not to mention the damages such as confidential information theft or corruption of the information. Coverage of cyber liability insurance policy may include damages and protection costs associated with a breach of information, virus threats to the third party data, unauthorized access to third party information, access to system codes, software theft, employees' disclosure of confidential information, and so forth.

Moreover, it is also possible to be insured, optionally, with policy coverage of any damages associated with an interruption in network functions, payments made to third parties in order to eliminate any security threats, corruption of electronic information due to negligence, and any costs arising from protective measures taken.

CYBER SECURITY RISKS

Aon, one of the global leaders in risk management, insurance, reassurance brokerage and human resources consultation, publishes a number of reports annually based on the opinions of specialists, their know-how and research data available. And one of the most important reports is the Global Risk Management Survey. According to the survey made in 2017, "Damage to Reputation/Brand" was listed on top of a list of 10 risks, which emphasizes the need to manage this risk properly in enterprises. Defective products, fraudulent business practices and corruption remained among the major risks threatening a company's reputation. Cyber risk, on the other hand, was listed in the fifth position.