Chapter 4

Cyber Risk: A Big Challenge in Developed and Emerging Markets

Maria Cristina Arcuri
University of Modena and Reggio Emilia, Italy

Marina Brogi
University of Roma “La Sapienza”, Italy

Gino Gandolfi
University of Parma, Italy

ABSTRACT

The dependence on cyberspace has considerably increased over time, as such, people look at risk associated with cyber technology. This chapter focuses on the cyber risk issue. The authors aim to describe the global state of the art and point out the potential negative consequences of this type of systemic risk. Cyber risk increasingly affects both public and private institutions. Some of the risks that entities face are the following: computer security breaches, cyber theft, cyber terrorism, cyber espionage. Developed nations but also emerging markets suffer from cyber risk. It is therefore important to examine the different security regulation implemented across different markets. Moreover, cyber risk is a concern for all economic sectors. In particular, it is a crucial issue in banking sector because of the negative effects of cyber attacks, among others, the financial losses and the reputational risk. However, the awareness is increasing and cyber insurance is growing.

INTRODUCTION

The growth of the internet has been a big social and technological change. It reduces barriers to trade and allows people across the world to communicate and collaborate. In other words, information technology represents an important driver for the economic development.

The dependence on cyberspace has considerably increased over time, as such, we look at risk associated with cyber technology. Cyber risk could be considered as an emerging risk, a “newly developing or
Cyber Risk

changing risk that is difficult to quantify and could have a major impact on society and industry” (Swiss Re, 2013). Considering its potentially systemic nature, cyber risk is a global risk.

Cyber risk increasingly affects both public and private institutions. Some of the risks that entities face are the following: computer security breaches, cyber theft, privacy theft, cyber terrorism, cyber extortion, cyber espionage, cyber threats to infrastructure. Therefore, an information security breach can have negative economic impacts: lower sales revenues, higher expenses, decrease in future profits and dividends, worse reputation, reduction in the market value. Since the market value represents the confidence that investors have in a firm, measuring the market value allows to calculate the impact of a cyber attack.

In recent years, cyber-crime has become increasingly sophisticated, making it difficult to prevent, detect and mitigate. Developed nations but also emerging markets suffer from cyber risk.

Information security breaches are a concern for all economic sectors, from telecommunications, to media and entertainment, from energy to transportation, from military industries to banking and finance. All rely on increasingly-sophisticated, critical information technology infrastructures which must be protected.

According to a recent estimate, cyber crime costs the global economy about USD445 billion every year and in the last years about 90% of large organisations suffered at least one security breach.

Recent surveys reveal that today approximately 80% of executives are not confident in their company’s current level of protection but only about 60% plans to invest on cybersecurity in the future. Nevertheless, the awareness is increasing. The demand for cybersecurity jobs is expanding and cyber insurance is growing.

The objective of the chapter is to describe the global state of the art and point out the potential negative consequences of this type of systemic risk.

INFORMATION SECURITY: A GROWING CHALLENGE

In the last years, digital technology has revolutionised economic and social interaction. Internet has often improved the way to conduct business. Nevertheless, widespread interconnectivity has increased the vulnerability of the critical infrastructures to information security breaches.

A 2013 PwC survey demonstrates that more than 90% of large organisations recently suffered a security breach. Moreover, a 2013 ACE survey conducted of 650 executives across a range of industries and 15 countries all over the world shows that businesses expect cyber risk will have significant financial impact in the next two years. It follows that cyber risk has become a very debated issue.

Some of the risks that entities face in this realm include:

- Legal liability;
- Computer security breaches;
- Privacy breaches;
- Cyber theft;
- Cyber espionage (it is the use of computer networks to gain illicit access to confidential information, held by a government or other organization);
- Cyber spying (it is a form of cybercrime in which hackers target computer networks in order to gain access to profitable information);