Chapter 8
Economics of Cyber Security and the Way Forward

Taiseera Al Balushi
Sultan Qaboos University, Oman

Saqib Ali
Sultan Qaboos University, Oman

Osama Rehman
Bahria University, Pakistan

ABSTRACT

Initiatives carried by companies, institutes and governments to flourish and embellish the Information and Communication Technology (ICT) among the public have led to its penetration into every walk of life. ICT enhances the efficiency of various systems, such as the organisation and transfer of data. However, with the digital and remote access features of ICT comes the motivation towards financial, political and military gains by rivals. Security threats and vulnerabilities in existing ICT systems have resulted in cyber-attacks that are usually followed by substantial financial losses. This study discusses the security in ICT from a business, economic and government perspective. The study makes an attempt to understand the seriousness of the security issues and highlights the consequences of security breech from an economic perspective. Based on the performed analysis, the factors behind these attacks are provided along with recommendations for better preparations against them.

1. INTRODUCTION

Information and Communication Technology (ICT) is a vital component in our current society, reaching and accessing within every level of the surrounding environment. Along with the implementation of ICT, comes the critical part of securing it as well. The significance of this challenge was demonstrated in 2009 when President Barak Obama, just after taking charge of the office, identified the criticality of cyber security and ordered a review of the ICT security in the country (White House, 2010). This matter was further consolidated by the FBI Director, Robert Mueller, who predicted that Cyber threat would

DOI: 10.4018/978-1-5225-5634-3.ch008

equal or even eclipse the terrorist threat with the passage of time (Mueller, 2013). The accuracy of this statement could be realised by observing the financial loss of $800 million in 2014 as compared to $18 million in 2001, which was reported to the Internet Crime Complaint Centre (IC3) (Statista). As a result of this, the governments all over the world have taken major initiatives to secure their ICT based systems. Among them is the government of UK, that spends £16 billion every year on ICT (Office, 2009). In the modern times, after land, sea, air, and space, the cyber domain has become the fifth largest competitive component of war among the nations across the world (Hayden, 2011).

This particular study discusses the issues of ICT security from the economical and regional perspective. It points out the threats, vulnerabilities, attacks, damages, approaches and recommendations for the state-of-the-art ICT based systems. The paper examines several penetration incidents of the ICT in various critical sectors of the society. The seriousness of ICT security is demonstrated by the losses incurred to the finances, properties and lives because of security attacks. In addition, the paper follows an approach to uncover the root causes behind the attacks from a social and geo-political perspective.

Since most of the ICT security incidents are sensitive information, it is a challenge to find a complete and clear picture on the security status around the world. The literature and analysis performed in this work have shown that the society and the social structure form a major factor in the context of ICT security. In all the security incidents, humans have always been involved either as attackers or victims. As a consequence, it is required to create an awareness and education among the humans in the organizations to be ethical, loyal and vigilant. This research studies the trends and requirements for achieving an effective ICT security by considering reports, news articles, research papers and technical information of various countries around the world with the intent of obtaining a broader picture.

Rest of the paper is organized in the following order. Section 2 discusses the background of this field and lists several cases of cyber-attacks and fatalities that have incurred. Section 3 discusses the impact of cyber-attacks and crimes on the economy of various countries. The lessons learnt by major organisations and countries are given in Section 4. The various approaches from the technical, legal, managerial and standardisation aspects for cyber safety and security are discussed in Section 5. Section 6 analyses the causes of the security breaches and attacks, and also offers recommendations to overcome these issues. Finally, Section 7 summarises and concludes this paper.

2. BACKGROUND

Cybercrimes are usually initiated with the vulnerabilities that are present in a given ICT system. Observing these loop-holes, a hacker plans and executes an attack. A combination of skills, resources, motives and opportunities leads to the optimum blend required to perform an attack. Any breach in the ICT security can lead to a heavy losses and even casualties, thus making it equivalent to any other war attack. Some cases of the cyber-attacks that lead to significant losses are given below.

One of the types of attacks on ICT based systems is the insider attack that is usually initiated by trusted employees, students or contractors, who are granted authorised access to systems. The attackers are usually familiar with the organisation's policies, systems working procedures and network architecture. Based on different reports, 14% to 87% of the cyber-attacks worldwide are initiated internally within the organisation (DoD, 2000; Verizon, 2013). One example is a group of insiders at a wireless telecommunication firm who had created clones of more than 16,000 customer cell phones and made approximately $15 million from the unauthorised calls (Lewellen, 2012). Another example is that of a