Chapter 68
Cyber Security:
Future IT-Security Challenges for Tomorrow's Leaders and Businesses

Michael A. Goedeker
Hacker Defense Network, USA

ABSTRACT

This chapter focuses on the understanding and skills needed by tomorrow's business leaders, namely understanding what security teams do and why security is so challenging based on external influences such as cyber espionage, warfare, and crime, which are currently having an adverse impact on the trust that customers have on the Internet and e-Business and e-Commerce. The introduction starts with issues that the business and IT security face in regards to a common language, which has caused issues in the past in understanding how vital security is to international business revenue through a secure and Internet-connected infrastructure and data. Details are then discussed about how cyber espionage and warfare hinder business and have adverse negative consequences through customer mistrust of Internet-based company resources and data storage. Lastly, this chapter looks at how both government and business lack a common connection between the business and IT as well as the vital security function in projects as well as the usage of proactive security teams, understanding the hacking process to secure systems, and the need and proper usage of security awareness campaigns to decrease risk and increase business value of the security function.

INTRODUCTION

This chapter focuses on reviewing the current literature, trends and best practice information to determine what cyber security challenges tomorrow's business leaders face and which skills will be needed to protect enterprises from criminal hackers and cyber warfare, as well as espionage in the future. Cyber espionage and warfare have led to an increase in cyber crime (through reverse engineering of attacking technology and infection methods). The need has arisen for executive managers to have a basic understanding of digital or cyber security so that both aspects of the business are integrated into a more efficient team and better overall security posture. Answering this question seems very obvious in lieu of what has happened recently in regards to the NSA and the intelligence

DOI: 10.4018/978-1-4666-8111-8.ch068

community through Mr. Snowden's leaked information. Discussions about dark budgets and secret spy programs that include the recording of all encompassing data collection that includes phone records, emails and Internet traffic concern many businesses. If this chapter had been written a few years ago, many would not have even read it because the rift between cyber security departments and the rest of the business were so big that the value of what cyber security departments do was questioned and viewed as an unrealistic return on investment. Additionally some business executives believed an unjustified perception that only a little security is needed because nothing will happen. On one hand, there are a security team and its initiatives of checking and creating policies that aim at protecting the enterprise from disruptions and cyber crime, and on the other side are business departments that are expected to be in budget and highlight the value of projects in regards to how these help create more revenue for the company. Other business functions of an organization understanding and recognizing how cyber security is a vital business function have, however, been an issue and a challenge for many CISOs (Chief Information Security Officer) and Security Officers in the past. Business managers in the past did not understand cyber or digital security as a vital business function, nor did they understand what exactly needed to be reported when a breach occurred (Salmon & Collins, 2013). Today we see how complex a topic cyber security is and how this protects revenue, and helps to add more revenue by helping to introduce new technologies to maintain technical advantages in markets while still protecting company production and process secrets from cyber criminals. Factors that lead to misunderstandings in the past was a false sense that minimal security was needed because nothing happened, this was wrong because many hacked companies only found out much later that hackers or cyber criminals broke into systems and stole data. Security Officers were wrong when they expected the business to spend money on new products without justifying why those products and solutions were needed in a language that business executives understood. The implementation of security solutions also could be measured by metrics and revenue or reduced costs so that advantages to the business were clearer.

Currently, newspaper articles from the Guardian, the New York Times as well as other prevalent and well-known newspapers recently highlighted the NSA's (National Security Agency) global espionage data collection program in detail. Information could be read about how data was being collected (also in which countries) of any and all communications from network traffic as well as telephone calls and social media transactions, being captured, analyzed and assessed or passed on to various other departments for action. Whistleblowers are a very good example of how risks of information leaks (wither ethical or not) from insiders (contractors, partners or even employees) are still a big threat to all as well as the impact of that risk is very real and prevalent. Many have seen current covert espionage activities (and the way that data was collected) as one of the biggest infringements on the global community's use of the Internet for normal communications. Businesses and citizens agree that these actions of espionage could be seen as a violation of their human rights, not to mention the national sovereignty of those nations being spied on (Dinniss, 2012). In this maelstrom of emotions, accusations as well as fantastic claims, a bigger and even more important problem comes to light. The insider is a huge threat and poses a higher risk factor in cyber crime.

Cyber or digital security is vital to international business because it helps to protect businesses from the threat of losing competitive advantages and information of its business practices to competitors due to unauthorized access or unintentional Data theft. Security helps protect businesses from disruptions due to cyber crime, espionage and criminal hackers by implementing the systems, mechanisms and awareness needed to detect, log