Chapter 8
Cyber Security:
Cyber Risk Challenges for Future Leaders and Businesses

Michael A. Goedeker
Independent Researcher, Germany

ABSTRACT

New attacks and methods seen today indicate an emerging trend and dependency on reverse-engineered technology that was used in the past by espionage and intelligence agencies and their tactics as well as use of modern technology to obtain information and data that is turned into usable intelligence. One of the many disturbing consequences of this is that we are faced with attackers that are versed in stealth, deception, planting false information, and increased training in newer attack technologies that classical tools can no longer reliably find. In addition, advanced attack and deception skills now use OSINT (open source intelligence) data collection tactics that have moved entire attack chains into the espionage and surveillance realm.

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 cybercrime (through reverse engineering of attacking technology and infection methods). The need has arisen for executive managers to

DOI: 10.4018/978-1-7998-4861-5.ch008

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 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 cybercrime, 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 helps 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