Chapter 79
Cybersecurity Concerns in International Business

Joel F. Williquette
Bank of Luxemburg, USA

ABSTRACT

The topic is cybersecurity concerns in international business. The issue of cybersecurity and cybercrime is a complex one with several sources for cybercrime including activities by individual criminals, organized crime, and governments. The research question explored is, "Can companies protect themselves given the rise in cybercrime?" Research findings conclude that businesses need to increase their efforts and invest in technologies, staff, technical training, and processes and programs aimed at improving the use of risk-based assessments, defenses, intrusion and anomaly detection, and the business's ability to recover should a cybercrime take place.

INTRODUCTION

Businesses have always been a target for thieves and criminals, and in today's cyber age this is particularly the case. Through the use of computers, instead of criminals who ride a horse or drive a getaway car, we now have cyber criminals who can attack or rob from thousands of miles away. Worldwide the number of cybercrime incidents increased by 48% between 2013 and 2014. This represents a total increase of 66% in cybercrime incidents since 2009 (Oliver, 2014). There are also shared costs of cybercrime which do not need to be directly perpetrated against a business to have an impact. As an example, in 2013 the US retailer Target was hacked and lost information on 40 million debit and credit cards (Upton & Creese, 2014). The cost and consequences were carried by Target, its customers, and by banks and credit unions who had to pay over US$200 million for the reissuance of the compromised debit and credit cards (Krebs, 2014).

Businesses often do not possess the resources, staff, systems, programs, or training to mount successful, multilayered defenses given the increasing occurrence and sophistication of cybercrime. Not only is it difficult to keep staff trained, but there is significant competition for cybersecurity employees in general. In 2014, the assistant director of the United States Federal Bureau of Investigation's (FBI) Cyber

DOI: 10.4018/978-1-5225-9866-4.ch079

Division, Joseph Demarest, stated the agency had had hopes of hiring 2,000 new cyber professionals but faced challenges in their ability to attract enough qualified candidates. Competition for properly trained cyber professionals is fierce even for the largest firms, agencies, and organizations (Simmins, 2014).

Given the increase in cybercrime occurrences, the changing strategies used by cyber criminals and the difficulty in finding cybersecurity staff, businesses are finding it difficult to keep up with what is required to maintain a robust cybersecurity defense. However, there are strategies that can be employed including hardening existing defenses, deploying new technology, and switching to risk based mitigation strategies, aimed at focusing existing resources where they will be the most beneficial.

LITERATURE REVIEW

The literature review involved examining definitions, the US Government's response to rising cybercrime, the players that account for the rising tide in cybercrime, the cost of cybercrime, and the solutions that exist for businesses including investing in technology, staff, and training.

Definitions

It is important to define five terms for clarity in the remainder of this chapter. The Oxford Dictionary (2015) defines "cyberthreat" as the possibility of a malicious attempt to damage or disrupt a computer network or system; "cybercrime" as being crime conducted via the Internet or some other computer network; "cyberwar" as the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems; "cybersecurity" as the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this; and "human capital" as the skills, knowledge, and experience possessed by an individual or population, viewed in terms of their value or cost to an organization or country.

US Government's Response to Rising Cybercrime

To understand the current cybersecurity situation for businesses, we must first understand the response of governments. Because of growing cybersecurity threats to US interests, the Top Secret National Security Presidential Directive (NSPD) 38 was signed by President George W. Bush in 2004 (EPIC, 2014). Though the exact contents of NSPD 38 are still classified, the White House released a document with the same title that requested that the US develop the following:

1. A National Cybersecurity (NCS) Response System;
2. An NCS Threat and Vulnerability Reduction Program;
3. An NCS Awareness and Training Program;
4. Secure the Government's Cyberspace; and
5. Develop a National Security and International Cyberspace Security Cooperation (EPIC, 2014).

In 2008, in response to increased hacking activity believed to be perpetrated by the Chinese Government on US companies and US Governmental installations, President Bush issued NSPD 54 which added several new initiatives including the development and implementation of a government-wide cyber