Chapter 87
Cybersecurity and Human Capital in Community Banks

Joel F. Williquette
University of Wisconsin-Green Bay, USA

ABSTRACT

The topic is cybersecurity and human capital. The research question explored is, "Do United States (US) community businesses have the right human capital and technology resources to effectively counter the rising threat of cybercrime in the US?" Research findings conclude that US 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 in the United States (US) have always been a target for thieves and criminals. In today's cyber age that is no different. 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, from the comfort of their own homes. Worldwide the number of cybercrime incidents has gone up 48% between 2013 and 2014. This represents a total increase of 66% in cybercrime incidents since 2009 (Oliver, 2014). Cybercrime does not need to be directly perpetrated against a community bank to have an impact. As an example, in 2013 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 $200 million for the reissuance of the compromised debit and credit cards (Krebs, 2014).

Businesses in the US often do not have the resources or the staff to mount successful multilayered defenses given the increasing occurrence and sophistication of cybercrime. Businesses are often understaffed or undertrained to manage and maintain programs aimed at protecting them from cyber criminals. 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 FBI's Cyber Division, Joseph Demarest, stated that the

DOI: 10.4018/978-1-5225-7909-0.ch087

FBI 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, the difficulty in finding cybersecurity staff, and a stricter regulatory US, businesses are finding it difficult to keep up with what is required to maintain a robust cybersecurity defense. All is not without hope, as there are strategies, including hardening existing defenses, deploying new technology, and switching to risk based mitigation strategies, aimed at focusing existing resources where they will do the most good.

LITERATURE REVIEW

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

Definitions

To add clarity, it is important to define five terms. 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 community banks in the US we need to first understand our nation's actions and responses over the course of the last eleven years. 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, 1) develop a National Cybersecurity (NCS) Response System, 2) develop an NCS Threat and Vulnerability Reduction Program, 3) develop 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 6) develop and implement a government-wide cyber counterintelligence (CI) plan, 9) define and develop enduring "leap-ahead" technology, strategies, and programs, and 10) define and develop enduring deterrence strategies and programs (EPIC, 2014).