Chapter 12
The 2009 Rotman–TELUS Joint Study on IT Security Best Practices:
Compared to the United States, How Well is the Canadian Industry Doing?

Walid Hejazi
University of Toronto, Rotman School of Business, Canada

Alan Lefort
TELUS Security Labs, Canada

Rafael Etges
TELUS Security Labs, Canada

Ben Sapiro
TELUS Security Labs, Canada

ABSTRACT

This chapter describes the 2009 study findings in a series of annual studies that the Rotman School of Management at the University of Toronto in Ontario and TELUS, one of Canada's major Telecommunications companies, are committed to undertake to develop a better understanding of the state of IT Security in Canada and its relevance to other jurisdictions, including the United States. This 2009 study was based on a pre-test involving nine focus groups conducted across Canada with over 50 participants. As a result of sound marketing of the 2009 survey and the critical need for these study results, the authors focus on how 500 Canadian organizations with over 100 employees are faring in effectively coping with network breaches. In 2009, as in their 2008 study version, the research team found that organizations maintain that they have an ongoing commitment to IT Security Best Practices. However, with the 2009 financial crisis in North America and elsewhere, the threat appears to be amplified, both from outside the organization and from within. Study implications regarding the USA PATRIOT Act are discussed at the end of this chapter.

DOI: 10.4018/978-1-61692-805-6.ch012

INTRODUCTION

2008-2009: A Challenge for IT Security in Canada

In 2008, TELUS and the University of Toronto's Rotman School of Management jointly developed a study to provide clarity on the state of IT Security in Canada. Responses from 300 IT and security professionals allowed the study team to understand for the first time how Canada differs from the U.S. in terms of system vulnerability threats and how prepared Canada is to deal with those threats, in terms of people, process, and technology. The 2008 study was also meant to serve as an important data base that could be coordinated with study findings in other jurisdictions, such as in the U.S., where the annual Computer Security Institute's computer crime survey and findings are reported (CSI, 2008).

As a result of the authors' 2008 study undertaking in the Canadian domain, they discovered some key Best Practices of the top industry performers in terms of IT Security. These practices included a stronger focus on communication and risk management, a greater focus on protecting applications, and a commitment to optimizing budgets to reduce risks and to maintain business continuity when network breaches occur.

After concluding their 2008 study, the study team set a 2009 goal to validate and expand on their many useful findings, which they shared with colleagues in the IT Security sector. However, in late 2008, the Canadian economy experienced a serious crisis, with adverse impacts felt across all business sectors. The magnitude of that downturn forced the research team to rethink their approach to the 2009 study.

Before we get into the approach that we finally settled on, we first look at the 2009 U.S.-based Computer Security Institute key survey findings. We then ask the Question of, Given the annual Computer Security Institute (CSI) computer crime and security survey, Why undertake a separate Canadian study?

The U.S. Computer Security Institute (CSI) 2009 Key Study Findings

As noted, the CSI Computer Crime and Security Survey (CSI, 2009) is part of an annual undertaking describing what kinds of attacks U.S. IT Security respondents' organizations experienced over the previous 12 months, and how much these security incidents cost those organizations. The annual survey includes information about targeted attacks, incident response, and the impacts of both malicious and non-malicious insiders' exploits. It also contains details about how respondents' IT Security programs (including budgeting, policies, and tools) were implemented, respondents' satisfaction with their organizations' tools and budgets, and the effects of compliance with legal and "Best Practices" requirements.

During the tumultuous financial environment of 2009, some of the key findings of the 2009 CSI annual survey included the following (CSI, 2009):

- The IT Security respondents reported big jumps in the incidence of password sniffing, financial fraud, and malware infections.
- The average losses due to security incidents in 2009 were down from those in 2008—from $289,000 per respondent in 2008 to $234,244 per respondent in 2009.
- This decrease in cost was generally perceived by respondents to be a serious commitment by their organizations to maintaining industry "Best Practices" in terms of IT Security compliance.
- Generally, the survey respondents were satisfied but not overjoyed with the security techniques employed by their organizations.
- When asked what actions were taken following a security breach, 22% of the re-