Chapter 10
Information, Innovation and the Boogeyman:
Contextual Factors That Influence the Canadian Government's Response to Cyberspace Risk

Trevor Fowler
Dalhousie University, Canada & City of London, Canada

Kevin Quigley
Dalhousie University, Canada

ABSTRACT

Governments around the Western world are becoming increasingly concerned about cyber security. This paper uses the Hood et al. Risk Regulation Regime (2001) framework to describe Public Safety Canada's Cyber Security Strategy and analyze the social and economic pressures that will influence the manner in which the strategy will be operationalized. This paper recommends that government: takes a balanced approach to securing its own systems, recognizing the costs of an overly precautionary stance; continues to work and exchange information on cyber security with owners and operators of critical infrastructure while at the same time recognizing the market context in which they operate, which constrains this exchange; and helps Canadians to be secure online with enhanced public education programs that have a longer-term view and recognize people's desire for flexibility and convenience in the technology they use. The research in this paper is drawn from academic literature, media analysis and semi-structured interviews.

INTRODUCTION

When the Auditor General of Canada (2009) criticized the Canadian government's weak performance in critical infrastructure protection (CIP) and emergency response, she noted plans had been ready for months but had failed to receive Cabinet approval. The government's cyber strategy was among the plans that had languished. Following the audit, the government moved quickly to ensure these long-waiting plans

DOI: 10.4018/978-1-5225-8897-9.ch010

received Cabinet approval. Two years after the audit and one year after the cyber plan was announced, in February 2011, a cyber attack infiltrated key central government agencies, including Treasury Board Secretariat, the Finance Department and a research agency for the Department of National Defence (Defence Research and Development Canada) (Weston, 2011, February 16). The result: government took multiple systems offline, for weeks. Several public servants were without even basic email service. Given that the cyber plans had been in place for so long, the systems seem remarkably vulnerable and the response unimaginative, and unimaginable.

Governments in the Western world are becoming increasingly fascinated by cyber security [see, for example, Whitehouse (2009) and United Kingdom Cabinet Office (2009)] but it's not entirely clear why the sudden urgency and – as the example above shows – how effective their responses to cyber challenges will be.

How vulnerable are our systems? The IT industry reports regularly about the increasing amount of cyber crime and privacy breaches; they warn us about our vulnerability due to our dependence on these complex and interdependent systems, and of a pending cyber war with other nations (see, for example, Clarke & Knake, 2012). Yet the IT industry has oversold problems before: Y2K, for example. Government bureaucratic processes approved billions on Y2K projects that seemed unable to distinguish between low and high probability/consequence risks (Quigley, 2008). In fact, despite the claims of science fiction movies, there are very few large-scale Internet failures. It could be argued the redundancies of the Internet create more sources of resilience than vulnerability.

There have been calls to encourage people to treat cyber security as a civic duty (Harknett & Stever, 2009) but to date public opinion polls and media coverage would suggest most people are not concerned. Indeed, people are more concerned about service flexibility and using their devices of choice. The Internet is arguably the most remarkable innovation in decades and remains largely unregulated. At the same time, public opinion is fickle. Fifteen years ago, no one would have supported the kinds of security checks we endure in airports today, but 9/11 was a game-changer – a focusing event – that forced people to adjust to a new normal. A large-scale cyber attack in North America, as we witnessed in Estonia in 2007, for example, could prompt a similar shift in public expectations and government response.

The Canadian government's cyber strategy has emerged from this highly uncertain and fluid context. The strategy is a high-level document that has few specifics. As the devil is often in the detail, the purpose of this article is to explore the contextual factors that influenced its development and will influence the manner in which the strategy is operationalized. The cyber strategy does not exist in a vacuum: policymakers need to understand and indeed anticipate the political, social and market pressures that may influence the policy process in the cyber security domain. This awareness will help them strike a necessary but difficult balance between security, on the one hand, and innovation and efficiency on the other.

The paper is divided into four parts. First, we introduce the Hood *et al*. framework as the methodological tool that structures the paper and dictates the sources of data from which we will draw. The framework examines contextual factors that influence government risk regulation regimes and is appropriate for an exploratory discussion of a relatively nascent topic such as cyber security and Canada's new cyber security strategy, in particular. Second, we describe briefly the Canadian government's new national cyber strategy. Third, given the framework, we examine the extent to which markets, public opinion and special interests are likely to influence the government's approach to cyber security. This section will consider, for example, the role of the law, insurance, the media and concentration of power in different critical sectors. We conclude with a discussion of risks and opportunities that lie ahead for government, organized by the three strategic priorities in the plan.