The ChronicleHerald

THE MILITARY AFFAIRS COLUMN BY TIM DUNNE

The cyber economy's soft underbelly

October 1, 2014

The Internet is critical to Canadian commerce and to federal, provincial, territorial and municipal governments. The federal government alone offers more than 130 commonly used services online, including tax returns, Employment Insurance applications and student loan applications.

It is no longer simply an easy way to send personal messages.

According to Public Safety Canada's Cyber Security Strategy:

- 74 per cent of Canadian households had paid Internet service in 2008;
- 59 per cent of personal tax filings were electronic in 2008;
- 67 per cent of Canadians banked online in 2009;
- Canadian online sales in 2007 were estimated at $62.7 billion; and
- In 2007, 87 per cent of Canadian businesses used the Internet.

The identity protection and fraud detection service, CSID, of Austin, Tex., reported that in 2011, "more than 174 million records (were) compromised in data breaches, costing businesses US $5.5 million per breach in monetary damages."

Tim Page, then-president of the Canadian Association for Defence and Security Industries (now VP of Seaspan), told attendees at last fall's Security Technology Conference in Ottawa that there are "serious risks to public safety, threats to our ecosystems, traditional way of life and national security challenges abound and are growing in complexity, impact and cost."

Canada's Canadian Cyber Incident Response Centre (CCIRC) provides a cushion for Canadian business and government. Working with the private sector and all levels of government, CCIRC is the guard and guardian against cyber attacks on government and industrial information and data systems.

Its website notes that it is "Canada's national co-ordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events," and has probably dealt with any malware that the Canadian private sector might encounter.

CCIRC assists industry with cyber-related challenges. But significant numbers of Canadian businesses only see disincentives to sharing information with government. As one conference speaker asked: "What do they get in return?"

They are concerned that privileged information affecting competitiveness may be inadvertently leaked to rival interests if cyber incidents are shared.

CIRC has acknowledged industry concerns about sensitive commercial information and ensures that only information related to cyber threats is shared, and that clients' competitive positions are preserved. Still, the centre only receives notice of about one-tenth of incidents occurring in Canadian business each year.

Canadian enterprise and government have become increasingly susceptible to cyber attack as more employees ask for data to be uploaded to the Internet to allow them to work on their personal devices.

This BYOD (bring your own device) approach to business may appear to reduce hardware costs, but it has introduced new threats as employees seek access to data through their personal computers, smart phones and tablets, opening the door to the more than one million pieces of malware lurking in cyberspace.

However, 80 to 85 per cent of cyber attacks can be prevented by simply applying patches for the systems and office suites on which critical infrastructure and industrial control systems rely. Maintaining system updates, upgrades and patches, and limiting the number of people with administrator rights remain the most effective and least expensive measures available.

Our success in cyberspace is one of our greatest national assets. Protecting this success means protecting our cyber systems against malicious misuse and other destructive attacks. But there is no simple way to detect, identify and recover from attackers who cannot be seen or heard, who leave no physical evidence behind them, and who hide their tracks through a complex web of compromised computers.

Cyber security affects all Canadians. Even attackers with basic skills have the potential to cause real harm. Sophisticated attackers can disrupt the electronic controls of our power grids, water treatment plants, hospitals and telecommunications networks. They interfere with the production and delivery of basic goods and services provided by our governments and the private sector, and they undermine our privacy by stealing our personal information.

Every year, we detect more attackers than the year before. And every year, those seeking to infiltrate, exploit or attack our cyber systems are more sophisticated and better resourced than the year before. And they are increasingly successful.

Whether they know it or not, many Canadian companies have already been compromised

---

Tim Dunne is a Halifax-based communications consultant and military affairs writer, a Research Fellow with Dalhousie University's Centre for Foreign Policy Studies and a member of the Royal United Services Institute (NS) Security Affairs Committee. He is a veteran of peacekeeping operations in the Middle East, Bosnia Herzegovina, Macedonia and Kosovo.