As cyberattacks skyrocket, Canada needs to work with—and not hinder—cybersecurity experts

28 July 2021, by Yuan Stevens and Stephanie Tran

When assessing whether the Government of Canada meets standards for vulnerability disclosure in comparison to G20 members, we discovered that Canada is falling behind its peers. Credit: Cybersecure Policy Exchange, Ryerson University, Author provided

Cyberattacks are on the rise, impacting people, systems, infrastructures and governments with potentially devastating and far-reaching effects. Most recently, these include the massive REvil ransomware attack and the discovery that the Pegasus spyware was tracking more than 1,000 people.

A common cause of cyberattacks involves the exploitation of security vulnerabilities. These are conditions or behaviours that can enable the breach, misuse and manipulation of data. Examples can include poorly written computer code or something as simple as failing to install a security patch.

Exploiting vulnerabilities

There can be particularly significant impacts when attackers exploit security vulnerabilities involving digital systems used by federal governments.

For example, in July 2015, the United States Office of Personnel Management announced that malicious hackers had exfiltrated highly sensitive personal information and fingerprints of roughly 21.5 million federal workers and their associates, due to a string of poor security practices and system vulnerabilities.

The massive data breach served as a wake-up call for the U.S. federal government. Barack Obama's administration consequently announced the Department of Defense would be responsible for storing federal employee data.

Not long after that, the "Hack the Pentagon" pilot program was announced, where the U.S. government invited external experts to responsibly report security flaws.

This pilot paved the way for what has become a standard security practice used by the U.S. government. Since 2020, all American federal agencies have been required to enable the disclosure of security vulnerabilities.

Canada lagging behind

By comparison, our recent report found that the government of Canada is lagging behind countries like the U.S. by failing to welcome vulnerability reports from external experts.

We haven't had an attack the size of the Office of Personnel Management breach in the U.S., but we aren't immune either.

Consider the Equifax breach in 2017, when 19,000 Canadians were affected when attackers exploited a security vulnerability in an online customer portal.

In August 2020, the Canada Revenue Agency [locked more than 5,000 user accounts] due to cyberattacks partially enabled by the agency's lack of two-factor authentication.

Our report, published through the [Cybersecure Policy Exchange] at Ryerson University, is the first publicly available research that examines how Canada treats the reporting of security flaws in comparison to other countries.

We discovered that while 60 percent of G20 members have distinct and clear processes for reporting security vulnerabilities in public infrastructure, Canada does not.

Cybersecurity experts can disclose "cyber incidents" to the [Canadian Centre for Cyber Security]. But this term is [defined so narrowly] that it excludes vulnerabilities that have not yet been weaponized.

Security research activity	Potential applicable law and provision	Brief summary of provision
Hacking (i.e., unauthorized access), including unsolicited security or penetration testing	Section 342.1 of the *Criminal Code*	Unauthorized use of computer, computer service, or computer password
	Section 380(1) of the *Criminal Code*	Fraud
	Section 430 of the *Criminal Code*	Mischief, or wilfully destroying or damaging property, including overloading computer systems, "causing chaos"
	Section 184 of the *Criminal Code*	Wilful interception of private communications
Obtaining, storing or retrieving computer data without permission	Section 342.1 of the *Criminal Code*	Unauthorized use of computer data, requiring intent to commit mischief under s. 430 of the *Criminal Code*
Impersonation (a technique that is commonly referred to as "social engineering" in the computer security industry)	Section 402.2 of the *Criminal Code*	Identity theft or identity fraud
Possessing, importing or using devices made for hacking	Sections 342.2 of the *Criminal Code*	Possession or use of hardware, software or other tools used to commit hacking (section 342.1 of the *Criminal Code*) or mischief (section 430 of the *Criminal Code*)
Circumventing security measures, including decryption	Section 41.1(1) of the *Copyright Act*	Circumvention of a "technological protection measure" for any technology, device or component that controls access to a copyrighted work or sound recording

Some of the legal risks in Canada for discovering and disclosing security vulnerabilities found in software and hardware. Credit: Cybersecure Policy Exchange, Ryerson University

And while the [United Kingdom] and [the U.S.] governments have promised to make efforts to fix security flaws that are reported, the Canadian Centre for Cyber Security has made no such promise.

By not supporting and protecting security researchers in identifying vulnerabilities, these gaps ultimately put Canada and Canadians at greater risk.

Vulnerable systems, vulnerable people

Cybersecurity experts can face significant legal risks when they report security flaws to the Canadian government. Computer hacking is prohibited by the [Criminal Code], and in certain circumstances by laws like the [Copyright Act].

But unlike in [the Netherlands] and the U.S., there is no legal framework here for reporting security vulnerabilities in good faith.

Canada's current approach has a chilling effect on the disclosure of security weaknesses found not only in government systems, but also for all software and hardware.

This approach largely leaves cybersecurity researchers in the dark about whether—and how—they should notify the government when they spot security flaws that could be exploited.

A cybersecure Canada requires working with experts who identify the security risks faced by our institutions and infrastructure.

The phases of vulnerability disclosure: discovery, reporting, validation and triage, developing a solution, applying that solution, and informing the public. Credit: Cybersecure Policy Exchange, Ryerson University

It's not too late for the federal government to institute a process allowing experts to report security flaws, and to draw on best practices while doing so.

Our work outlines the importance of defining who can submit vulnerability reports, and describes what the reporting and fixing process can look like. It's important to credit or recognize the experts who disclosed. The public should be given information about vulnerabilities and the solutions required to fix them.

Imperative improvements

Cybersecurity experts are "a significant but underappreciated resource" when it comes to reducing security risks of government systems. They want to help.

The Canadian government needs to implement clearer processes and policies to foster co-operation with cybersecurity experts working in the public interest.

As cyberattacks grow in frequency, scale and sophistication, better cybersecurity practices in Canada are not just desirable—they are imperative.