engineerscanada
ingénieurscanada

# PROFESSIONAL PRACTICE IN CYBER SECURITY

## THE ENGINEERING PROFESSION'S POSITION

- Cyber security legislation must consider the need for engineer input in the development and maintenance of cyber security software, hardware, systems, and critical infrastructure
- Regardless of whether it is a federal, provincial or territorial statute, cyber security requires the involvement of an engineer licensed with a provincial or territorial licensing authority.
- Incorporating engineers' accountability into federal, provincial or territorial legislation and regulations related to cyber security infrastructure and systems weaves the engineering regulatory process into the fabric of government and thereby keeps Canadians safe.
- Engineering regulators in Canada exist to protect the public interest. They set high professional and ethical standards, establish and maintain codes of conduct, and administer regulatory processes for engineers to ensure protection of the public interest and the natural environment.

## The challenge(s)

Cyber security is described as the techniques of protecting computers, networks, hardware, software, programs, and data from unauthorized access or attacks that are aimed for exploitation[1]. In a progressively digital world, Canadians expect that technological systems are protected against cyber security threats and susceptibilities. Canada's economic stability and national security depend on resilient critical infrastructure. Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructures can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructures could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence[2]. As these infrastructure systems become increasingly interconnected, particularly with the development of artificial intelligence systems, and as essential services become gradually managed online; cyber security vulnerabilities, incidents, and premeditated cyberattacks against critical infrastructure have the serious potential to compromise national security and the personal safety of Canadians.

As the technology develops and as digital systems become more complex and sophisticated, so do the skills of individuals who attempt to undermine them. Significant cyber hacks and data breaches have become increasingly common today. In 2017, a Statistics Canada study outlined that approximately 21 per cent of Canadian businesses reported that they were impacted by a cyber attack incident that affected their day-to-day operations. They also found that 41 per cent of larger businesses were more than twice as likely than smaller businesses to have identified an impactful cyber incident.[3]

With the growing demand for cyber security professionals, and the immediate requirement to defend against future cyberattacks, it is important that the federal government remains vigilant in ensuring that engineers licensed with provincial or territorial regulators, namely engineers working in cyber security, who are experts in communications and safety, are involved in the design, implementation, and maintenance of cyber security software, hardware, systems and critical cyber infrastructure.

Engineers in specialized disciplines, at a minimum, have the same skills as other IT professionals but are held professionally and ethically accountable by the engineering regulators through provincial and territorial legislation across Canada. Other IT professionals are not bound by a regulatory environment. Including engineers in the development and maintenance of software, hardware, systems and critical infrastructure will hold individuals accountable for the work that they do through the existing enforcement, investigation, and discipline process. Without the inclusion of engineers in this process, there is limited accountability, other than resorting to the justice system.

engineerscanada
ingénieurscanada

# PROFESSIONAL PRACTICE IN CYBER SECURITY

## How Engineers Canada has contributed

Engineers Canada actively participates in federal consultations regarding legislation and regulations that impact the work of engineers and address initiatives that require the expertise of an engineer.

In addition, engineering regulators in Canada exist to protect and enhance the public welfare. They set high professional and ethical standards, establish and maintain codes of conduct, and administer regulatory processes for engineers to ensure protection of the public and the natural environment.

## Recommendations to the federal government

Engineers Canada was encouraged by the federal government's commitment towards protecting the critical cyber systems that underpin the infrastructure and services that are integral to the daily lives of Canadians through Budget 2019.

Engineers Canada supports the federal government's cyber initiatives, specifically the work of The Canadian Centre for Cyber Security, to ensure a safe and secure cyberspace, which is important for the security, stability, and prosperity of Canada. To further support Canadians from future cyberattacks, the federal government should:

- Ensure that any legislation and regulations that refer to engineering work are prepared with the input from engineers licensed in accordance with provincial and territorial engineering acts.
- Use demand-side legislation to drive the need for engineering work to be performed by individuals who are licensed to do so, thereby encouraging compliance with professional regulatory legislation.
- Further develop, clarify and enforce regulations, rules, cyber security guidelines, and standards regarding the development and maintenance of critical infrastructure to require licensed practitioners perform work that protects the public when safety management and regulatory compliance is delegated to federally regulated industries.

## How Engineers Canada will contribute

Engineers Canada will continue to contribute in the following ways:

- Monitor the government agenda, legislative initiatives, and proposed cyber security regulations to bring recommendations on demand-side legislation to the attention of the government.
- Request that decision-makers ensure that cyber security legislation retains explicit references to engineers and engineering in the interest of public safety across Canada.
- Actively identify opportunities to require input from engineers within federal legislation and regulations where such involvement would be in the public interest.
- Support the work of provincial and territorial regulators to enforce the engineering acts as they pertain to the practice of engineering disciplines impacting public safety.
- Through the Canadian Engineering Accreditation Board, advise undergraduate engineering programs in cyber security on how to meet the accreditation criteria.

[1] The Economic Times (2019). "Definition of 'Cyber Security'." Retrieved October 3, 2019 from: https://economictimes.indiatimes.com/definition/cyber-security.

[2] Public Safety Canada (2018). "National Strategy for Critical Infrastructure". Retrieved May 29, 2020 from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

[3] Statistics Canada (2018). "Impact of cybercrime on Canadian businesses, 2017." Retrieved July 8, 2019 from: https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm.

300–55 Metcalfe Street, Ottawa, ON K1P 6L5 (613) 232-2474 | government.relations@engineerscanada.ca | www.engineerscanada.ca