Building Security Awareness in the Academic Community

Canada is at the forefront of innovation, research and development in an array of disciplines, including Science, Technology, Engineering and Health, some of which requires the collection of sensitive data from Canadians. This cutting edge research supports Canada's economic interests, as well as broader social and national interests. Therefore, it is imperative that university administrators and researchers are aware of the threats faced by their institutions' valuable research.

What is at stake?

Advanced research conducted in Canadian academic institutions presents an attractive target for foreign states or groups. From an academic standpoint, the illicit acquisition of the results of this often cutting edge research can result in the loss of intellectual property, can negatively impact publication opportunities and subsequent patent rights, and the ability to realize the economic fruits of this research. In addition to potentially damaging the integrity of Canadian academic institutions and their research programs, the illicit transfer of certain types of research could also potentially contribute to advancements in the military and intelligence capabilities of states or groups whose aims run counter to Canadian interests, and may also place institutions and researchers in violation of Canadian law or regulations.

Safeguarding Academic Research

The open and collaborative environment in Canadian academic institutions promotes creativity and is vital to advancing Canadian innovation and research. However, this environment can also be vulnerable to threats to the integrity of research, and may, depending on the area of research, compromise national security or undercut Canada's research or economic competitive advantage. Thus, academic communities should evaluate the security measures they have in place and, where necessary, take measures to strengthen weak access controls and reduce the potential for exploitation. In doing so, Canadian academic institutions can better defend themselves against potential losses resulting from the theft of their research and contribute to safeguarding Canada's national interests.

What are the threats?

Threats to Canadian research can involve individuals or groups from inside and outside of the Canadian academic community. In either case, they seek the same thing: access to valuable information, technology and expertise.

Although the majority of students, university employees, and/or contractors who have direct or indirect access to knowledge or proprietary materials have lawful and legitimate intentions, a small proportion could exploit this access for malicious purposes. Similarly, the ability to safeguard academic research could also be vulnerable for misuse, including by visiting students or faculty, private sector partners, foreign government representatives, intelligence operatives, hackers, or activists who seek to collaborate with members of an academic community. In all such cases, these individuals, wittingly or unwittingly, work on behalf of an outside interest, including foreign governments or non-state groups (e.g., a terrorist group, an organized crime group).

The security of research data may also be threatened by ransomware, phishing attacks or cyber-attacks that take advantage of vulnerabilities in the cyber security practices or information technology infrastructure at an institution.

The section below highlights some basic mitigation tools for researchers and their respective institutions to minimize the risk and improve the overall security environment within the research environment.

Did you know?

Some foreign states or groups use students, researchers, and others to acquire sensitive and proprietary information from Canadian individuals and entities. Often with little-to-no formal intelligence tradecraft training, but often in a position to acquire vast quantities of data or knowledge, these individuals wittingly or unwittingly use relatively open tools available to them to facilitate the transfer of technology (e.g. webmail, USB keys, and other electronic and hard-copy transfer mechanisms). In some cases, they are part of state programs aimed at attracting international talent, and receive salaries from the state while simultaneously collecting funding and/or salaries from Canadian institutions.

The Government of Canada is aware of individuals who seek to engage with Canadian universities in sensitive areas where research can enable foreign military, intelligence, and security capabilities (e.g., artificial intelligence, quantum computing, materials science, advanced computing, etc.). Technology transfer can be conducted without advising the joint partner in the initiative, and usually with the use of Canadian research resources.

Best Practices

1. Know your partners and collaborators

Institutions should conduct basic research, such as an open source background check, on potential partners. This will assist you in understanding the intentions and credibility of your collaborators.

Who have they partnered with in the past? Do they have affiliations that they have not disclosed? How will they benefit from the partnership? What is the intended end use or benefit for the partner? What will your institution gain from this partnership?

2. Strong cyber hygiene practices

Review the Canadian Centre for Cyber Security's Cyber Safe Guide: https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx

3. Be aware of dual use applications of your research and understand your responsibilities under laws and regulations

Dual-use refers to products, knowledge or technologies based on research, which, although conducted for other purposes, have the potential to be exploited to purposely cause harm, or to threaten public health or national security. Institutions should consider these factors to determine the likelihood of their data being targeted, and be mindful of how their research and data can be vulnerable to misuse, theft and/or cyber-attacks.

A general understanding of laws, regulations or institutional policies applicable to your area of research is critical. This understanding needs to go beyond safety, and incorporate considerations to secure your research.

Assess the control status of your research in the context of Canada's Domestic (Controls Goods Program) or Export Control Regulations (Export Control List, Nuclear Non-proliferation Import and Export Control Regulations). This assessment is an indicator of whether your research has dual-use potential or is sensitive from a proliferation point of view.

4. Research Integrity Policies, Transparency and Disclosure

Educate yourselves, employees and/or trainees on what is considered to be a conflict of interest and what this means for how they engage in their work, especially when partnering overseas.

Implement measures to control who is able to access sensitive data. Access rights should only be granted to those who you have determined to have a need.

GENERAL INDICATORS OF CONCERN

- Undeclared joint research affiliations with foreign government institutes and/or universities (indication that they may be using your research to inform foreign research without proper approval);
- Listing of participation in a foreign talent program or technology transfer program on a CV;
- Frequent, unexplained travel to high-risk locations that have civil-military fusions, or legal frameworks allowing governments to access and retain any information (indication that they may be lecturing and/or working abroad);
- High amounts of network bandwidth usage beyond normal work usage (indication that they are uploading/downloading amounts of data beyond what they normally require);
- Unusual work hours and/or unexplained and drastic work schedule changes.

WANT TO REPORT AN INCIDENT?

RCMP – National Security Information Network (NSIN)	Reporting of unrecognized persons, suspicious incidents, or computer-related activities.	Phone: 1-800-420-5805 Email: NSIN_RISN@rcmp-grc.gc.ca
Canadian Security Intelligence Service (CSIS)	Reporting of potential non-urgent national security threats or suspicious activities.	Phone: 1-800-267-7685 Website: https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html
Canadian Centre for Cyber Security (CCCS)	The CCCS Contact Centre is the single point of contact for questions on Cyber Security.	Phone : 1-833-CYBER-88 Email: contact@cyber.gc.ca

Public Safety's Safeguarding Science Program delivers free and interactive workshop with front-line researchers with the core objective of improving the security environment at academic institutions. For more information about this program or to inquire about scheduling, please contact: ps.safeguardingscience-scienceensecurite.sp@canada.ca

Cat. No.: PS4-261/2020E-PDF / ISBN: 978-0-660-34414-0

Public Safety Canada Sécurité publique Canada

Canada