Sensibilisation de la communauté universitaire à la sécurité

Le Canada est à l'avant-garde de l'innovation, de la recherche et du développement dans une gamme de disciplines, telles que la science, la technologie, l'ingénierie et la santé, dont certaines exigent la collecte de données sensibles auprès des Canadiens. Cette recherche de pointe appuie les intérêts économiques du Canada, de même que des intérêts sociaux et nationaux plus vastes. Il est donc essentiel que les administrateurs et les chercheurs des universités connaissent les menaces qui guettent les précieuses recherches de leur établissement.

Quels sont les enjeux?

Les recherches poussées réalisées dans les établissements universitaires canadiens constituent une cible de choix pour certains pays ou groupes étrangers. D'un point de vue universitaire, l'acquisition illégale des résultats de ces recherches souvent pointues peut entraîner la perte de propriété intellectuelle, nuire aux possibilités de publication et aux droits de brevet subséquents, et limiter la capacité de profiter des retombées économiques des travaux. En plus d'une éventuelle atteinte à l'intégrité et aux programmes de recherche des établissements universitaires du Canada, le transfert illégal de certains types de recherche pourrait contribuer à parfaire les capacités militaires et de renseignement de pays ou groupes dont les buts sont contraires aux intérêts du Canada, et amener des établissements et des chercheurs à contrevenir aux lois ou règlements du Canada.

Protection des recherches universitaires

L'environnement ouvert et coopératif des établissements universitaires canadiens favorise la créativité et est essentiel à l'avancement de l'innovation et de la recherche au Canada. Cet environnement peut toutefois être vulnérable aux menaces à l'intégrité des travaux de recherche et, selon le domaine de recherche, compromettre la sécurité nationale ou miner l'avantage concurrentiel du Canada en matière de recherche ou d'économie. Les communautés universitaires devraient donc évaluer leurs mécanismes de sécurité et, au besoin, prendre des mesures pour resserrer les contrôles d'accès déficients et réduire le risque d'exploitation. Ce faisant, les établissements universitaires du Canada peuvent mieux se défendre contre des pertes éventuelles attribuables au vol de leurs travaux de recherche, et contribuer à la protection des intérêts nationaux du Canada.

Quelles sont les menaces?

Les menaces aux travaux de recherche du Canada peuvent provenir de personnes ou de groupes de l'intérieur ou de l'extérieur du monde universitaire canadien. Dans l'un ou l'autre des cas, ils poursuivent un même but : accéder à des renseignements, des technologies et des expertises de grande valeur. Malgré les intentions légales et légitimes de la majorité des étudiants, du personnel universitaire et des fournisseurs qui ont un accès direct ou indirect aux connaissances ou aux documents exclusifs, une poignée d'entre eux pourrait exploiter cet accès à des fins malveillantes. Dans la même veine, la capacité de protéger les recherches universitaires pourrait être utilisée à mauvais escient, notamment par des étudiants ou des professeurs invités, des partenaires du secteur privé, des représentants de gouvernements étrangers, des agents secrets, des pirates informatiques ou des activistes qui cherchent à collaborer avec les membres d'une communauté universitaire. Dans pareils cas, ces personnes travaillent, sciemment ou non, pour des intérêts extérieurs tels que des gouvernements étrangers ou des groupes non étatiques (p. ex. groupes terroristes ou groupes du crime organisé).

La sécurité des données de recherche peut aussi être menacée par des logiciels rançonneurs, des attaques d'hameçonnage ou des cyberattaques qui exploitent les points faibles des pratiques de cybersécurité ou de l'infrastructure informatique d'un établissement.

Voici les éléments clés de certains outils de base d'atténuation des risques proposés aux chercheurs et à leur établissement respectif, afin de minimiser le risque et d'améliorer le cadre de sécurité global du milieu de recherche.

Le saviez-vous?

Certains pays ou groupes étrangers se servent d'étudiants, de chercheurs et d'autres personnes pour obtenir des renseignements sensibles et exclusifs auprès de Canadiens et d'entités canadiennes. Ne comptant bien souvent que peu de formation officielle sur les techniques de renseignement, sinon aucune, mais capables d'obtenir de grandes quantités de données ou de connaissances, ces personnes utilisent, sciemment ou non, les outils relativement ouverts à leur portée pour faciliter le transfert de technologie (p. ex. messagerie Web, clés USB et autres mécanismes de transfert électroniques ou papier). Certains prennent part à des programmes nationaux de recrutement de talents à l'étranger, et touchent à la fois un salaire versé par leur pays et des fonds ou un salaire provenant d'établissements canadiens.

Le gouvernement du Canada sait que des personnes cherchent à travailler avec des universités canadiennes sur des sujets de recherche sensibles qui peuvent renforcer à l'étranger les capacités militaires, de renseignement et de sécurité (p. ex. intelligence artificielle, informatique quantique, science des matériaux et informatique de pointe). Le transfert de technologie peut se faire à l'insu du partenaire, et habituellement au moyen de ressources canadiennes de recherche.

Pratiques exemplaires

1. Sachez qui sont vos partenaires et vos collaborateurs

Les établissements devraient assujettir les partenaires éventuels à des vérifications de base, entre autres de leurs antécédents auprès de sources ouvertes. Cette mesure vous aidera à comprendre les intentions et la crédibilité de vos collaborateurs.

À qui se sont-ils associés par le passé? Ont-ils omis de déclarer des affiliations? Qu'est-ce que le partenariat leur apportera? Quelle est l'utilisation finale prévue par le partenaire ou l'avantage qu'il en retire? Qu'est-ce que votre établissement gagnera de ce partenariat?

2. Pratiques de cybersécurité rigoureuses

Consultez le guide *Pensez cybersécurité pour les petites et moyennes entreprises* : https://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx.

3. Méfiez-vous du double usage de vos travaux de recherche et comprenez vos responsabilités en vertu des lois et règlements

Le double usage fait référence aux produits, aux connaissances ou aux technologies issus de travaux de recherche qui, bien que menés à d'autres fins, pourraient être exploités de façon à causer du tort ou à menacer la santé publique ou la sécurité nationale. Les établissements devraient soupeser ces facteurs pour évaluer le risque que leurs données soient ciblées, et être attentifs à ce qui peut exposer leurs travaux de recherche et leurs données à une mauvaise utilisation, au vol ou à une cyberattaque.

Une compréhension générale des lois, des règlements ou des politiques de l'établissement en ce qui a trait à votre domaine de recherche s'avère essentielle. Cette compréhension doit aller au-delà de la sécurité, et intégrer les éléments à considérer pour protéger vos travaux de recherche.

Évaluez l'état de contrôle de vos travaux de recherche dans le contexte des règlements du Canada sur le contrôle intérieur (Programme des marchandises contrôlées) ou sur le contrôle des exportations (Liste des marchandises et technologies d'exportation contrôlée du Canada, Règlement sur le contrôle de l'importation et de l'exportation aux fins de la non-prolifération nucléaire). Cette évaluation fournit un indicateur du risque que vos travaux de recherche se prêtent à un double usage ou à la prolifération.

4. Examen des politiques d'intégrité, de la transparence et de la divulgation

Assurez-vous que vous, vos employés ou vos stagiaires savez en quoi consiste un conflit d'intérêts et comment aborder vos travaux en conséquence, surtout dans le cadre de partenariats outremer.

Instaurez des mesures pour contrôler l'accès aux données sensibles. Vous ne devez accorder l'accès qu'aux personnes qui, selon vous, en ont besoin.

INDICATEURS GÉNÉRAUX DE PRÉOCCUPATION

- Les travaux de recherche affiliés non déclarés avec des institutions gouvernementales ou universités étrangères (indication qu'elles pourraient se servir de votre recherche pour étoffer des travaux de recherche à l'étranger sans obtenir les autorisations requises);
- Inscription sur un c.v. d'une participation à un programme de talent étranger ou à un programme de transfert de technologie;
- Voyages fréquents et inexpliqués vers des endroits très à risque où les forces civiles et militaires sont fusionnées, ou dont les cadres juridiques permettent à des gouvernements de consulter et de conserver tout renseignement (indication que la personne intéressée pourrait donner des conférences ou travailler à l'étranger);
- Utilisation de la bande passante du réseau qui va bien au-delà d'une utilisation professionnelle normale (indication que la personne télécharge ou télédécharge des quantités de données supérieures à la normale);
- Heures de travail inhabituelles ou inexpliquées, et modification considérable de l'horaire de travail.

VOUS SOUHAITEZ SIGNALER UN INCIDENT?

GRC – Réseau info-sécurité nationale (RISN)	Pour signaler la présence d'inconnus ou des incidents ou activités informatiques suspects.	Téléphone : 1-800-420-5805 Courriel : NSIN_RISN@rcmp-grc.gc.ca
Service canadien du renseignement de sécurité (SCRS)	Pour signaler d'éventuelles menaces pour la sécurité nationale ou des activités suspectes non urgentes.	Téléphone : 1-800-267-7685 Site Web : https://www.canada.ca/fr/service-renseignement-securite/organisation/signaler-des-informations-relatives-a-la-securite-nationale.html
Centre canadien pour la cybersécurité (CCC)	Les Services à la clientèle du CCC servent de guichet unique où poser des questions sur la cybersécurité.	Téléphone : 1-833-CYBER-88 Courriel : contact@cyber.gc.ca

Le programme Science en sécurité de Sécurité publique propose un atelier gratuit et interactif aux chercheurs de première ligne, dans le but d'améliorer l'environnement de sécurité des établissements universitaires. Pour en savoir plus au sujet de ce programme ou pour connaître le calendrier de formation, veuillez écrire à : ps.safeguardingscience-scienceensecurite.sp@canada.ca.

No de cat. : PS4-261/2020F-PDF / ISBN : 978-0-660-34415-7

Sécurité publique Canada | Public Safety Canada

Canada