Cyber Threat Intelligence Report

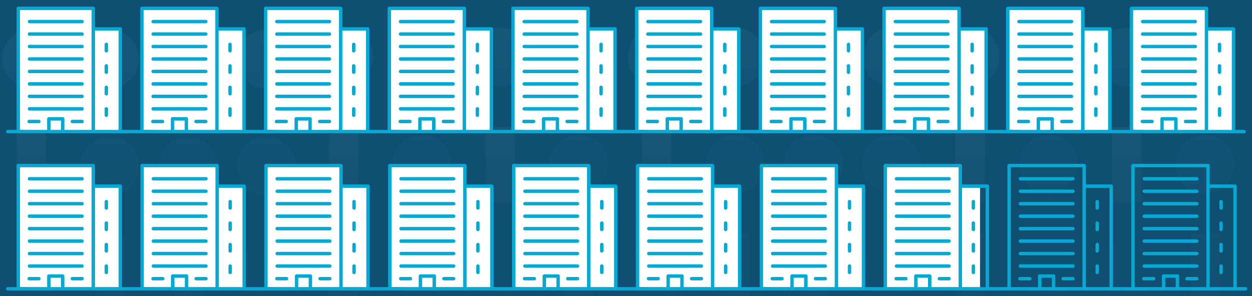
Lacking Cyber Knowledge: The Dangers and Consequences

Cybersecurity Division
Compiled by Sarah Hunt

Date: 29 March 2023

Summary of Threat

In 2022, 89.8% of Canadian companies experienced a successful cyber attack, up from 85.7% in 2021 (CyberEdge Group, LLC, 2021; CyberEdge Group, LLC, 2022).



As these statistics show, as technology continues to advance cyber threats have become increasingly prevalent across Canada. One of the biggest challenges in combating these threats is the lack of cyber knowledge among individuals and organizations. Cyber knowledge refers to the understanding of how to use technology safely and securely and how to protect oneself and one's assets from cyber threats. This lack of knowledge is becoming an ever more significant threat as technology has become an integral part of our daily lives.

Once upon a time, not so long ago, both the methods and vectors for attack were simpler. However, as we have reaped the benefits of interconnectedness, the internet, and smart devices, these methods and vectors have become more complex and difficult to stop. Emails, desktops in offices, and USB keys used to be the extent of the problem. But now there are smartphones, smart watches, laptops, and online digital services to consider. We used to be worried about simple, easy to spot phishing emails, purporting to be from princes with fortunes, but now it could be a very well researched spear phishing email from your boss asking for a simple favour. With this changing landscape and without adequate cyber knowledge, people are more likely to fall prey to cybercriminals and their malicious activities, resulting in financial loss, data breaches, reputational damage, and potentially even legal repercussions for the individual or organization.

Not all the threats associated with poor cyber knowledge need even be as active as clicking on the link of a spear phishing email. A lack of cyber knowledge can also lead to poor cyber hygiene practices, such as weak passwords and failure to update software. These failures to act can be just as damning, making individuals or groups more vulnerable to external threat actors. As such, it is essential to raise awareness about cybersecurity and educate people on how to protect the data and devices they have control over in the digital space to prevent cyber incidents from occurring.

Throughout this report we will go into more depth about the causes and impacts a lack of cyber knowledge can have before going into some actions that can be taken to protect Albertan organizations and citizens in the digital age.

Look out for these pop outs throughout this report, as we will be taking time to discuss a cyber attack on an an Alberta post-secondary institution from 2017. Even though this event took place six years ago, there is lots to learn, especially since we can see how the changes they've made have improved their cybersecurity posture!

Why is There a Lack of Cyber Knowledge?

Quick, what is your source for up-to-date knowledge on cybersecurity? Is it:

A A specific website, such as the Government of Canada's "Get Cyber Safe".

B A cybersecurity-focused organization, such as CyberAlberta or the Canadian Centre for Cyber Security.

C Your partner, child, or other tech-savvy family member.

D I do not have a go-to source for learning more about cybersecurity.

The truth is that a lot of Albertans would probably answer D if asked this question. A 2022 survey commissioned by the Government of Canada found that most Canadians do not think it is likely they will be affected by cyber threats (EKOS Research Associates, 2022).

Herein lies one of the biggest reasons for a lack of cyber knowledge— there is no standardized repository that can be accessed and referenced for cybersecurity. Engineers have their Black Book. Psychologists the Diagnostic and Statistical Manual of Mental Disorders [DSM]. Police have the Criminal Code of Canada. But for cybersecurity there is no such fundamental resource. Having to actively seek out this information from multiple sources results in people allowing their cyber knowledge to lapse as it requires a sustained effort. Given the lack of validation for these sources, they may also give bad or out-of-date information. For example, several websites still state that one of the best ways to pinpoint a phishing email is to look for bad spelling and grammar. However, with improved proofreading applications and software this is not necessarily true, especially for the most effective phishing emails. So, if you were relying on one of these websites for your cyber knowledge, there would be a definite gap.

The lack of cyber resources is not borne out of malicious intent, more out of the overwhelming nature of cyberspace. The rapid pace of technology advancement is introducing new technologies with increased frequency, leading to people being less aware of crucial information about their device configurations and associated risks. Devices are increasingly interconnected, making the digital ecosystem more complex and harder to secure. These networks also increase the risk of compromise. For example, if you fail to update your smart thermostat software, an attacker could exploit newly discovered vulnerabilities to access your network and compromise other devices. Not knowing how your devices interconnect or the security risks involved— such as the difficulty of updating security patches for smart home devices— can put individuals or organizations at risk of cyber attacks.

In the Government of Canada's 2022 survey, the following percentage of respondents indicated that they felt it was likely in the next year that they would be affected by a cyber threat that:

would cause their personal information to be compromised

16%

would cause them to lose files, photos

7%

would cause them financial loss

6%

would result in their data being held for ransom

4%

Some combination of the above

8%

(EKOS Research Associates, 2022, p.12)

This is why there is no defined set of instructions for cybersecurity compared to the other industries mentioned: sheet metal bending allowances rarely change in the Black Book; the DSM has had only five major revisions since 1952; and the Criminal Code had its last major revision in the mid-1980s. Unfortunately, cyberspace is not so defined, with its landscape shifting almost daily. This changing cyber landscape compounds the threat of the lack of cyber knowledge as the budget to keep training and resources updated is lacking, resulting in outdated or simplified materials being positioned against new and complex threats and risks.

In 2017, an Alberta post-secondary institution received a phone call from a vendor they had been working with. The construction company was perplexed why the school had failed to pay its bill. This came as a bit of a shock to the staffers as they'd believed they'd been communicating with the vendor since June, when they'd received an email stating that the construction company had new banking information and requested that school update the account information on their end. Between June and August, the institution had made three payments to the vendor totalling almost $12 million.

What happened?

The staff members fell victim to a phishing scam. However, this wasn't a classic phishing scam where the staffers had been asked in a poorly spelled email to give an unknown party access to their bank account. This was a highly targeted spear phishing campaign. The cybercriminals researched both the school and vendor, and using this research created believable communication that appeared to be from the actual vendor. They even made the email and associated website look like they were from the vendor, with the proper layout and logos used.

Evolutions in cybercrime haven't just been occurring in technical ways, making them hard to keep up with; cybercriminals are now using advanced psychology to trick people. Banal requests are the ones that no one considers and, therefore, make great masks to hide cybercrimes behind. For the post-secondary institution, it was completely reasonable, potentially even expected, that a company may update their banking information. Plus, the threat actors took the time to groom the staffers, communicating with them regularly, before they asked for the change of account. This helped build trust and is the foundation of one of the costliest types of digital fraud, known as Business Email Compromise.

How Business Email Compromise Works... Cybercriminals will:

Identify and research the target

Groom the target with spear phishing emails and/or phone calls to manipulate the individual

Convince the individual to exchange information (e.g., banking information, credentials)

Transfer the target's funds to another account controlled by the cybercriminal

Even though the staffers likely knew how to spot a regular phishing email, they lacked the knowledge to detect such a carefully honed spear phishing email, resulting in the school losing millions of dollars.

What's the Damage?

With the increasing number of cyber attacks worldwide in recent years, it has become clear that a lack of cyber knowledge is a contributing factor to this continued growth. But what exactly are the impacts that could be felt as a result of a lack of cyber knowledge? Listed below are some examples of the damages and effects that knowledge deficiencies can have:

Data Breach

What is it?

A data breach is when there is a breach of confidentiality and protected or sensitive information is exposed to someone who is not authorized to view the data.

What could it cost?

A data breach could result in data being stolen including:

- Personally identifiable information [PII] of staff, clients, and/or users;
- Research/ development data; and/or
- Any kind of protected/ sensitive/ confidential data housed by the organization or individual.

How does a lack of cyber knowledge exacerbate the issue?

According to a Verizon report, 82% of breaches in 2021 were tied back to a human cause, including compromised users, phishing victims, careless users, or human error (Verizon, 2022). Improving people's ability to protect themselves in the digital realm helps reduce the likelihood of data breaches.

Did you know...

According to a 2022 Government of Canada survey, the province with the greatest issue with viruses and malware is Alberta? This correlates with another finding from the survey that indicates that Albertans are the least likely in Canada to take preventative steps to protect themselves online

(EKOS Research Associates, 2022, pp.20, 23).

Identity Theft

What is it?

Identity theft is when an unauthorized party uses misappropriated information to impersonate an individual in some way, most often for financial gain (e.g., applying for loans, accessing bank accounts, etc.). Stolen identities may also be used to access business accounts and information, potentially resulting in data breaches or financial loss for an organization.

What could it cost?

Identity theft could see PII used by cybercriminals to:

- Open or access bank accounts;
- Access personal or work devices, accounts, and files;
- Transfer money out of accounts;
- Apply for loans or credit cards;
- Buy goods and/or services;
- Hide other criminal activities;
- Apply for government benefits or grants; and/or
- Obtain a passport.

How does a lack of cyber knowledge exacerbate the issue?

Social engineering methods—such as phishing, SMiShing (phishing via text message), and vishing (phone call-based phishing)—are the most common ways that cybercriminals steal identities. Since 2019, there has been a steep increase in the number of reported instances of identity theft, according to the Canadian Anti-Fraud Centre, with a 45% increase in the number of identity fraud victims between 2020 and 2021 (Royal Canadian Mounted Police, 2022, p.19). Having knowledge about and being able to spot the different types of social engineering would help reduce the effectiveness of specific methods of identity theft, such as phishing and spoofed websites, reducing the overall impact of identity theft.

Disclaimer

Reputational Damage

What is it?

Reputational damage is hard to quantify but occurs when the reputation or good name of an organization or individual is tarnished based on the actions (or inactions) they took when faced with an event. The reputational loss could be from the public, external stakeholders, internal stakeholders, or any combination of the three. There are several aggravating factors that can increase the level of reputational damage. In the table below are some examples of aggravating factors.

Aggravating Factor	Example
Size of the organization	A larger, more established organization will often experience more of a reputational loss as a result of a cyber attack compared to smaller, less established counterparts.
Perceived level of expertise of the organization	An organization that specializes in technology or security would suffer more reputational damage due to to the perception they should have “known better” in the case of a cyber attack.
Popularity level of the organization	The public may experience a level of schadenfreude when an unpopular or controversial organization fails.
What was impacted in the cyber attack	If the attack caused the loss of the public’s data, the reputational loss may be greater from the public. Conversely, if research and development data was impacted, the organization may lose the confidence of their stakeholders.
Complexity of the attack	A successful attack that is perceived to have a lower complexity level is more likely to result in higher reputational damage, as it is believed the organization should have been able to stop the simple attack.

What could it cost?

The cost of reputational damage can vary depending on the aggravating factors; however, generally it can result in:

- Financial losses from decreased sales, reduced funding, or impacted stock price;
- Loss of trust and goodwill from the public, stakeholders, employees, etc.;
- Stakeholders and investors pulling out of projects or agreements; and/or
- Difficulty hiring new staff or maintaining existing staff.

How does a lack of cyber knowledge exacerbate the issue?

As detailed in the data breach section, more often than not a cyber incident involves the human element. Since most cyber attacks result in at least some form of reputational damage this means that an organization’s potential reputation may rest on the least cyber savvy person in the organization. What can make this worse is the simplicity of the attack. If an employee falls for a phishing email—often considered a simple attack—because they think all phishing emails have pixelated graphics and poor spelling, this could result in greater reputational damage.

Legal and/or Regulatory Issues

What is it?

There are several laws and regulations that govern data and cybersecurity in both Canada and Alberta. More laws are being drafted as a response to the increasing frequency and severity of cyber attacks in recent years. In Alberta, there are several acts enforced that pertain to responsibilities of organizations and individuals to protect privacy, as well as federally regulated statute and common laws regarding the definition of and repercussions for cybercrime. See the reference sheet on the next page for some of the major acts and laws relating to digital crimes.

What could it cost?

Violation of laws or regulations could result in several types of repercussions. The most common of these are financial penalties or fines; however, depending on the type of breach and level of culpability of individuals in the organization, there is the potential for arrest and incarceration. Aside from these legal impacts, there is also the potential for civil litigation if regulations or laws were violated in the course of a cyber attack.

How does a lack of cyber knowledge exacerbate the issue?

Canada has a legal principle that ignorance of a law cannot be used as an excuse when a violation occurs. This places the onus on organizations and individuals to have knowledge of the cyber laws to best protect data and data systems.

Financial Loss

What is it?

Financial loss is any loss which is pecuniary in nature and may result from direct causes (e.g., theft) or indirect causes (e.g., fines, devaluation of brand/image).

What could it cost?

Financial losses could come from several areas related to cyber attacks and cyber negligence, including losses incurred from:

- the direct theft of assets by cybercriminals;
- the cost associated with replacing damaged assets or services;
- stakeholder withdrawal following reputational damage from an attack;
- loss of competitive edge due to research and/or development being leaked;
- payment of fines due to legal or regulatory failure;
- remuneration owed in civil cases due to failure to adequately protect digital and informational assets; and/or
- increases in cyber insurance premiums <u>or</u> the costs arising from the necessity to purchase cyber insurance.

How does a lack of cyber knowledge exacerbate the issue?

A lack of cyber knowledge creates ideal conditions for both negligent use of digital assets and the conditions necessary for malicious threat actors to taken advantage of digital spaces. These conditions make both the frequency and severity of cyber attacks larger, resulting in more extreme financial repercussions.

When considering the case of the 2017 cyber attack on the Alberta post-secondary institution, there are several ways the cyber attack impacted the school. The most obvious impact was financial. Even after working with law enforcement and legal counsel, the school was only able to recover just over 92% of the funds transferred to the cybercriminals. Recovering this amount cost the institution a quarter of a million dollars on top of the unrecovered $880,000. Other costs were likely also incurred, as in direct response to this scam the school changed reporting structures, increased the number of checks and balances associated with payments, and instituted other controls.

A level of reputational damage was likely also incurred when a political leader instructed all Alberta post-secondary institution board chairs to review and update their financial controls based on this incident. Contemporaneous news articles from the time are quite harsh on the school, and particularly the staffers, and an aforementioned political leader outright stated that he “expect[ed] post-secondary institutions to do better to protect public dollars against fraud.” None of this looks good for any organization, but also likely reflected even more poorly on an educational institution, as they are considered pillars of knowledge and intelligence.

Laws & Regulations Reference Sheet

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is the current federal privacy legislation that governs private-sector organizations in Canada who—in the course of commercial activities—collect, use, or disclose personal information.

Personal Information Protection Act (PIPA)

PIPA is an act that governs private-sector organizations, businesses, and some non-profits that collect, use, or disclose personal information in the course of commercial activities. The difference between PIPA and PIPEDA is that PIPA is a provincial act applying to Alberta, while PIPEDA is a federal act, applying across Canada.

Freedom of Information and Protection of Privacy Act (FOIP)

FOIP is a provincial privacy legislation that governs the collection, use, and disclosure of personal information by public-sector organizations in Alberta. It also governs the public's right to privacy and the right Albertans have to know how their information is being used.

Health Information Act (HIA)

HIA is a privacy act that focuses on the protection, use, and disclosure of health-related personal information in Alberta.

Criminal Code of Canada

The Criminal Code details all statute criminal laws in Canada. This includes two sections often tied to cyber-related crimes: Section 184(1), which details the consequences of using digital devices to intercept private communication, and Section 342.1(1), which details the penalties associated with the unauthorized use of a computer device or service.

Case Law

Case law is based on precedents decided in previous criminal or civil trials. Concerning organizations, there are three broad categories of cybercrimes where precedent has been set relating to organizations: (1) employee errors, (2) employee misconduct, and (3) data breaches.

Canada's Anti-Spam Law (CASL)

CASL is a federal regulation which documents and provides guidance as to what is considered spam, unwanted software or malware, and malicious redirection or interception of digital traffic. It also details the administrative monetary penalties associated with the distribution or enactment of spam, malware, or altering of digital transmission in the course of commercial activities.

An Act Respecting Cyber Security (Bill C-26)

An Act Respecting Cyber Security is not currently in effect but is being tabled as Bill C-26 on the federal level. If passed, this act would:

- amend the current *Telecommunication Act* to better secure communication systems in Canada against the threats of intrusion, manipulation, or interruption;
- amend the *Canada Evidence Act* to ensure the confidentiality of disclosures made under the Telecommunication Act regarding breaches; and
- enact the wholly new *Critical Cyber Systems Protection Act* defining strict cybersecurity guidelines for digital systems associated with critical infrastructure in Canada, as well as the repercussions if the guidelines are not followed.

Digital Charter Implementation Act (Bill C-27)

The Digital Charter Implementation Act is not currently in effect but is being tabled as Bill C-27 on the federal level and, if passed, would replace PIPEDA. This Act would update the laws surrounding the collection and use of data by private-sector organizations to meet the current reality of information sharing, including provisions surrounding the use of AI tools relating to privacy.

What Can Be Done?

The lack of cyber knowledge can have multiple causes, including the fast-paced changes in technology, a failure to recognize the importance of cybersecurity, and inadequate training materials. As a result, addressing the risks associated with the lack of cyber knowledge requires a comprehensive, multi-layered strategy.

Education is obviously key to improving cyber knowledge; however, not all education has to involve classes with tests and homework. The expanding knowledge-base that people are exposed to each day means individuals are constantly bombarded with information. Thus, to avoid being completely overwhelmed, people only retain the information they feel is important to them. As such, classroom-based education is not always the best way to have individuals internalize the importance of such issues. There are three types of education that should be considered to bring greater understanding to the nuances of our digital landscape and cybersecurity: informal, formal, and non-formal.

Informal Knowledge Growth

Informal education is difficult to measure because it encompasses all the knowledge and skills acquired through life experiences. This unstructured, lifelong learning is intensely personal to the individual, which is what makes it so crucial to improving cyber knowledge. Educational theories suggest that the concepts that stick with people the most are those which people consider beneficial to their self-interests or the interests of their friends and families. More formalized education has an effect of disconnecting people from the concepts since they have no first-hand connection to the topics. It is one thing to read about the effects of a data breach, but another thing entirely to be given notice that your information was stolen during a data breach.

A shift that needs to occur to advance the ability for people to improve their cyber knowledge is people's willingness to discuss the topic. For example, the author of this report had their data stolen as part of the 2023 Chapters-Indigo ransomware attack. When they discussed the topic with others it became apparent that several of them had also had firsthand experience of a cyber attack. By one person starting the conversation, a greater discussion of cybersecurity was able to occur, ranging from mitigation tactics people had tried to some of the root issues that lead to cyber attacks. While this is just a small, personal experience, it highlights how transparency can breed understanding and information sharing.

A shift in perspective has already begun to occur, seen in the rise of news reporting on cyber-related subjects; however, the closer an individual is to the person sharing the information the more they will get out of the experience. The development of safe spaces to discuss these topics is crucial to the overall improvement of cyber knowledge. This could take many forms, ranging from digital options, such as websites and social media, to public discussions of cybersecurity in different forums, such as schools, public libraries, or seniors' facilities. On an organizational level, groups—such as CyberAlberta's Community of Interest—are key to improving informal learning. These groups include experts in the field, mitigating the risk of misinformation, while also allowing a forum through which organizations can share cyber knowledge and ask for recommendations.

The CyberAlberta Community of Interest, led by the Government of Alberta and formed with cybersecurity leads of Alberta public and private sector organizations, works collaboratively to strengthen Alberta's overall cybersecurity posture.

Click here to learn more about the **CyberAlberta Community of Interest!**

Formal Knowledge Growth

Formal education refers to the traditional classroom-based learning and can have some benefit in bolstering an individual's digital knowledge. There have been recent pushes for more formalized cyber education at all age levels, such as Ontario's recent move to make technological education credits a mandatory part of achieving a high school diploma; some of Alberta's post-secondary institutions, such as NAIT, SAIT, and MacEwan, are developing cybersecurity-specific programs and courses; and in 2021 the USA signed the K-12 Cybersecurity Act to help develop cyber training for young students. Proliferating cyber knowledge at these different levels helps raise awareness of the topic, positioning this as a field to learn more about.

Apprentice-style programs are another avenue to be explored, as it is a type of education which mixes formal training with on-the-job (or informal) learning. Germany promotes *duale ausbildung*, a type of vocational training similar to an apprenticeship that is not limited to trades-type occupations. This allows for German students to work in a field, such as technology or cybersecurity, while also studying the topic in school. This mix of practical and theoretical learning allows students to immediately apply their learnings in the real world, better cementing the training, while also allowing individuals to try out a job before spending extensive time and resources studying the field (potentially only to find out they do not like the work). The introduction of ausbildung-like programs for post-secondary students or people looking for a new career could encourage individuals to take a chance on a different career path, helping to improve their cyber knowledge and career prospects. In 2021, the GoA test piloted a training program similar to ausbildung in the Cybersecurity Division. Four recent graduates were contracted from technical and security programs at NAIT and MacEwan to test the effectiveness of vocational training in the field of cybersecurity. Thus far the program has been successful, with the learners gaining cyber knowledge from a vast array of subject areas, all while aiding the organization.

Future considerations for Alberta's cyber education may include the development of grade school training for students, implementing similar training mandates to those outlined in the USA's K-12 Cybersecurity Act. In the same way typing and other computer skills are now taught in schools, bringing more awareness to other cyber topics at a younger age would help bring ubiquity to the subject, making it something that is discussed in households.

Non-Formal Knowledge Growth

Non-formal education is the term for learning that occurs somewhere between formal and informal learning. It is structured education that takes place outside of formalized teaching institutes. The best example of this type of training is organizational training provided by a workplace, such as the Information Management and Cybersecurity training provided by the GoA. Because this type of education tends to be either sought out by the individual or provided as part of workplace training there is the potential for this form of learning to greatly enhance a person's cyber knowledge. This is because, as discussed in the informal learning section, the more the individual can see the value of the information in their life, the more likely they are to internalize it.

Non-formal cyber courses are freely available online through organizations such as Microsoft, Amazon, and Cisco. Some public libraries, such as the Edmonton Public Library, have deals with services such as LinkedIn Learning, which allow all individuals with a library card to access structured training on a number of topics—including cybersecurity and technology—for free. These services allow people to search for topics that interest them, which allows for them to create a more personal connection with the information, improving retention.

With non-formal education the hardest barrier to overcome is knowing where to start. It can be overwhelming to go on a site with thousands of courses at all different skill levels without an express goal beyond learning more about cyber. This is where informal learning and having cyber knowledge more widely discussed in public would be helpful. For example, hearing people talk about multi-factor authentication gives an interested individual a term to search on these training sites.

Another potential form of non-formal education that organizations can implement is workplace cybersecurity training. This, however, can be a difficult type of training to get right. This training needs to connect to people for them to absorb it, which can be difficult, particularly in larger organizations where individuals have different roles and therefore have different types of digital interactions (e.g., the employee who only uses email and Word versus the technician that uses role-specific software). Listing what an individual needs to do to keep safe in cyberspace will not have value unless there is an explanation of why this is important and even better, why it affects the person taking the training. Workplace cyber training should be an iterative process, taking into account feedback and adjusting the materials regularly. With cyberspace changing regularly so should the training.

Following the successful phishing attack on the school, the post-secondary institution made several changes to mitigate the chances of this happening again. The key change noted in news reports was the development of new controls with more checks and balances at different levels before payments are made.

The institution's website has several indicators that cyber education is something being promoted by the institution. Reports of ethical hacking clubs, notices of the school participating in cybersecurity competitions, and basic information about identifying phishing messages and malicious websites—two of the things that tricked the school—can be found on the school's website.

Other Mitigations to Consider

Education helps treat the root issues associated with a lack of cyber knowledge; however, there are other suggestions that can help mitigate the impacts:

- Development of cybersecurity policies and procedures in organizations.
- Implementation of security controls and technologies to detect, prevent, and remediate impacts.
- Hiring a third-party management service to help keep the organization updated and informed about external risks and threats and to make suggestions on appropriate mitigations.
- Qualifying for and purchasing cyber insurance might be a useful mitigation approach, especially if your organization lacks staff and knowledge to protect your digital assets.

Conclusion

In conclusion, a lack of cyber knowledge is a significant threat that requires immediate attention. Cybersecurity should become a part of everyday conversation, and organizations and individuals should take steps to increase their knowledge and awareness of cyber threats. Outside of what the individual can do to improve their own knowledge, larger changes also need to be made to ensure the security posture of Alberta remains strong. This includes investing in programs and services that promote cyber knowledge to all Albertans. Recommendations for actions include continued investment in cyber education and training programs, increased public awareness campaigns, and encouragement to start a conversation on cyber at all levels. All these changes will help make it easier for individuals and organizations to protect themselves from cyber threats, while a failure to address this issue could result in severe consequences for individuals, organizations, and the province as a whole.

Individuals and organizations need to prioritize cyber knowledge and take proactive measures to protect themselves and their assets from cyber threats. It is only through a collaborative effort that Alberta can hope to overcome the growing threats to our digital cyberspace and fully reap the benefits it provides.

References & Further Reading

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248, DOI: 10.1080/0144929X.2012.708787.

Abawajy, J., & Kim, T.-H. (2010). Performance analysis of cyber security awareness delivery methods. In: Security Technology, Disaster Recovery and Business Continuity. *Communications in Computer and Information Science*, 122, 142-148. DOI: 10.1007/978-3-642-17610-4_16.

Acharjee, S. (2021, February 19). Impact of cyber security: An overview (2021). *UNext*. https://u-next.com/blogs/cyber-security/impact-of-cyber-security/

Alphanauten. (2022, June 27). Ausbildung in Germany: Detailed guidelines (A to Z). *Alphanauten*. https://alphanauten.de/en/ausbildung-in-germany/

Alva Group. (2020, May 14). What is reputational damage?. *Alva*. https://www.alva-group.com/blog/what-is-reputational-damage/

An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c. 23. https://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html

Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. 44th Parliament, 1st Reading, June 14, 2022. Retrieved from the Parliament of Canada, LEGISinfo website on March 24, 2023: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading

Bisson, D. (2021, December 29). K-12 Cybersecurity Act signed into law. *Security Intelligence*. https://securityintelligence.com/news/what-is-k-12-cybersecurity-act/

Brooks, C. (2023, March 05). Cybersecurity trends & statistics for 2023; What you need to know. *Forbes*. https://tinyurl.com/ycktzd2n

Cain, A.A. (2016). Trust and complacency in cyber security. *Master's Theses*, 4679. DOI: 10.31979/etd.a4nf-q57u.

Cain, A.A., Edwards, M.E., & Still, J.D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36-45. DOI: 10.1016/j.jisa.2018.08.002.

Canada Revenue Agency. (2021, October 17). Protect yourself against identity theft. *Government of Canada*. https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/rc284/protect-yourself-against-identity-theft.html

Canadian Anti-Fraud Centre. (2021, May 17). Identity theft and fraud. *Government of Canada*. https://antifraudcentre-centreantifraude.ca/scams-fraudes/identity-identite-eng.htm

Canadian Press. (2023, March 12). Ontario to require tech education course for high school graduation. *SooToday*. https://www.sootoday.com/local-news/ontario-to-require-tech-education-course-for-high-school-graduation-6686677

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Educ Inf Technol*, 28, 1809-1831. DOI: 10.1007/s10639-022-11261-8

Chevalier, M. (2020, October 15). Why cyber hygiene should be a top priority. *Genetec*. https://www.genetec.com/blog/cybersecurity/why-cyber-hygiene-should-be-a-top-priority

Cisco. (n.d.). What is a data breach?. *Cisco*. https://www.cisco.com/c/en/us/products/security/what-is-data-breach.html

Coleman, K. (2022). What is reputational damage, and how bad is it for your business? *StatusLabs*. https://statuslabs.com/what-is-reputational-damage/

Criminal Code, RSC 1985, c. C-46. https://www.laws-lois.justice.gc.ca/eng/acts/C-46/page-1.html

CyberEdge Group, LLC. (2021). 2021 cyberthreat defense report. *CyberEdge Group*. https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf

CyberEdge Group, LLC. (2022). 2022 cyberthreat defense report. *CyberEdge Group*. https://cyber-edge.com/cyberthreat-defense-report-2022/

EKOS Research Associates. (2022). Get Cyber Safe awareness tracking survey: Final report. *Government of Canada*. https://publications.gc.ca/collections/collection_2022/cstc-csec/D96-17-2022-eng.pdf

Federal Bureau of Investigation. (n.d.). Business email compromise. *FBI*. https://tinyurl.com/7b2r58pd

Ferrier, N. (2009). *Fundamentals of emergency management: Preparedness.* Emond Montgomery Publications.

Freedom of Information and Protection of Privacy Act, RSA 2000, c. F-25. https://open.alberta.ca/publications/f25

Friedman, K., & Saville, J. (2014, September 22). Privacy law litigation in Ontario - From the bank to the hospital and beyond. *CanLII Connects.* https://canliiconnects.org/en/commentaries/29907

Get Cyber Safe. (2022, October 14). Oh, Behave! The annual cybersecurity attitudes and behaviors report 2022. *Government of Canada*. https://www.getcybersafe.gc.ca/en/resources/oh-behave-annual-cybersecurity-attitudes-and-behaviors-report-2022

Glaspell, B., & Girlando, D. (2015, December 22). Canadian Businesses Increasingly Face Privacy Breach Class Actions Absent Traditional Forms of Damages. *CanLII Connects.* https://canliiconnects.org/en/commentaires/39614

Gliga-Belavic, A. (2022, October 06). Bill C-27: What your organization needs to know. *MNP Digital*. https://mnpdigital.ca/insights/bill-c-27-what-organizations-need-to-know/

Gurchiek, K. (2019, July 16). Lack of awareness, poor security practices pose cyber risks. *SHRM*. https://tinyurl.com/ycy9dnpt

Health Information Act, RSA 2000, c. H-5. https://open.alberta.ca/publications/h05

Horne, C.A. (2016, November 02). Lack of cyber security knowledge leads to lazy decisions from executives. *The Conversation*. https://theconversation.com/lack-of-cyber-security-knowledge-leads-to-lazy-decisions-from-executives-68065

IBM Corporation. (2022). X-Force threat intelligence index 2022. *IBM Security*. https://www.ibm.com/downloads/cas/ADLMYLAZ

Johnson, J. (2017, December 18). New study: Many consumers lack understanding of basic cyber hygiene. *Tenable*. https://www.tenable.com/blog/new-study-many-consumers-lack-understanding-of-basic-cyber-hygiene

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access*, 9, 99339-99363. DOI: 10.1109/ACCESS.2021.3097144.

Kenton, W. (2022, December 05). Reputational risk: Definition, dangers, causes, and example. Investopedia. https://www.investopedia.com/terms/r/reputational-risk.asp

Klein, G., Zwilling, M., & Lesjak, D. (2022) A comparative study in Israel and Slovenia regarding the awareness, knowledge, and behavior regarding cyber security*. Research Anthology on Business Aspects of Cybersecurity*. DOI: 10.4018/978-1-6684-3698-1.ch020

Koczerginski, M., Wasser, L.A., & Lyons, C. (2017). Cybersecurity – The legal landscape in Canada. *McMillan*. https://mcmillan.ca/insights/publications/cybersecurity-the-legal-landscape-in-canada/

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The relationship between cyber security awareness, knowledge, and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, 6, 1-19. DOI: 10.25147/ijcsr.2017.001.1.123.

Neigel, A., Claypoole, V., Waldfogle, G., Acharya, S., & Hancock, G. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92(5). DOI: 10.1016/j.cose.2020.101731.

Norton Rose Fulbright. (2016). Dealing with a data breach: Key takeaways from the Home Depot class action. *Norton Rose Fulbright*. https://tinyurl.com/2ndbz9y2

Patel, K. (n.d.). Top 11 ways poor cyber security can harm you. *GreenGeeks*. https://www.greengeeks.com/blog/top-11-ways-poor-cyber-security-can-harm-you/

Personal Information Protection Act, RSA 2003, c. P-6.5. https://open.alberta.ca/publications/p06p5

Personal Information Protection and Electronic Documents Act, SC 2000, c.5. https://www.laws-lois.justice.gc.ca/eng/acts/P-8.6/

Pop, I-A. (2022). Prevention of computer crime through knowledge of the concept of cyber security. *International Journal of Legal and Social Order*, 1. DOI: 10.55516/ijlso.v1i1.83.

Powell, O. (2022, December 27). The most dangerous cyber security threats of 2023. *Cyber Security Hub*. https://www.cshub.com/attacks/articles/the-most-dangerous-cyber-security-threats-of-2023

Royal Canadian Mounted Police. (2022). Canadian Anti-Fraud Centre annual report 2021. *Government of Canada*. https://publications.gc.ca/collections/collection_2022/grc-rcmp/PS61-46-2021-eng.pdf

Sarah. (2017, September 22). Don't blame your employees when you're phished in. *Make IT Work*. https://makeitworkcomputersolutions.ca/dont-blame-your-employees-when-youre-phished-in/

Sjouwerman, S. (2022, March 30). A lack of employee cyber hygiene is the next big threat. *KnowBe4*. https://blog.knowbe4.com/lack-of-employee-cyber-hygiene-next-big-threat

Solomon, H. (2023, February 22). Phishing still the leading way attackers breach security controls: IBM. *ITBusiness.ca*. https://tinyurl.com/4b797z7x

Verizon. (2022). Data breach investigations report. *Verizon*. https://www.verizon.com/business/resources/T245/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128. DOI: 10.1016/j.dss.2019.113160.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basım, N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*. 62. 82-97. DOI: 10.1080/08874417.2020.1712269.

Zwilling, M., Lesjak, D., Natek, S., Phusavat, K., & Anussornnitisarn, P. (2019). How to deal with the awareness of cyber hazards and security in (higher) education?. *ResearchGate*. https://tinyurl.com/3zfduycn