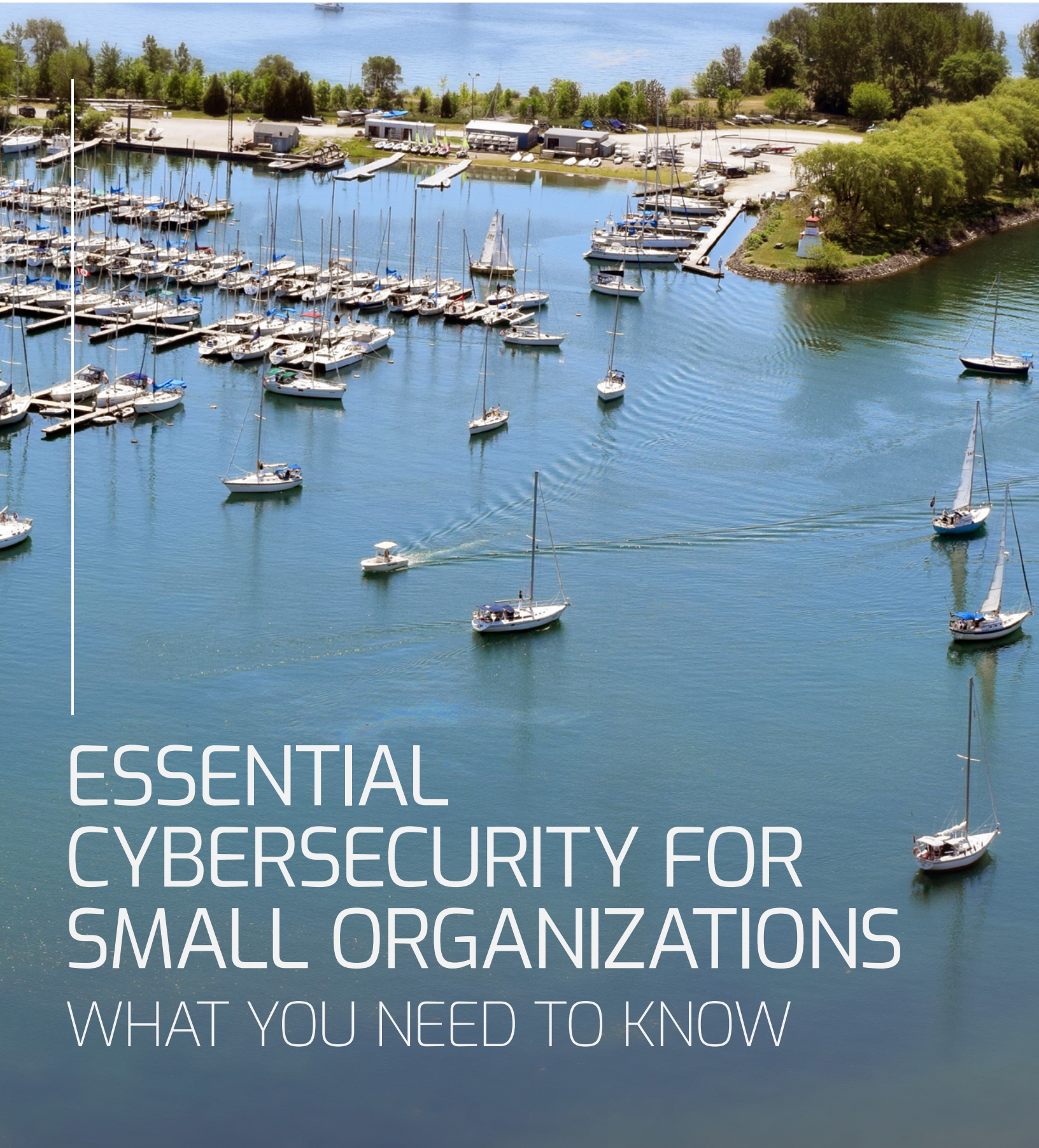
NORD OUVERT OPEN NORTH



ESSENTIAL CYBERSECURITY FOR SMALL ORGANIZATIONS

WHAT YOU NEED TO KNOW

ACKNOWLEDGMENTS

Recommended Citation

Open North. 2025. "Essential Cybersecurity for Small Organizations: What you need to know." Open North.

Attribution

Disclaimer

If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work by Open North. The views and opinions expressed in the adaptation are the sole responsibility of the author and the adaptation is not endorsed by Open North.*

Author

Open North

To learn more about the research that went into this guide please contact info@opennorth.ca.

Acknowledgements

This guide was produced thanks to the contributions of the following current and former Open North staff and advisors: Merlin Chatwin, PhD; Jérémy Diaz, PhD; Judith François-Langevin; John Griffin; Christian Medina; Tona Mutimura; and Cristiano Therrien, PhD.

Cover image: Kelly O'Connor

CONTENTS

Cybersecurity is an increasingly important consideration for small and medium organizations (SMOs). The rapid pace of digitalization, a push for automation in business and operational processes, and the exponential growth of data and artificial intelligence means that new cybersecurity risks emerge constantly for all organizations. Many SMOs are limited to reacting to these risks and often scramble to adapt strategies to address them. In response, Open North developed this guide for SMOs to proactively engage with cybersecurity best practice. Ultimately, Open North's objective is to ensure that organizational data and operational environments, regardless of an organization's size, capacity or resources, are secure and protected from cyberattacks.

This guide provides an introduction to cybersecurity concepts, frameworks and the current security landscape in Canada. This introduction includes the specific risks and consequences associated with SMOs due to their operating environment, size and capacity constraints. Next, the guide introduces legislation and expectations for SMOs in Canada to comply with various data protection regulations and laws, and the consequences of failure to do so. Finally, the guide discusses initial first steps to implement cybersecurity measures and mitigate risks at the organizational level. The guide includes checklists and tools for SMOs to start engaging in cybersecurity practice and to better prepare for implementation of risk mitigation.

Implementing robust cybersecurity measures, however, such as regular security assessments, employee training, and advanced threat detection, is crucial to safeguarding organizational operations, data, and reputation, and require an ongoing commitment to maintain organizational practices, procedures and culture.

Beyond this guide, Open North is able to support organizations seeking to protect their data and operations through its different service offerings including:

1. Risk assessments that enable partners to better understand the depth and weight of current cybersecurity controls and identify gaps and existing deficiencies,
2. Cybersecurity plan development to define realistic goals, and prioritize bespoke actions aligned with specific organization needs.
3. Targeted implementation support to ensure there is increased security in an organization's data environment through updated policies and standards, secure tools, audits, tested procedures for threat detection and response, and training to equip staff to handle current and future threats.

To find out more about Open North's service offering please follow this link or contact us info@opennorth.ca.

WHAT IS CYBERSECURITY AND HOW DOES IT AFFECT YOUR ORGANIZATION?

Cybersecurity can be defined as "any technology, measure or practice for preventing cyberattacks or mitigating their impact."[1] As such, cybersecurity goals and objectives are to protect an organization's confidentiality, integrity, and availability. When all three components are adequately addressed by an organization, the organization is better situated to mitigate cybersecurity threats.

In Canada, small and medium organizations (SMOs) often underestimate the **cybersecurity vulnerabilities** within their organization. Indeed, the Canadian Chamber of Commerce estimates **43% of cyberattacks target small and medium businesses**,[2] with many of them struggling to recover from cyberattacks that disrupt their operations, leading to significant costs. Not-for-profit organizations are not immune from cyberattacks either, with 59% of Canadian not-for-profits reported fraud or scams like phishing[3] in 2023. The impact of these attacks can be severe, with 27% of affected organizations reporting that cybersecurity incidents prevented the use of essential resources or services.[4] These vulnerabilities are troubling because not-for-profits often handle sensitive personal data, but typically have fewer resources to defend against cyberthreats.

The consequences of a cybersecurity incident, such as the disclosure of sensitive data, can be devastating for SMOs, including not-for-profit organizations. Beyond immediate operational disruptions, financial loss and possible penalties, a cybersecurity incident can cause reputational damage. Although these consequences are true for organizations across the board, SMOs are particularly susceptible. Given their size and operating environment, these organizations often rely on trust and close relationships with key partners, stakeholders and clients. Damage to their reputation can be an existential blow - devastating funding relations, straining revenue streams and affecting future operations.

Elements related to IT, privacy, security and data interact to ensure the safety and security of information. Some of these aspects are outside of the direct control of individuals. New security threats emerge and evolve continuously. IT software and hardware are built by a myriad of companies and actors in fragmented and uncoordinated environments. Malicious actors aim at exploiting vulnerabilities to access private personal information to gain leverage and/or monetary rewards.

(1) *"What is Cybersecurity" (Lindemulder, Kosinski, 2024)*

(2) *"A Roadmap to Fortifying the Digital Future of Small Business in Canada"(Hewie, 2023)*

(3) Phishing is "a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person." - *An Introduction to Computer Security: The NIST Handbook (NIST, 2017)*

(4) CICP-PCPOB Weekly Report- Rapport Hebdomadaire No. 2.6.20 (CICP-PCPOB, 2024)

Worryingly, SMOs are exposed and underprepared to face the worst impacts of cyberthreats. SMOs often underestimate the impact that cybersecurity can have on their organization due to lack of resources and a dedicated IT security team. In addition, SMOs often have outdated or insufficiently secured systems to address cyber threats. In a recent effort to further understand this issue, The Canadian Centre for Nonprofit Digital Resilience (CCNDR) worked closely with around 50 organizations from across Canada. CCNDR led-working groups found that organizations face multiple constraints to address cybersecurity risks - from awareness of the issue to lack of funding.[5] Particularly concerning was a misalignment of scale when it came to guidance provided by leading organizations and respected standards in cybersecurity. For example, widely used cybersecurity standards such as those created and maintained by the US-based National Institute of Standards and Technology (NIST) are designed for large organizations and governments. Even standards designed specifically for "small" and "medium" sized organizations might not be a proper fit. The Canadian Digital Governance Standards Institute's (DGSI) *Baseline Cyber Security Controls for Small and Medium Organizations* standard is designed for an audience of "up to 500 or less employees."[6] Though useful for many, our experience at Open North has shown that there are significant differences in needs, capacity and funding between a front-line service providing organization of 10 staff, and a small enterprise with multiple locations and staff of hundreds, for example. Right-sizing standards and guides is necessary to maximize the usefulness and impact of recommendations and actions.

(5) Building The Cybersecurity And Resilience Of Canada's Nonprofit Sector (Canadian Centre for Nonprofit Resilience, 2023)

(6) "DGSI Publishes New Revision of CAN/DGSI 104: Baseline Cyber Security Controls for SMEs" (Digital Governance Standards Institute. 2024)

Did you know?

- In a 2024 survey,[7] the Canadian Internet Registration Authority (CIRA) reported that 44% of Canadian organizations faced a cyber attack in the last 12 months;
- In a recent assessment, the Canadian Centre for Cyber Security states that the global number of ransomware incidents rose 74% in 2023 compared with 2022, and the average ransom paid in Canada in 2023 was $1.130mi CAD;[8]
- In 2023, only 14% of small not-for-profits provided cybersecurity training to their staff, and only 7% of small nonprofits and 15% of medium-sized ones said they were aware of the existence of cybersecurity standards.[9]
- By 2023, recovery costs from cyber incidents had doubled since 2021,[10] highlighting the rising need for cybersecurity preparedness in Canadian organizations;
- Cybersecurity threats are growing every year, even hitting large Canadian public organizations, such as municipalities and hospitals, that have greater resources to protect themselves.[11]
- Despite the increased threat, almost half (47%) of Canadian small businesses surveyed conducted on behalf of the Insurance Bureau of Canada (IBC)[12] say they do not allocate any portion of their annual operating budget to cyber security;
- A recent report by Policy Horizons Canada[13] underscores the cyber security risks posed by AI-generated disinformation;
- In 2022, a survey revealed that 63%[14] of Canadian small and medium business experienced at least one cyberattack, highlighting the widespread nature of these threats;
- This survey also shows that 81% of small and medium businesses see artificial intelligence as a tool that could strengthen their cybersecurity but also enable new forms of cyberattacks.

(7) 2024 CIRA Cybersecurity Survey *(CIRA, 2024)*

(8) National Cyber Threat Assessment 2025-2026 *(Canadian Centre for Cyber Security, 2024)*

(9) What Newly Available Data Tell Us About Cybersecurity in Canadian Nonprofits (Shim and Barr, 2024)

(10) "Impact of Cybercrime on Canadian Businesses" *(Statistics Canada, 2024)*

(11) As We Enter 2024, Cyberthreats to Canada Are Growing (Hilt, 2023)

(12) "Many small businesses vulnerable to cyber attacks" (IBC, 2021)

(13) Disruptions on the Horizon (Policy Horizons Canada, 2024)

(14) *"Cybercrime strikes more than six in 10 Quebec companies" (KPMG, 2023)*

Leaders in different organizations can make decisions around security and protecting data and technology systems (from planning to implementation and long-term maintenance) that determine whether systems are useful and whether they support needs and objectives. In addition, external controls imposed by authorities, and standards promoted by organizations, such as the aforementioned NIST Cybersecurity Framework, can both change the threat environment an organization operates in and influence organizational decision making. For example, required standards enforced by legislation - such as Quebec's Law 25 on privacy, also reduce cybersecurity threats. Law 25 requires personal private information to be handled with minimum standards to protect unauthorized access, leading organizations to seek ways to protect this information.

Understanding the threat environment and possible external controls in the forms of legislation or standards is a minimum first step to cybersecurity. Leaders need to understand existing practices and controls (both internal and external) in areas of IT, privacy, security and data management. Changes in legislation, global business environments, political interests, legal and court decisions and a myriad of other external factors shape the way different interconnected elements of cybersecurity are implemented by organizations. For example, overreliance on US-based firms and software companies might increase risk as these face increased pressure and influence by the Trump administration to release data and information on foreign individuals, organizations or activities.[15] Gold standards such as NIST are updated and supported by the US Department of Commerce, and, as such, could be at risk of being affected by US political decisions, influenced by private-narrow interests of big-tech or the current drive to reduce US government bureaucracy.

As such, this guide is meant to complement existing efforts, and help small and medium sized organizations that fall outside of current targeted support on offer. The objective is to adapt to the reality of cybersecurity risks and resource constraints specific to SMOs. Furthermore, this guide and Open North service offering responds to calls for a stronger, resilient and safe Canadian landscape, where all organizations, regardless of size are able to respond and prevent cyberthreats.

(15) "IRS and ICE Reach Deal to Share Data on Undocumented Immigrants." *(The Guardian, 2025)*

In depth: The CIA triad of cybersecurity

Term	Definition
Confidentiality	**Protecting the confidentiality of information in an organization** Ensuring sensitive business information is only accessible to authorized people through: • Access control (right people, right information) • Data encryption • Clear policies for the use of personal devices • Regular security awareness training
Integrity	**Protecting the integrity of information where the data in use is authentic, free of any tampering, accurate, and reliable** Maintaining the accuracy and trustworthiness of your organization's data through: • Protection against unauthorized changes • Regular data audits to verify the authenticity • Routine verification of data accuracy • Systematic backup procedures with integrity checks
Availability	**Ensuring systems and data are accessible when needed by authorized users** Making data available to authorized users requires: • Regular system updates and maintenance • Comprehensive backup strategy (onsite and offsite) • Protection against service disruptions • Safeguards against ransomware

Cybersecurity compliance, expectations and the law

If your organization collects, uses, or discloses personal information in Canada, you may be required to take steps to protect data through cybersecurity measures. Depending on the jurisdiction, small and medium sized organizations have a legal obligation to comply with both explicit requirements and different expectations set forth in Provincial and Federal privacy legislation. Laws like the Personal Information Protection and Electronic Documents Act (PIPEDA) mentions that "(p)ersonal information shall be protected by security safeguards appropriate to the sensitivity of the information".[16]

In short, data privacy and cybersecurity go hand in hand. Failure to comply can result in penalties, financial losses, and reputational damage.

Key Canadian privacy laws

PIPEDA (Personal Information Protection and Electronic Documents Act) is the main federal privacy law that requires organizations to:

- Protect personal information with appropriate security safeguards
- Obtain consent before collecting, using or disclosing personal information
- Report significant data breaches to affected individuals and authorities[17]
- Organizations can face fines of up to $100,000 for PIPEDA violations

Alberta, British Columbia and Quebec have their own private-sector privacy laws that have been deemed substantially similar to PIPEDA. Organizations that are subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use, or disclosure of personal information that occurs within that province.

Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have also adopted substantially similar legislation regarding the collection, use, and disclosure of personal health information.

Although PIPEDA applies to organizations engaging in commercial activities - the Canadian Bar Association mentions that "not-for-profit organizations are not automatically exempt from PIPEDA. The fact that an organization is non-profit for purposes of taxation does not determine whether its collection, use or disclosure of personal information is carried out in the course of commercial activity." [18]

(16) Government of Canada. (2000). Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, 4.7 Principle 7 – Safeguards https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html

(17) *"What you need to know about mandatory reporting of breaches of security safeguards" (Office of the Privacy Commissioner of Canada)*

(18) Canadian Bar Association. (2023). Why charities and not-for-profits should comply with PIPEDA. Retrieved from https://www.cba.org/sections/charities-and-not-for-profit-law/member-articles/why-charities-and-not-for-profits-should-comply-with-pipeda/#edn9

If your organization is in Québec or deals with data of Quebec residents:

- Québec's Privacy Act with fines up to $10M for non-compliance
- Requires explicit opt-in consent for any tracking technologies
- Mandates appointment of privacy officer and privacy impact assessments

If your organization is in British Columbia (BC) or deals with data of BC residents:

- BC's Personal Information Protection Act (PIPA) with fines up to $100,000 for noncompliance
- Applies to any *private* organization collecting personal data of BC residents
- Requires organizations to protect personal information against unauthorized use

If your organization is in Alberta or deals with data of Alberta residents:

- Alberta's PIPA fines could cost up to $100,000 for violations
- Regulates all *private* sector organizations processing Alberta resident data
- Requires reasonable purpose and limited collection of personal information

Additional examples of regulations

Your organization might also need to comply with:

- CASL - Canada's Anti-Spam Legislation
  - Applies to organizations sending commercial electronic messages
  - Fines up to $10M for organizations and $1M for individuals for noncompliance
- Québec's Bill 3 - Act respecting health and social services information (HSSI)
  - Applies to organizations providing HSSI in Quebec
  - Fines up to $150,000 for first offense (doubling and tripling in the next ones)
- Ontarios's PHIPA - Personal Health Information Protection Act
  - Applies to health data custodians handling personal health information
  - Fines up to $200,000 for individuals and $1M for organizations

Protecting your organization

To ensure legal compliance, consider:

- Appointing a privacy officer from a legal, IT, or operational background
- Implementing a comprehensive privacy and cybersecurity legal compliance audit
- Staff training on privacy and cybersecurity risk management

WHAT CAN MY ORGANIZATION DO TO PROTECT AGAINST CYBERSECURITY THREATS?

As mentioned, SMOs face unique challenges often overlooked in cybersecurity frameworks designed for large enterprises, government and the private sector. This limited available cybersecurity guidance, expertise and resources that are bespoke to SMOs operational environment makes them prone to becoming prime targets for threat actors. Recognizing this gap, this section summarizes first steps SMOs can take to protect themselves against cybersecurity threats. Based on Open North's experience working with SMOs, this section includes appropriate tools for leaders at these organizations to use. Finally, the section includes common discussions that emerge once SMOs engage in cybersecurity practice. Although the chosen topics are not exhaustive of the doubts and questions that Open North has encountered, the guide includes initial recommendations and contextual knowledge to illustrate some of the unique challenges and considerations SMOs face.

Tool: Cybersecurity self-assessment checklist

Implementing cybersecurity best practices is complex and each threat environment is uniquely challenging. As a first step, Open North created the below checklist to enable an initial self-assessment of key cybersecurity risk areas and the best practices to mitigate them. Generally speaking, completing the self-assessment will assist your organization in seeking further guidance to improve your security posture.

Organizational awareness and training

- [ ] Does the organization provide updated training to employees related to anti-phishing and social engineering, and have policies and procedures in place if these attacks were to happen?
- [ ] Does the organization provide guidance and recommendations on password policies, and access to cloud services, software, and hardware?
- [ ] Does the organization provide onboarding training to new staff and annual training on recognizing and avoiding phishing attacks?
- [ ] Does the organization train staff on how to effectively report suspected or confirmed cyber breaches and phishing attacks?
- [ ] Does the organization provide ongoing awareness building of existing policies and procedures to ensure staff know what is expected of them?
- [ ] Does the organization provide specialized training for technical staff (ie. IT, HR)?

Hardware/software inventory

- [ ] Does the organization have a detailed hardware and software asset register and procedures for ensuring it is up-to-date?
- [ ] Does the organization create an inventory of the data it holds and its respective access points that would allow proper system access restrictions implementation?
- [ ] Does the organization have policies and procedures for new software procurement and installation?
- [ ] Does the organization have an off-boarding checklist for technology assets held by employees, including access controls, password changes, hardware return, and wiping procedures?
- [ ] Does the organization allocate an annual budget for technology upgrades?
- [ ] Does the organization have procedures to assess its technology assets?

Data management

- [ ] Does the organization have data governance policies covering collection, retention, and disposal?
- [ ] Does the organization have policies, procedures, and protocols in place for data backup to prevent data loss and allow for timely recovery?
- [ ] Is the organization communicating consent regarding data in research activities and standardized across different research projects, particularly as it pertains to data that might/could be used for purposes other than research?
- [ ] Does your organization implement access controls around sensitive information within the organization? If so, are these access controls being monitored and reviewed, and at what frequency.

Security assets and practices

- [ ] Does the organization have an in-house team or external IT support?
- [ ] If the organization has employees working from home, does it have a remote work-from-home policy in alignment with cybersecurity best practices?
- [ ] Does the organization have policies and security procedures for personal devices (like phones, tablets, or home computers) when employees use them to access work email, cloud services, or other organizational systems?
- [ ] Does the organization encrypt devices within the organization, such as laptops?
- [ ] Does the organization ensure all staff use secure VPN connections when working outside the office, and do you set this up for both new and current employees?
- [ ] Does the organization automate updates on security defenses for hardware?
- [ ] Does the organization use cloud services, and if so, are laptops configured to send working files to the cloud automatically?

- [ ] Does the organization have a password manager to secure accounts used across the organization?
- [ ] Does the organization require two-factor authentication (2FA) on mobile devices alongside password managers to reduce the risk of unauthorized access?

Legal compliance

- [ ] Does the organization assign "compliance officer stewardship" responsibilities and accountabilities to existing organizations' leadership (which include management and board roles)? "Compliance officers stewardship" means individuals who are making decisions about how the organization should comply with determined requirements.
- [ ] Does the organization review any relevant privacy compliance legislation regularly to ensure that the organization is following guidelines and best practices put out by relevant authorities, even if not necessarily required by law?
- [ ] Does your organization have privacy compliance policies, procedures, and third-party management implemented within the organization?

Breach response preparedness

- [ ] Does the organization have a comprehensive cybersecurity breach response plan readily accessible to key personnel?
- [ ] Does the organization have a crisis communication plan in place in case of a breach incident or any type of cyberattack?

Vendor management

- [ ] Does the organization review current and future agreements signed with third-party technology providers as they pertain to the organization's own policies?
- [ ] Does the organization ensure external marketing/website vendors access restrictions with website hosting providers to ensure email addresses cannot be controlled or shared by the marketing organizations?
- [ ] Does the organization require security service providers to notify you about significant changes - for example, if your VPN provider is bought by another company that might have different privacy and security policies?

Working through the above checklist helps SMOs understand current cybersecurity strengths and weaknesses without requiring external expertise. As mentioned, understanding possible controls to threats is a first step. We strongly recommend seeking further guidance to identify potential cybersecurity threats, prioritize actions and implement appropriate controls.

Cybersecurity audits

An organization might choose to conduct a cybersecurity *audit* with the help of experts. An audit provides an independent, detailed verification of your security measures against specific standards, which could be defined by your organization's policies, industry best practices, and/or legal requirements. The need to conduct a cybersecurity audit might stem from external pressures, such as a grant or partnership requirement (which might necessitate following a particular set of specifications and parameters set by an external actor), or it might be an internal decision driven by a specific business or an organizational purpose. An audit, its associated costs (including financial, staff effort, and other organizational resources) have to be balanced by its potential organizational and strategic benefit on a case by case basis.

On the other hand, an assessment offers a broader view of organizational cybersecurity practice, gaps and existing risks. A cybersecurity assessment is a crucial step in identifying and addressing vulnerabilities that put an organization's data and operations at risk. An assessment can provide base-line knowledge, understanding and a clear line of sight to practices, policies and organizational functions (such as IT and HR) as they pertain to cybersecurity. Leaders and managers at SMO's should choose based on their specific needs: if you need a comprehensive, independent review of your security compliance, an external audit is more appropriate; if you want to understand and improve your overall security position with more flexibility, an assessment might be the better choice. Organizations can always begin at a cybersecurity assessment and make an informed decision about whether an audit is a necessary and beneficial next step. If your organization chooses to pursue an audit, a prior assessment process using a risk matrix is recommended, whether conducted with internal or external resources.

Aspect	Cybersecurity audit	Cybersecurity assessment
Purpose	Verifies compliance with specific security standards and evaluates the effectiveness of existing controls	Provides a high-level analysis of overall security health and identifies weaknesses
Description	Detailed examination of security controls, policies, and procedures against specific framework requirements (e.g., PIPEDA, Law 25)	Broad evaluation of security maturity and effectiveness of controls, focusing on identifying vulnerabilities and risks
Outcome	Produces a compliance snapshot and detailed report of gaps in security controls, with specific recommendations for meeting standards	Delivers insights about security risks, prioritized vulnerabilities, and recommendations for improving overall cybersecurity practices

Tool: Cybersecurity preparatory documents

Whether an organization chooses to do an audit or an assessment, leadership and management will need to collect documentation and information on existing practices related to data, IT and security. This preparatory work helps guide and narrow down the scope of cybersecurity needs and priorities before engaging further. Whether an organization's cybersecurity journey is in the context of a specific audit process or in other forms of improving organizational cybersecurity, Open North has put together this guide of the most common documents to gather in preparation for this journey.

Asset and documentation management

- [ ] Locate the asset management inventory - including hardware, software and data storage locations. Note the date it was last updated.
- [ ] Locate all written security procedures and note the date they were each individually updated.
- [ ] Locate the registry for previous cybersecurity incidents and how they were handled.
- [ ] Locate documentation on the identified data, software, and physical assets that are critical to the organization. Examples would be financial or customer data, business-critical applications and data servers.

Policy framework

- [ ] Locate the organizational policy and guidelines related to security, risk appetite/tolerance and cybersecurity strategy.
- [ ] Identify best practices and standards used for creating cybersecurity policies (ie. ISO or NIST)
- [ ] Locate policy for system access permission granting and removal for staff hiring and termination.

Infrastructure

- [ ] Locate organizational guidance and recommendations on password policies, accessing cloud services, software and hardware.
- [ ] If your organization uses cloud services, document laptop configuration and automations for saving and backup.

Team readiness

- [ ] Locate most up-to-date maps of how the organizations IT network is set up.
- [ ] Locate documentation of privileged users and systems administrators.

Risk management

- [ ] Locate documentation of known security problems and plans to fix them.
- [ ] Locate plans for mitigating security risks.

Privacy compliance

- [ ] Document which privacy laws apply to your operations and how your organization records compliance.
- [ ] Locate any findings from previous privacy reviews and how issues were addressed.

Incident response

- [ ] Locate step-by-step plan for handling cybersecurity incidents and any documented practices for responding.

Training and documentation

- [ ] Locate records on staff cyber security training sessions, including specialized training for technical staff.
- [ ] Gather examples of communication that informs staff about cybersecurity.

Third-party assurance

Today's organizations increasingly rely on external service providers for essential operations - from storing data in the cloud to managing emails and customer information. While these services are necessary for most organizations, they can also create security risks. One security incident at your service provider could directly impact your organization's reputation, operations and data.

Why should you care about service provider security?

- Your organization's data and operations depend on these providers
- You are responsible for protecting your data, even when it's in someone else's hands

What are security assurance reports?

Service providers like Microsoft, Amazon, or your local IT company should be able to prove their security measures through independent security assessments. These assessments result in standardized reports that you can request and review:

- SOC 2 Reports: An internationally recognized standard of security controls
- CSAE 3000: A Canadian standard that evaluates security measures

These reports check five key areas that are vital for the operations of your organization: security, availability, processing integrity, confidentiality, and privacy.

Practical tips

- When choosing new service providers, ask if they have SOC 2 or CSAE 3000 reports
- Include the requirement for these security reports in your service contracts
- Review these reports annually or when renewing contracts
- Keep in mind that providers might charge extra for these reports due to their cost

Remember: Your organization can't directly control or inspect large service providers like Microsoft or Amazon. That's why these **independent security reports are crucial** - they give you assurance that your providers are maintaining proper security measures.

GET STARTED TODAY!

Now it's time to put cybersecurity measures into action in your organization. Here are some **extra resources that can support** your organization.

Relevant service offerings in cybersecurity

Our services provide an in-depth view of your organization's data capacities and readiness for further transformation. The suggested assessments use industry standards and benchmarks to measure performance and highlight areas for improvement.

Data capacity assessment

We evaluate how well your organization is managing its data, from collection and storage to quality management and governance, providing a roadmap to improve your data capabilities.

Privacy compliance assessment

We conduct a comprehensive privacy risk assessment and provide recommendations for improving your organization's compliance with relevant data privacy regulations.

Cybersecurity assessment

We assess your cybersecurity defenses, helping you identify vulnerabilities and build a stronger defense against cyber threats.

About Open North service offerings

Our wider services help governments and civic-minded organizations of all sizes to build their capacity to manage their data, ensuring it is useful, actionable, secure, and trustworthy throughout its entire lifecycle. Our core areas of expertise are:

Data management

Supporting effective and strategic use and sharing of data across your organization.

Cybersecurity

Supporting the confidentiality, integrity and availability of your organization's data.

Privacy compliance

Establishing compliance with regulatory standards for data privacy.

Data hub development

Supporting inter-organizational data sharing and collaboration through governance models and digital infrastructure.

Contact us today to learn how we can help your organization.

Email us at info@opennorth.ca

Visit our website: opennorth.ca

Essential Cybersecurity for Small Organizations