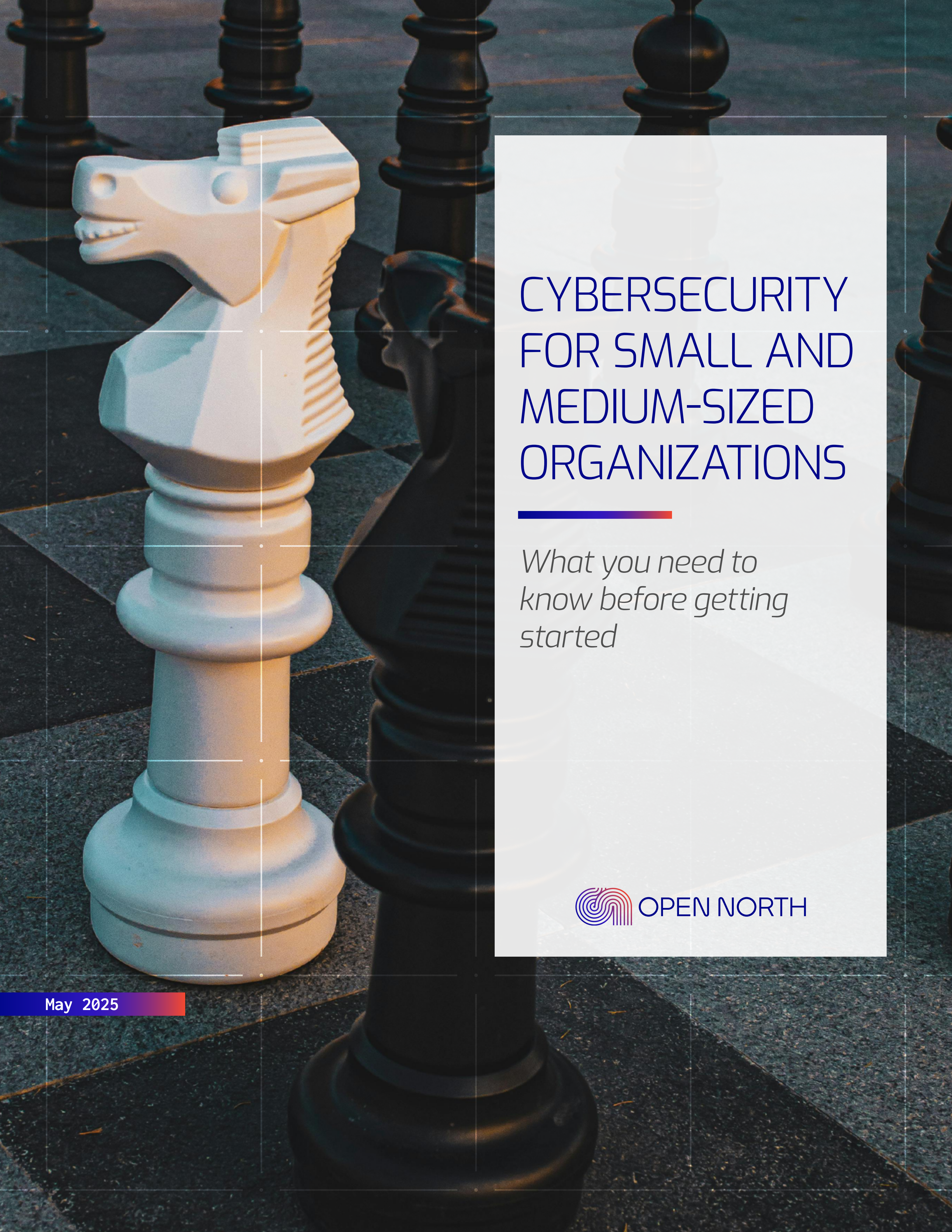


CYBERSECURITY FOR SMALL AND MEDIUM-SIZED ORGANIZATIONS

What you need to know before getting started

OPEN NORTH

May 2025

CONTENTS

WHY SHOULD YOUR ORGANIZATION PROTECT ITSELF AGAINST THREATS?

Understanding the main threats: It can happen to you, just like any other organization!

When it comes to Canada, according to the Canadian Chamber of Commerce, small and medium businesses (SMBs) often underestimate the **cybersecurity vulnerabilities** within their organization. In fact, **43% of cyberattacks target SMBs**,[1] with many of them struggling to recover from cyberattacks that disrupt their operations and can lead to major costs.

When it comes to not-for-profit organizations (NPOs), **59% of Canadian NPOs reported fraud or scams**, such as phishing, in 2023. The impact of these attacks can be severe, with 27% of affected NPOs reporting that cybersecurity incidents prevented the use of essential resources or services.[2] These vulnerabilities are concerning because **NPOs often handle sensitive personal data**, but typically have fewer resources to defend themselves against cyber threats.

In this guide, the term "Small and Medium-sized Organizations" (SMOs) refers to both SMBs and NPOs.

Small and Medium-sized Organizations (SMOs) are increasingly exposed to cyberattacks. SMOs often underestimate the impact that cybersecurity can have on the organization. They lack the resources and a dedicated IT security team, and have outdated or insufficiently secured systems to address cyber threats. This guide exists to help your SMO in aligning your cybersecurity strategy with the specific risks and resources of your organization.

[1] "A Roadmap to Fortifying the Digital Future of Small Business in Canada"(Hewie, 2023)

[2] CICP-PCPOB Weekly Report- Rapport Hebdomadaire No. 2.6.20 (CICP-PCPOB, 2024)

Not yet convinced of the importance of cybersecurity?

Let’s look at some statistics:

- In a 2024 survey,[3] 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 reported a 74% increase in global ransomware incidents in 2023 compared to 2022, with the average ransom paid in Canada amounting to $1.13 million CAD in 2023;[4]
- In 2023, only 14% of small nonprofits provided cybersecurity training to their staff. Only 7% of small nonprofits and 15% of medium-sized ones said they were aware of the existence of cybersecurity standards;[5]
- By 2023, recovery costs from cyber incidents had doubled since 2021,[6] highlighting the rising need for cybersecurity preparedness in Canadian organizations;
- Cybersecurity threats continue to grow each year, impacting even large Canadian public organizations that possess greater resources for protection;[7]
- Despite the growing threat, nearly half (47%) of Canadian small businesses surveyed on behalf of the Insurance Bureau of Canada (IBC) reported allocating no portion of their annual operating budget to cybersecurity;[8]
- Despite the fact that 95% of cyber attacks are caused by human error,[9] 57% of small businesses in Canada still don’t provide cybersecurity training;[10]
- A recent report by Policy Horizons Canada[11] underscores the cybersecurity risks posed by AI-generated disinformation;
- In 2022, a survey revealed that 63%[12] of Canadian SMBs experienced at least one cyberattack, highlighting the widespread nature of these threats;
- This survey also shows that 81% of SMBs see artificial intelligence as a tool that could strengthen their cybersecurity, but also enable new forms of cyberattacks.

[3] 2024 CIRA Cybersecurity Survey (CIRA, 2024)

[4] National Cyber Threat Assessment 2025-2026 (Canadian Centre for Cyber Security, 2024)

[5] What Data Tell Us About Cybersecurity in Canadian Nonprofits (Shim and Barr, 2024)

[6] “Impact of Cybercrime on Canadian Businesses” (Statistics Canada, 2024)

[7] As We Enter 2024, Cyberthreats to Canada Are Growing (Hilt, 2023)

[8] “Many small businesses vulnerable to cyber attacks” (IBC, 2021)

[9] The Global Risks Report 2022 (World Economic Forum)

[10] Cyber Attacks: Not a matter of if, but when - and what’s next? (Mastercard)

[11] Disruptions on the Horizon (Policy Horizons Canada, 2024)

[12] “Cybercrime strikes more than six in 10 Quebec companies” (KPMG, 2023)

What is cybersecurity? The CIA triad and its role in protecting your organization

Cybersecurity is defined as “any technology, measure or practice designed to prevent cyberattacks or mitigate their impact.”[13] Its primary objectives are centered around safeguarding **the components of the CIA triad: Confidentiality, Integrity, and Availability.**[14]

When all three components are adequately addressed, an organization is better situated to mitigate cybersecurity threats. Each component is defined as follows:

TERM	DEFINITION
Confidentiality	**Protecting the confidentiality of information in an organization** Ensuring that sensitive business information is only accessible to authorized people is crucial. Think of it as keeping your organization's secrets safe through: ▪ Access control (right people, right information); ▪ Data encryption; ▪ Clear policies for the use of personal devices; ▪ Regular security awareness training.
Integrity	**Guaranteeing data integrity by ensuring the information used 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.

[13] “What is Cybersecurity” (Lindemulder, Kosinski, 2024)

[14] “What is the CIA Triad?”(Fortinet)

Understanding these core principles of cybersecurity - Confidentiality, Integrity, and Availability - is essential as **they constitute the foundation of regulatory requirements and compliance standards**. Next, we will examine the specific legal obligations in Canada that may apply to your organization regarding data and systems protection.

Is cybersecurity a legal requirement for my organization?

Yes! If your organization collects, uses, or discloses personal information in Canada, you have legal obligations to protect it. **Data privacy and cybersecurity go hand in hand.** Failure to comply can result in severe penalties, financial losses, and reputational damage.

Key Canadian privacy laws

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

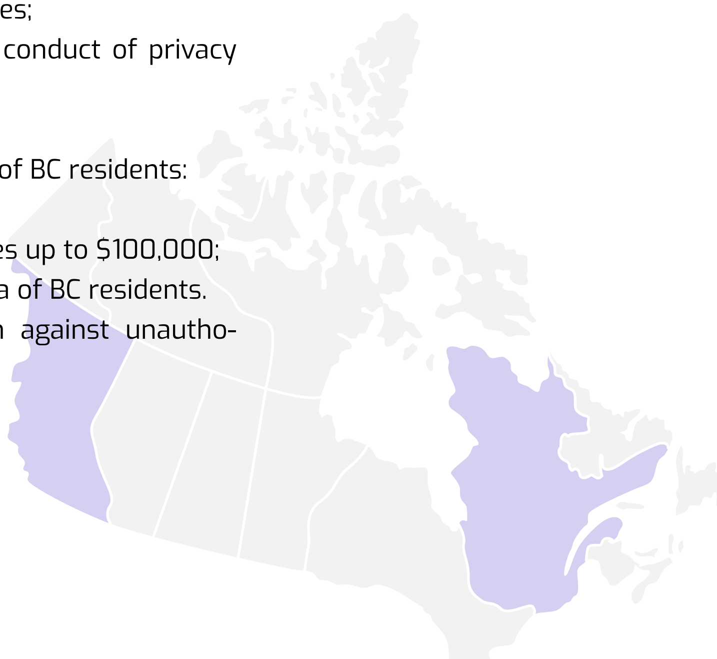
- Protect personal information with appropriate security safeguards;
- Obtain consent before collecting, using or disclosing personal information;
- Report significant data breaches to affected individuals and authorities;[15]
- Organizations can face fines of up to $100,000 for PIPEDA violations.

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

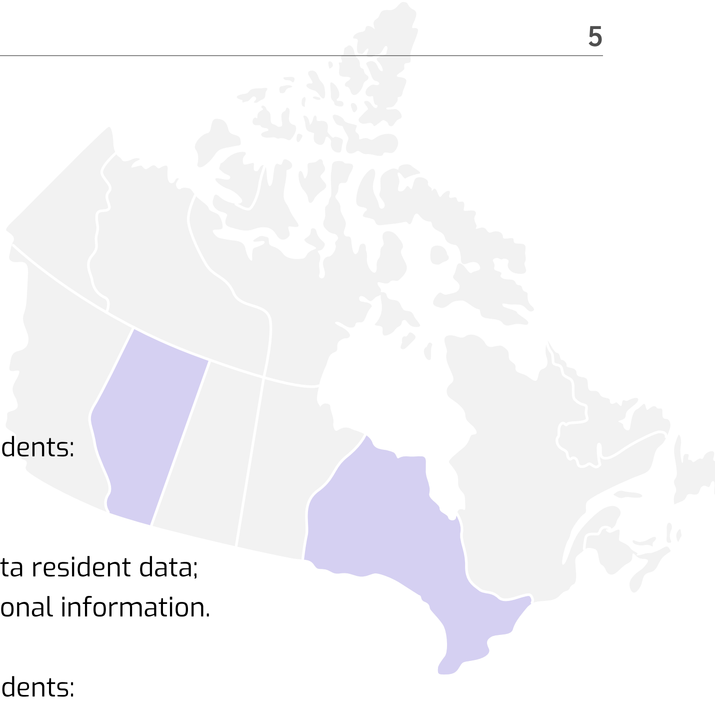
- Québec's Privacy Act (Law 25) imposes fines up to $10 million for non-compliance;
- It requires explicit opt-in consent for any tracking technologies;
- It mandates the appointment of a privacy officer and the conduct of privacy impact assessments.

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

- BC's Personal Information Protection Act (PIPA) imposes fines up to $100,000;
- It applies to any private organization collecting personal data of BC residents.
- It requires organizations to protect personal information against unauthorized use.



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



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;
- It regulates all private sector organizations processing Alberta resident data;
- It requires reasonable purpose and limited collection of personal information.

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

- Recent FIPPA amendments apply to Ontario provincial public sector institutions;
- It requires mandatory Privacy Impact Assessments before collecting personal data;
- It mandates breach reporting when there is real risk of significant harm.

Additional regulations

Your organization may also need to comply with:

- CASL - Canada's Anti-Spam Legislation:
  - Applies to organizations sending commercial electronic messages;
  - CASL imposes fines up to $10 million for organizations and $1 million for individuals.
- Other provincial health information laws with privacy requirements and major fines;
  - Québec's Act respecting health and social services information (Bill 3);
  - Ontarios's Personal Health Information Protection Act (PHIPA);
  - New Brunswick's Personal Health Information Privacy and Access Act;
  - Newfoundland and Labrador's Personal Health Information Act;
  - Nova Scotia's Personal Health Information Act.

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;
- Training staff members on privacy and cybersecurity risk management.

HOW CAN MY ORGANIZATION MITIGATE CYBERSECURITY THREATS?

What you can do right now, without external help

Often overlooked in frameworks designed for large enterprises in government and the private sector, not-for-profits face unique challenges, including a lack of cybersecurity-trained personnel and budget. A recent report suggests that **68% of not-for-profit organizations do not have cybersecurity policies and procedures in place, and do not have a response plan if a cyberattack occurs.**[16] This limited cybersecurity expertise and bespoke knowledge makes them prone to becoming prime targets for attackers. For SMOs, cultivating a culture of security and awareness as well as implementing proper cybersecurity training can help detect and prevent cybersecurity attacks.

Implementing cybersecurity best practices is a complex endeavor. **This checklist enables a first self-assessment of key cybersecurity risk areas and provides the best practices to mitigate them.** Taking this self-assessment can help organizations obtain further guidance to improve their security posture. In addition, it will help organizations contextualize cybersecurity to the specific organizational context of their IT functions and capacities.

Organizational awareness and training

- Does the organization provide updated training for employees on anti-phishing and social engineering, and does it have policies and procedures in place to respond to such attacks?
- 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?

[16] "Cybersecurity Challenges and Best Practices for Nonprofits" (Eide Bailly)

Hardware/software Inventory

- Does the organization have a detailed hardware and software asset register as well as procedures for ensuring it is up-to-date?
- Does the organization maintain a comprehensive inventory of its data and corresponding access points to facilitate the effective implementation of system access restrictions?
- 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?
- Does the organization ensure that consent for data use in research activities is clearly communicated and standardized across projects, especially for data that could be used beyond research purposes?
- Does the organization implement access controls around sensitive information? 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 (such as phones, tablets, or home computers) when employees use them to access work email, cloud services, or other organizational systems?
- Does the organization encrypt its devices, such as laptops?
- Does the organization ensure all staff use secure VPN connections when working outside the office, and is this up for both new and current employees?
- Does the organization automate security defense updates for its 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 its existing leadership (which include management and board roles)? “Compliance officers stewardship” refers to individuals who make decisions about how the organization should comply with established requirements.
- Does the organization review relevant privacy compliance legislations regularly to ensure that it is following guidelines and best practices put out by relevant authorities, even if not required by law?
- Does your organization have privacy compliance policies, procedures, and third-party management in place?

Vendor management

- Does the organization review current and future agreements with third-party technology providers to ensure they align with internal policies?
- Does the organization enforce access restrictions for external marketing and website vendors to prevent them from controlling or sharing email addresses with hosting providers?
- 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 may have different privacy and security policies?

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?

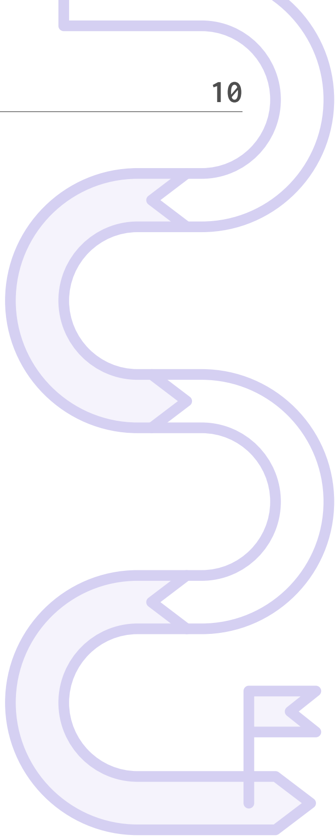
Now that your organization has identified cybersecurity issues, you can move on to action.

Working through this checklist will help your organization understand its current cybersecurity strengths and weaknesses without requiring external expertise. However, cybersecurity is an ongoing journey rather than a one-time exercise. Knowing whether plans and policies are in place is the first step, but it is equally important to ensure they are adequate, understood, and implemented by staff. While some identified issues can be addressed internally, others may require external guidance in order to implement solutions.

What you should consider to take it further: the value of cybersecurity audits and assessments

After having carried out the aforementioned self-assessment, a cybersecurity audit or assessment conducted by external experts could prove crucial to identify and address security vulnerabilities. While both approaches contribute to improving security practices, they serve different purposes. An external 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, or legal requirements. An assessment offers a broader view of your security, health and risks. Small and medium-sized organizations should choose based on their specific needs: an external audit is best for a comprehensive, independent review of security compliance, while an assessment offers more flexibility to understand and improve overall security.. Organizations can start with a cybersecurity assessment and later decide if an audit is necessary. If opting for an audit, it is recommended to first conduct an assessment using a risk matrix, whether internally or with external resources.

ASPECT	CYBERSECURITY AUDIT	CYBERSECURITY AUDIT
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



How to prepare for a cybersecurity audit: Are your assessment documents in order?

A cybersecurity audit is a crucial step in identifying and addressing security vulnerabilities that put your organization's data and operations at risk. An effective and meaningful audit requires your organization to properly prepare documentation. The **pre-audit readiness self-assessment checklist** helps organizations pinpoint essential elements that should be in place before engaging with external auditors.

By completing this checklist, your organization can recognize gaps in their documentation, processes, and controls that should be addressed first. This preparation serves as **a roadmap to make the audit process more efficient**. This process involves gathering the necessary documentation and preparing staff for the audit to ensure that it yields meaningful insights into real security risks.

Asset and documentation management

- Does the organization maintain an updated asset inventory of all computers, equipment, software licenses, and data storage locations?
- Does the organization keep written security procedures available and regularly updated for consultation?
- Has the organization 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

- Has the organization documented its security risk tolerance, specifying the level of risk it is willing to accept?
- Has the organization identified best practices and standards used for creating cybersecurity policies (i.e, ITSAP.00.137 - Canadian Centre for Cyber Security, ISO 27001 and 27002, or NIST CSF)?
- Is there a written process for giving and removing system access when staff join or leave the organization?

Infrastructure

- Does the organization provide guidance and recommendations on password policies, accessing cloud services, software and hardware?
- Does the organization use cloud services, and if so, are laptops configured to send working files to the cloud automatically?

Risk management

- Has the organization performed a basic review to identify weak points in cybersecurity?
- Does the organization maintain a list of known security problems and plans to fix them?

Team readiness

- Does the IT team have up-to-date maps of how the network is configured?
- Is there a listing of privileged users and systems administrators?

Incident response

- Is there a step-by-step plan for handling cybersecurity incidents?
- Are security events and incidents recorded systematically?

Privacy compliance

- Has the organization identified which privacy laws apply to its operations?
- Does the organization keep records to show how it complies with these laws?

Training and documentation

- Are records available for staff cyber security training sessions?
- Are specialized security trainings documented for technical staff (IT, HR, finance)?

Now that you have assessed your internal security using the checklist above, it is essential to **look beyond the boundaries of your organization**. Your operations likely depend on various external service providers - from cloud storage to email services - who can introduce additional security risks to your organization. Let's explore how to ensure these partners maintain the same level of security commitment you are working to achieve.

Third-party security assurance: Is your data safe with your service providers?

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 security.

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 is in someone else's hands

What are security assurance reports?

Service providers such as Microsoft, Amazon, or your local IT company should be able to prove the effectiveness of 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 examine five key areas that are vital for your organization’s operations: security, availability, processing integrity, confidentiality, and privacy.

Practical tips for your organization

- 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 not directly control or inspect large service providers such as Microsoft or Amazon. That is why these **independent security reports are crucial** - they give you assurance that your providers are maintaining proper security measures.

GET STARTED TODAY!

Now it is time to put cybersecurity measures into action. Here are some **extra resources that can support** your assessment and implementation process.

More checklists

Explore, use and adapt other Open North cybersecurity-related checklists:

- Checklist - Best Practices of Cybersecurity for SMOs
- Privacy Self-Assessment: Personal Data Protection in Québec (Law 25)
- Privacy Self-Assessment: PIPEDA and PIPA (British Columbia and Alberta)

Maturity assessment

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

- **Data maturity 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.

Contact Open North (info@opennorth.ca) to learn more about how we can help your organization.

About Open North

Open North is a not-for-profit organization dedicated to advancing the common good. Working alongside governments and civic-focused organizations of all sizes, we provide data expertise to enhance decision-making, drive innovation, optimize public and civic services, and address society's most pressing challenges. Our work spans the entire data lifecycle, with a core focus on data governance — guiding the human decisions that determine whether or not data is useful, actionable, secure and trustworthy.

Authors: Cristiano Therrien, Jérémy Diaz, Judith François-Langevin, Tona Mutimura, Merlin Chatwin, Christian Medina, John Griffin

Cybersecurity for Small and Medium-Sized Organizations