COMMUNITY FOUNDATIONS OF CANADA | The Learning Institute

Fact Sheet: Community Foundations of Canada CYBERSECURITY AND PRIVACY

July 18, 2024

We are awash in a sea of data, and we're not handling it well. Literally. Nonprofits, like every other organization or corporation, are taking in more information than ever before, and more than we know how to handle.

We handle personal and financial information on a daily basis, and we are putting clients and ourselves at risk. When it comes to the safe handling and storage of data, ignorance is not bliss.

All nonprofits must collect data to ensure their success and effectiveness, and sometimes this information can be very sensitive. Your community foundation has the mandate to safeguard the data you've collected, but often this responsibility isn't fully understood until after something goes wrong.

Understanding Cybersecurity Threats

Where are you storing the data you collect? The usual places are filing cabinets, network servers, and cloud storage. However, if that data is going places, you can get into trouble. As a nonprofit conducting business online and offline, here are some danger zones:

- **Phishing and Social Engineering:** Attackers manipulate individuals into divulging confidential information.
- **Ransomware:** Malicious software encrypts data and demands a ransom for its release.
- Insider Threats: Employees or volunteers may inadvertently or maliciously cause data breaches.
- **Advanced Persistent Threats (APTs):** Prolonged and targeted cyber-attacks aimed at stealing data.
- **Zero-Day Exploits:** Attacks exploiting unknown vulnerabilities in software.

Your Obligations When a Breach Occurs

A hacking attempt has serious consequences, but so does the loss or destruction of data. Laptops and smartphones holding sensitive data can be lost, damaged or even stolen, potentially putting your data in the wrong hands. Are you aware of your obligations?

The PCI Security Standards Council enacted the Payment Card Industry Data Security Standard that requires organizations to follow 'information security best-practices' if the organization handles major credit cards, such as Visa and MasterCard. Organizations that fail to comply with these standards can be penalized with substantial fines.

There are other data security regulations in Canada, such as Ontario's Personal Health Information Protection Act (PHIPA) that your nonprofit must comply with if you handle protected health information (PHI). These regulations are subject to change, so it's important to stay up to date. See Appendix A for provincial privacy legislation links and information.

Personally Identifiable Information

What makes up personally identifiable information (PII)? The definition can vary by province, but under the Personal Information Protection and Electronic Documents Act (PIPEDA), personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type
- opinions, evaluations, comments, social status, or disciplinary actions
- employee files, credit records, loan records, medical records, the existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).

According to PIPEDA: "Organizations covered by the Act must obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by appropriate safeguards."

What You Need to Have In Place

Have you asked yourself what you would do in the event of a breach? Do you know whom you would call first? You need to have a plan in place specific to your community foundation. It needs to layout procedures, identify whom to contact and have all the pertinent contact information available.

Organizations and businesses now need cyber liability coverage.This is an additional expense, but a necessary one, as the cost of not being insured far outweighs the price of the coverage. And the cost of premiums is nothing compared to the retainer required for a lawyer in the event of a breach. One upside is that in the course of applying (yes, applying) for this insurance, you will have to review your current security provisions. This is an excellent opportunity to improve areas of exposure. You need to have coverage not only for losses you may incur but against claims from losses suffered by third parties like donors or clients. Some costs you might incur include:

- Content liability
- Data breach liability
- Regulatory investigation expense
- Crisis management
- Notification expenses

Handling Data with Care

We have to be more aware of how we transfer data between storage spaces and devices. The Law expects corporations and businesses to safeguard this data regardless of where it is stored: paper, networks, mobile devices, personal devices, or stand-alone systems. When we think of “security” in this context, it can be defined as the “confidentiality, integrity & availability of data.” Privacy, however, is about “the appropriate use of data”.

What can you do to better secure the data you handle? It comes down to employing best practices that have been around a long time.

- Ensure you have a patch management program in place to protect the tech you use. These security updates are an excellent first line of defense.

- Practice strong encryption. Lock down laptop hard drives and secure all mobile devices with passcodes and Virtual Private Networks, which are a group of computers networked together over a public network, namely the internet. VPNs. Encrypt sensitive data. If possible, do not store PII (personally identifiable information) on mobile devices.
- Engage in regular training sessions with your employees. Build a security culture so that employees care for the data, instead of just watching a video once a year.
- Have a Bring Your Own Device (BYOD) policy. If employees are allowed to use their own devices, establish clear guidelines around access and authorization regarding personal information.

Assessing Organizational Cyber Readiness

It's critical that community foundations demonstrate some proactive measures in this area. At a minimum:

- Develop an Incident Response Plan
- Secure cyber insurance
- Create a business continuity plan as part of an exercise to get staff and board thinking about recovery measures, operational necessities, etc.

And when developing their cybersecurity plans, foundations need to find that balance between risk, reasonable measures, resources/capacity and cost.

The Vancouver Foundation (VF) has undertaken a lot of work in this area. Adhering to the following best practices helps mitigate risks and protect sensitive data:

1. Implement Strong Access Controls

- Multi-Factor Authentication (MFA): Require MFA for all accounts to add an extra layer of security.
- Least Privilege Principle: Grant users the minimum access necessary to perform their duties.

2. Regularly Update and Patch Systems

- Automated Updates: Ensure systems and applications are set to update automatically.
- Patch Management: Regularly apply patches to fix known vulnerabilities.

3. Conduct Regular Security Training

- Phishing Simulations: Conduct periodic phishing simulations to train employees to recognize threats.
- Security Awareness Programs: Implement ongoing education programs on security best practices.

4. Use Advanced Threat Detection Tools

- Endpoint Detection and Response (EDR): Deploy EDR solutions to monitor and respond to threats.
- Threat Intelligence: Utilize threat intelligence services to stay informed about emerging threats.

5. Develop and Test Incident Response Plans

- Incident Response Team (IRT): Establish an IRT with clear roles and responsibilities.
- Regular Drills: Conduct regular incident response drills to ensure preparedness.

6. Ensure Data Encryption

- Data at Rest and in Transit: Encrypt sensitive data both at rest and in transit to protect against unauthorized access.
- End-to-End Encryption: Implement end-to-end encryption for communications and data transfers.

7. Perform Regular Security Assessments

- Vulnerability Scans: Regularly scan for vulnerabilities in your network and applications.

- Penetration Testing: Conduct periodic penetration testing to identify and address security weaknesses.

8. Secure Third-Party Interactions

- Vendor Risk Management: Assess the security posture of third-party vendors and require them to comply with your security standards.
- Third-Party Access Controls: Limit and monitor third-party access to your systems and data.

9. Backup and Recovery Plans

- Regular Backups: Perform regular backups of critical data and verify their integrity.
- Disaster Recovery Plan: Develop and test a disaster recovery plan to ensure business continuity.

10. Monitor and Respond to Threats

- Security Operations Center (SOC): Implement a SOC to monitor, detect, and respond to security incidents.
- Continuous Monitoring: Utilize continuous monitoring tools to detect anomalies and potential threats in real-time.

Developing an Incident Response Plan

Cybersecurity experts warn it is not a question of *if* one's organization will be compromised but *when.* A comprehensive cybersecurity incident response plan is necessary to have as a sound guideline when the inevitable occurs. The key steps of any plan include:

1. Incident Identification – Detecting/Defining the Threat
2. Take Appropriate Action – Containment & Eradication
3. Recover Systems

4. Reporting & Follow-up

There are many resources freely available to IT professionals that prescribe comprehensive steps to cybersecurity best practices and incident response plans. The framework adopted by Vancouver Foundation leans heavily upon the work of the UK-based not-for-profit cybersecurity accreditation body, CREST. Their plan is outlined in Appendix B. Here's a link to another resource on developing such a plan: How to Create a Nonprofit Cyber Incident Response Plan

Know the Letter of the Law

While Canada's privacy laws do not have any rules against using the cloud, the CRA requires that certain records be kept in Canada. If done right, cloud storage is a secure option for most nonprofits.

It's also important to know how the US and Europe differ from Canada regarding privacy and data storage. Since 2015 when the Safe Harbour agreement between the US and Europe ended, new provisions are being put into place regarding data and privacy that will have a global impact.

There are some excellent and secure cloud storage options. Check with your community foundation colleagues to find out what options they are using.

How do you work with third parties like vendors? Put your terms in your contracts. It's a reasonable expectation that vendors will have errors and omissions coverage to protect you. Have a frank discussion about what liability the vendor is prepared to take on and how they will do so.

Privacy Policy Guidelines

Having a clear and comprehensive privacy policy is essential. Ensure your policy includes:

Information Sharing and Confidentiality

- Association of Fundraising Professionals Code: Adhere to guidelines such as: "Members shall not disclose privileged or confidential information to unauthorized parties; Members shall adhere to the principle that all donor and prospect information created by, or on behalf of, an organization or a client is the property of that organization or client and shall not be transferred or utilized except on behalf of that organization or client."

Policy Statements

- Privacy Protection Statement: Include a statement that the organization protects the personal privacy of constituents by maintaining the confidentiality of all constituent information.
- Information Release Protocols: Outline how and when information will be released, such as addresses, phone numbers, and email addresses.
- Third-Party Requests: Define the process to manage third-party requests for information and specify what staff are permitted to say.

Adapting to Data Growth

As data continues to grow exponentially, nonprofits must adapt to handle it better and be prepared to do things differently. Safeguarding data must be as prioritized as the causes served.

Resources

CFC's Key Policy Template Manual: Includes a sample Confidentiality and Privacy Policy.

Learn more:

- Canadian privacy law, cloud computing and how it applies to nonprofits
- A Nonprofit's Cyber Liability And Data Privacy
- Data Privacy and Cyber Liability: What You Don't Know Puts Your Mission at Risk
- Innovating Canada: Cybersecurity
- Supporting Your Secure Cloud Journey with 4 Questions
- How Remote Workforces Change the Way we Approach Digital Security

Acknowledgments

Thanks to TechSoup for permission to reprint excerpts from the guest blog “Privacy and Data Concerns for Nonprofits” by Cheryl Biswas, Threat Intel Consultant (May 18, 2016).

APPENDIX A: PROVINCIAL PRIVACY LEGISLATION

Not all provinces have their own legislation in this area. The following provinces have enacted their own legislation.

Alberta: Personal Information Protection Act (PIPA)

Description: Alberta's private sector privacy law, includes rules for collecting, using, and disclosing personal employee information.

Link: https://www.alberta.ca/personal-employee-information

British Columbia: Personal Information Protection Act (PIPA)

Description: Individuals have the right to access their own personal information; sets rules for organizations on collecting, using, and disclosing personal information.

Link: https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information

Nova Scotia: Personal Information International Disclosure Protection Act (PIIDPA)

Description: Limits the storage and access of Nova Scotia government personal information outside of Canada.

Link: https://novascotia.ca/just/iap/piidpaquest.asp#:~:text=PIIDPA%20makes%20it%20illegal%20for,Canada%2C%20unless%20certain%20circumstances%20exist

Quebec: Act Respecting the Protection of Personal Information in the Private Sector

Description: Regulates the protection of personal information collected, held, used, or communicated by private-sector employers.

Link: https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1

Nunavut: Access to Information and Protection of Privacy Act (ATIPP)

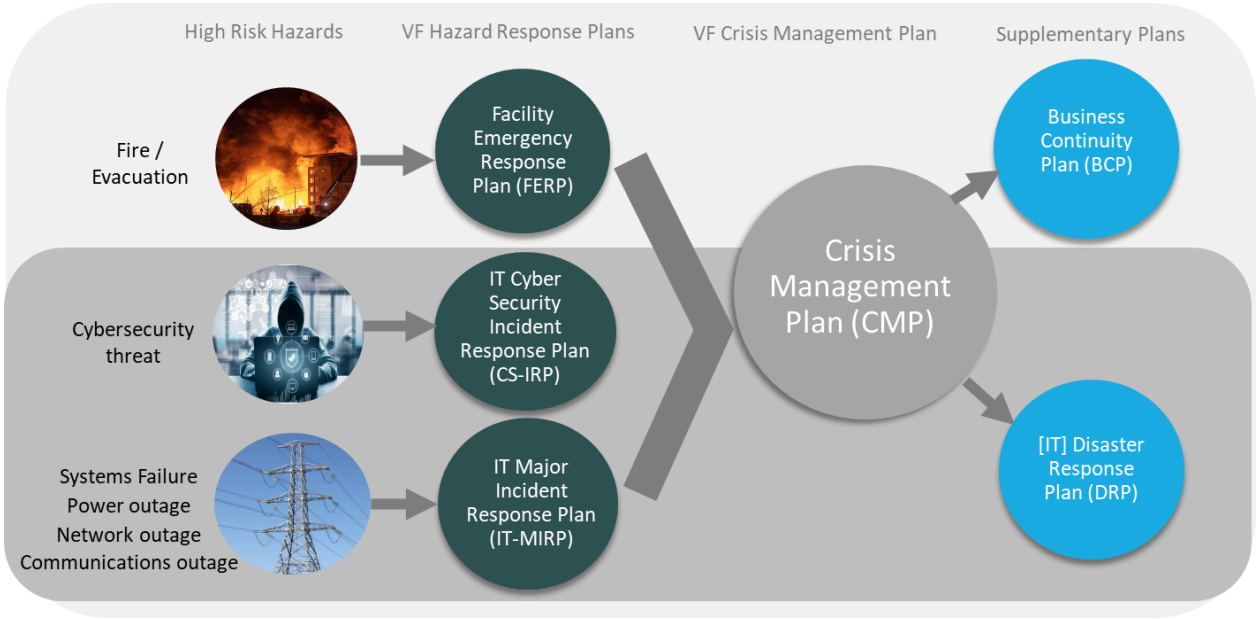
Description: Provides individuals with the right to access information held by public bodies and establishes privacy protections.

Link:
https://www.gov.nu.ca/sites/default/files/documents/2024-02/atipp_manual_-_part_1.pdf

APPENDIX B: Vancouver Foundation's Cyber Incident Response Plan

The Framework:

VF's Cyber Response Plan is a subset of a series of high risk hazards and hazard specific plans that dove tail into an overarching Crisis Management Plan (CMP), Business Continuity Plan (BCP) and Disaster Response Plan (DRP).



The following section covers the Cyber Security Incident Response Plan.

Incident Identification – Detecting/Defining the Threat:

A common cybersecurity trend, particularly in the case of intellectual property theft, is for intrusions to remain dormant in the system for some time before they are detected. Identifying a suspected cybersecurity incident (e.g., monitoring evidence of unusual occurrences and assessing trigger points) has been incorporated into VF's operational functions. Routine firewall logging reviews and anomalous port alerting mechanisms are part of the Fortinet firewall security fabric employed at the Foundation. Additionally, Vancouver Foundation staff are continually reminded to report all unusual network behavior, suspicious/unknown sender emails, and information failures or loss of services

to the Helpdesk. Staff should note all important details (e.g., type of breach, messages on screen, and other details of unusual occurrences), aiding technicians in recovery exercises, root cause analysis, and possible downstream litigation activities.

Understand the Attack:

Once a cybersecurity incident has been identified, IT staff define the objectives for the response by answering the following questions:

- How was the incident detected?
- Who reported the incident and when?
- What are the initial indicators of compromise (IOCs)?
- What immediate actions were taken upon detection?
- Which systems, applications, and data are affected?
- What is the extent of the compromise (e.g., number of systems, types of data affected)?
- Is the incident isolated or widespread across the network?
- What is the potential impact on business operations and data security?
- What type of cyber-attack is it (e.g., malware, ransomware, phishing, DDoS)?
- Who might be responsible for the attack (e.g., internal threat, external hacker, nation-state)?
- What are the attack vectors and methods used (e.g., email, web application, network intrusion)?

Determining what information has been disclosed to unauthorized parties, stolen, deleted, or corrupted is a key deliverable at this stage and will be accomplished swiftly and consistently.

Conducting Triage – Classifying and Prioritizing Incidents:

While each situation is different, IT staff are encouraged to categorize the intrusion using an incident classification matrix.

Category	Description	Example of Type of Event
Critical	Incidents causing severe damage or disruption, leading to significant operational impact or data loss, requiring immediate and comprehensive response.	Ransomware attack encrypting critical business data, major data breach of sensitive customer information, DDoS attack disrupting all services.
Significant	Incidents that have considerable impact on operations or data, potentially leading to serious disruptions, requiring prompt and focused response.	Targeted phishing attack compromising key employee credentials, malware infection on multiple workstations, unauthorized access to non-critical systems.
Minor	Incidents with limited impact on operations or data, causing minimal disruption, requiring routine response procedures.	Single user malware infection contained by antivirus, minor phishing attempt on non-critical staff, small-scale unauthorized access attempt with no data loss.
Negligible	Incidents causing negligible impact, primarily requiring monitoring and standard precautionary measures.	Spam emails without phishing links, unsuccessful brute-force attack attempts, low-risk reconnaissance activities.

"First Responder" Actions:

In addition to IT Ideas, Vancouver Foundation enjoys close relationships with expert cybersecurity vendors including Mirai Security, and legal counsel, Norton Rose Fulbright.

Knowing when to escalate and call in more specialized resources is an important aspect of initial analysis helping to ensure key details are captured. These include: date/time, IP address, port (source and/or destination), system (hardware/vendor, OS, application, etc.). As part of Vancouver Foundation's broader Business Continuity and Incident Response Plan, clear reporting channels and points of escalation are outlined in this document.

Log Type	Description	Example
Firewall Logs	Records of all incoming and outgoing network traffic through the firewall.	Log entries showing blocked unauthorized access attempts.
System Logs	Logs from operating systems detailing system events and activities.	Records of user logins, system reboots, and errors.

Log Type	Description	Example
Application Logs	Logs from applications capturing usage and errors.	Log entries showing application crashes or unusual activity.
Intrusion Detection System (IDS) Logs	Records of detected potential intrusions.	Log entries showing detected suspicious network activity.
Access Logs	Records of user access to systems and data.	Logs showing times and locations of user logins.
Email Logs	Logs of sent and received emails, including attachments.	Log entries showing suspicious email attachments or phishing attempts.
Authentication Logs	Records of authentication attempts and results.	Logs showing failed and successful login attempts.
Database Logs	Logs of database queries, updates, and access attempts.	Log entries showing unauthorized data access attempts.
Endpoint Logs	Logs from endpoint devices, including antivirus and security software logs.	Log entries showing malware detection on workstations.

Contain the Cyber Security Incident:

Once an initial investigation has occurred and a bona fide intrusion is recognized, the team will contain the damage by preventing the incident from spreading to other networks and devices. Containment activities include:

- Blocking (and logging) unauthorized access
- Blocking malware sources (e.g., email addresses and websites)
- Closing specific ports and mail servers
- Changing system administrator passwords where compromise is suspected
- Firewall filtering
- Relocating website home pages

- Isolating systems
- Preserving evidence and documenting steps taken (data captures, firewall log archives, etc.) is necessary for potential legal action.

Eradicating the Cause of the Incident:

Eradication involves eliminating key components of the incident, such as removing malware and disabling breached user accounts, while identifying and mitigating exploited vulnerabilities. Actions include:

- Identifying all affected hosts
- Conducting malware analysis
- Monitoring for any attacker response
- Developing a response plan for potential further attacks
- Ensuring network security and no attacker response

Gathering and preserving evidence

Gathering and preserving evidence is governed by the rules of admissibility and weight of evidence. Contacting legal counsel and cybersecurity experts is essential to maintain a chain of evidence.

- Admissibility of evidence – whether or not the evidence can be used in court
- Weight of evidence – the quality and completeness of evidence

Contacting/engaging the Foundation's legal counsel (Norton Rose FulBright) as well as cyber security experts (Mirai Security) is key at this juncture. It is essential that VF capture the chain of evidence for both paper-based and electronic information – keeping a detailed written log of every action during the investigation so that:

- Clear and precise evidence can be referred to at a later date, and

- The sequence of events and actions taken can be repeated by opposition experts, if required.

This action log will include:

- Identifying information (e.g. the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

Recover Systems, Data and/or Connectivity

The final step in responding to a cyber security incident is to restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents occurring. Understanding that reconnecting networks, rebuilding systems and restoring/recreating or correcting information is time consuming, the business must appreciate IT recovery priorities and the need to complete these steps thoroughly. Often based on the specifics of the compromise, appropriate recovery plans include:

- Rebuilding infected systems from known clean sources
- Replacing/restoring compromised files
- Removing temporary constraints imposed during containment
- Resetting passwords on compromised accounts
- Installing patches and tightening network security
- Thoroughly testing systems, including security controls
- Confirming business systems' and controls' integrity

An independent penetration test and a security controls assessment validate system recovery. IT Steering Committee stakeholders will receive a summary of the incident, eradication efforts, and significant findings, followed by a detailed explanation of activities.

Reporting & Follow-Up:

Research in this area stresses the importance of allocating time to follow-up activities following a cyber security incident.

Senior stakeholders will assist IT in ensuring sufficient resources are protected for these efforts to occur and that other priorities can and should wait while these important steps are completed:

- Conducting deep dive forensics to identify perpetrators
- Performing root cause analysis
- Quantifying the business impact
- Supporting criminal investigations
- Performing trend analysis

Once a cyber security incident has been successfully handled, formal reporting will occur for both internal and external stakeholders. Key questions to consider will vary by the nature of the intrusion but include:

- What are the Foundation's reporting requirements and to what constituents?
- What do I report?
- In what format do I report?
- What is the objective of reporting?

Finally, a full description of the nature of the incident, its history, and what actions were taken to recover is required:

- A realistic estimate of the financial cost of the incident, as well as other impacts on the business (e.g.

  reputational damage, loss of management control or impaired growth, etc.)
- Recommendations regarding enhanced or additional controls required to prevent, detect, remediate or recover from cyber security incidents more effectively.

Carry out a post-incident review

Review and improve response procedures, share lessons learned, and update relevant documents and controls. Questions for the review include how well staff performed, needed information, and corrective actions.

Questions to be answered in such a review can include:

1. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
2. What information was needed sooner?

3. Were any steps or actions taken that might have inhibited the recovery?
4. Could any unforeseen events have been prevented?
5. What would the staff and management do differently the next time a similar cyber security incident occurs?
6. How could information sharing with other organizations have been improved?
7. What corrective actions might prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?
9. How can results be fed back into VF's risk assessment methodology?
10. What lessons have we learned?

Communicate and build on lessons learned!

Clear communication with all stakeholders is essential, focusing on problem resolution and control improvement. Create an action plan to leverage lessons learned and enhance resilience against future attacks.

Update key information, controls and documents

Following a cybersecurity incident, update response approaches, controls, and related documents to reflect lessons learned and improve future responses.