COMMUNITY FOUNDATIONS OF CANADA | The Learning Institute

Fact Sheet: Community Foundations of Canada CYBERSECURITY AND PRIVACY

June 14, 2021

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.

What Are the Danger Zones?

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:

- Collecting credit card data and processing payments online
- The transfer and storage of personal data for employees, clients or donors via email
- Storing personal information on laptops or smartphones
- Granting access to personal information to third parties like vendors without proper safeguards
- Storing personal information on cloud servers or systems, or physically unsecured sites (e.g. unlocked filing cabinets).

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.

Businesses now need cyber liability coverage; this is no longer an extra expense. 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 defence.
- 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. VF accessed a 10-question survey that helped them to develop their plan.

1. **Antivirus**: Have you deployed antivirus software in your organization?

2. **Patch Management Strategy:** Have you (or has your IT service provider) implemented routine and automated security patch updates across your servers and workstations?

3. **Software/OS Compliance:** Are you using current operating systems and software versions? Are any of your server systems at or approaching "end-of-life" status?

4. **Workplace Culture & Staff Cyber Awareness:** Do you (or does your IT service provider) conduct cybersecurity awareness training within your organization at least once per year?

5. **Email Anti-Spam:** Have you deployed email anti-spam software filters at your organization?

6. **Password Management:** Are you enforcing minimum password standards (e.g. 8 characters or more, alphanumeric, complexity characters, no sharing passwords, no emailing passwords, etc.)?

7. **Third-Party Technology Reviews:** Has your organization considered a professional IT assessment (such as a network penetration test) to identify possible weak points/exploits?

8. **IT Policies:** Do you have current IT policies in place within your organization (e.g. acceptable use policy, email/internet use policy, social media policy, password policies)? Are staff members familiar with them?

9. **Physical Workplace Protections:** Does your organization's workplace employ physical security safeguards (office access keys/fobs, visitor sign-in sheet, etc.)?

10. **Business Continuity/IRP:** Do you have an Incident Response Plan in the event a breach occurs?

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

To learn more on cybersecurity, listen to or read the interview with James Law (Grantbook) and Charles Boname (Director Information Technology at the Vancouver Foundation) Digital Maturity and Cybersecurity

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.

Have A Privacy Policy

Do employees, trustees, and volunteers understand what information not to share or release? Here are the recommendations for acceptable use and dissemination of constituent information by the Association of Fundraising Professionals Code of Ethical Principles and Standards:

"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."

Your privacy policy should include a brief statement that the organization protects the personal privacy of constituents by maintaining the confidentiality of all constituent information. As well, there should be a statement that outlines how and when the information will be released, such as addresses, phone numbers, and email addresses. Lay out the process to manage third-party requests for information and what staff are permitted to say.

As data continues to grow exponentially, we need to adapt and handle it better; and be prepared to do things differently. Nonprofits must be as dedicated to the cause of safeguarding their data as they are to the causes they serve.

A resource that you should consider is CFC's Key Policy Template Manual which includes a sample Confidentiality and Privacy Policy.

Learn more:

- Online Privacy for Nonprofits
- Canadian privacy law, cloud computing and how it applies to nonprofits
- A Nonprofit's Cyber Liability And Data Privacy
- Protecting Your Constituents' Personal Information
- 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

Thanks To TechSoup for permission to reprint excerpts from a guest blog entitled “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
This act is Alberta's private sector privacy law and includes rules for how organizations collect, use, and disclose personal employee information and limits how that information can be used.
https://www.alberta.ca/personal-employee-information.aspx

BRITISH COLUMBIA: Personal Information Protection Act
Under the act, individuals have the right to access their own personal information. The law also states the rules by which organizations can collect, use and disclose personal information from customers, clients and/or employees.
https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information

QUEBEC: Protection of Personal Information in the Private Sector
The Act covers private-sector employers and regulates the protection of personal information that an employer collects, holds, uses, or communicates to third persons while carrying on its business. The legislation is being amended at the writing of this document. Employers should consult with their lawyer as to the current legislation and regulations.
http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1

APPENDIX B: Vancouver Foundation's Cyber Response Plan

The Framework:

Incident Identification – Detecting/Defining the Threat:

A common cyber security trend, particularly in the case of intellectual property theft, is for cyber security intrusions to remain dormant in the system for some time before they are detected. Identifying a suspected cyber security incident (e.g. monitoring evidence of unusual occurrences and assessing one or more 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. In addition, Vancouver Foundation staff are advised and continually reminded to report all unusual network behaviour, suspicious/unknown sender emails as well as information failures or loss of services, to a central point, namely *Helpdesk*. Staff are told to note all important details (e.g. type of breach, messages on screen, and other details of unusual occurrences), all of which aids technicians in recovery exercises, root cause analysis, as well as possible downstream litigation activities.

Understand the Attack:

Once a cyber security incident has been identified, IT staff next define what the objectives are for the response, answering such questions as:

- Who has attacked us?
- What is the scope and extent of the attack?
- When did the attack occur?
- What did the attackers take from us?
- Why and how did they do it?

Determining what information has been disclosed to unauthorised parties, stolen, deleted or corrupted is a key deliverable at this stage and will be accomplished in a consistent and swift manner.

Conducting Triage – Classifying and Prioritizing Incidents:

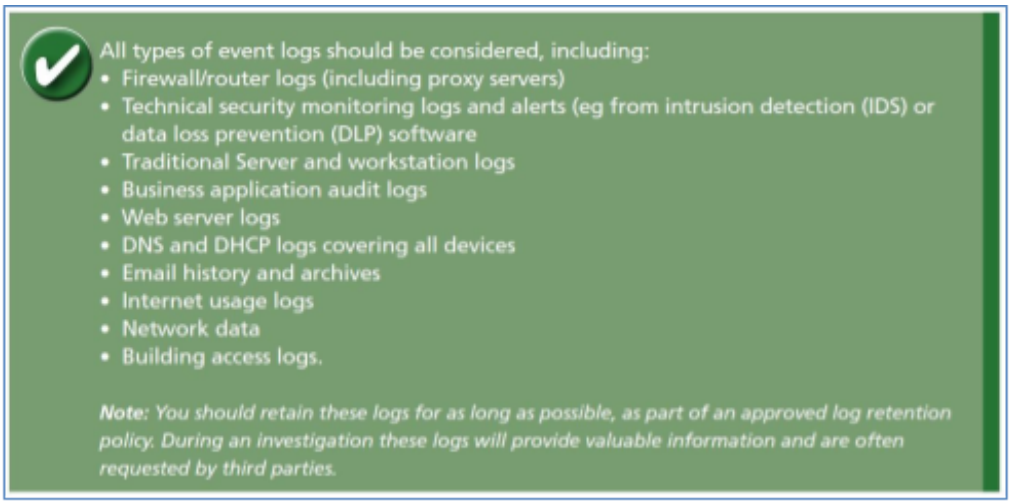
While each situation is different, IT Staff are encouraged to categorize the intrusion via the following example matrix:

Category	Description	Example
Critical	These incidents will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security, affect mission-critical equipment or services or damage public confidence in the organisation.	Targeted cyber security attacks or loss of publicly available online service.
Significant	Less serious events are likely to impact a smaller group of users, disrupt non-essential services and breaches of network security policy.	Website defacement or damaging unauthorised changes to a system.
Minor	Many minor types of incident can be capably handled by internal IT support and security. All events should be reported back to the information security team who will track occurrences of similar events. This will improve understanding of the IT security challenges and may raise awareness of new attacks.	Unsuccessful denial-of-service attack or the majority of network monitoring alerts.
Negligible	It is not necessary to report on incidents with little or no impact or those affecting only a few users, such as isolated spam or anti-virus alerts; minor computer hardware failure; and loss of network connectivity to a peripheral device, such as a printer.	Isolated anti-virus alert or spam email.

"First Responder" Actions:

In addition to IT Ideas, Vancouver Foundation enjoys close relationships with expert cyber security vendors including, MNP LLP, Mirai Security as well as legal counsel, Fasken LLP. 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.[1]

[1] Note: Acredo Consulting's *Business Continuity & Incident Response Plan* was completed and released in October 2018.



All types of event logs should be considered, including:

- Firewall/router logs (including proxy servers)
- Technical security monitoring logs and alerts (eg from intrusion detection (IDS) or data loss prevention (DLP) software
- Traditional Server and workstation logs
- Business application audit logs
- Web server logs
- DNS and DHCP logs covering all devices
- Email history and archives
- Internet usage logs
- Network data
- Building access logs.

Note: *You should retain these logs for as long as possible, as part of an approved log retention policy. During an investigation these logs will provide valuable information and are often requested by third parties.*

Contain the Cyber Security Incident:

Once initial investigation has occurred, and a *bona fide* intrusion recognized, the team will contain the damage done by the cyber security incident by stopping it from spreading to other networks and devices, both within the organization and beyond. Containment typically comprises many concurrent actions aimed at reducing the immediate impact of the cyber security incident, primarily by removing the attacker's access to Foundation systems. The objective of containment is not always to return (directly) to business as usual, but to make best efforts to return to *functional* operations while focussing technical efforts on analyzing the incident and planning longer term remediation. Containment activities include:

- Blocking (and logging) of unauthorised 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.

Finally, evidence preservation as well as documenting steps taken (data captures, firewall log archives, etc.) is necessary should legal action be required later in the process.

Eradicating the Cause of the Incident:

These actions are to be carried out with both speed and precision. After an incident has been contained, eradication is often required to eliminate key components of the incident (e.g. removing the attack from the network, deleting malware and disabling breached user accounts),

as well as identifying and mitigating vulnerabilities that were exploited. During the eradication process, actions IT will take include:

- Identifying all affected hosts within (and sometimes beyond) the organization, so that they can be remediated
- Carrying out malware analysis
- Checking for any response from the attacker to IT's actions
- Developing a response (preferably in advance) if the attacker uses a different method of attack
- Allowing sufficient time to ensure that the network is secure and that there is no response from the attacker.

Gathering and preserving evidence

Evidence will be gathered at various points during the investigation, but all evidence will be governed by two primary rules, which are:

- 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 (Fasken LLP) 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 (often from known 'clean' sources)
- Replacing/restoring compromised files with clean versions
- Removing temporary constraints imposed during the containment period
- Resetting passwords on compromised accounts

- Installing patches, changing passwords and tightening network perimeter security, such as firewall rule sets
- Testing systems thoroughly – including security controls
- Confirming the integrity of business systems and controls.

It is important to validate that systems are operating normally again, which can often be achieved by carrying out an independent penetration test of the affected systems, complemented by a security controls assessment. As above, monitoring may need to take place over an extended time to detect any further attacks (or attempted attacks). Once systems have been recovered and controls tested, IT Steering Committee stakeholders will be provided with a summary of what took place. The team will report on eradication efforts – that these steps were completed successfully, noting any exceptions and other significant findings. An initial, high-level communication will be issued within a week of the event, followed by a deeper explanation of the activities that took place.

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 sufficient investigation (e.g. deep dive forensics) to identify (and prosecute, if appropriate) the perpetrator(s)
- Performing root cause identification/analysis
- Quantifying the business impact of the incident
- 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

Important information about the cyber security incident will be discussed during a post-incident review.

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!

Communication to all stakeholders is to be clear, concise and focused on problem resolution and control improvement. These communications will clearly identify any gaps that remain and propose efforts to mitigate them. An action plan will then be created that explains how the organization will leverage lessons learned from the incident to become more resilient in the face of future cyber security attacks.

Update key information, controls and documents

Following a cyber security incident, it is important to update the cyber security incident response approaches, controls and related documents.