CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

The 2022 Ottawa Region
Charity & Not-for-Profit Law
Webinar
February 17, 2022

Online Privacy and Cybersecurity Issues for Charities and NFPs

By Esther Shainblum, B.A., LL.B., LL.M., CRM
eshainblum@carters.ca
1-877-942-0001

OVERVIEW

- Charities and Not-for-Profits (NFPs) with online operations face a number of risks that they need to manage actively
- Organizations operating online should have appropriate policies and procedures in place to manage the associated privacy and cybersecurity risks

3

A. CONTEXT

- Like their for-profit counterparts, charities and NFPs are increasingly operating in the digital/online landscape, including:
  - Public facing websites
  - Online presence/social media
  - Online donation forms
  - Cloud-based platforms for core business processes, such as video conferencing, donor management and payment processing (e.g. Zoom, Blackbaud, Stripe)
- The COVID pandemic has heightened reliance on the Internet

www.charitylaw.ca www.carters.ca

4

B. CYBER SECURITY ISSUES

- Cyber Threat Actors (Canadian Centre for Cyber Security)

Cyber Threat Actor	Motivation
Cyber Criminals	Profit
Nation States/ Advanced Persistent Threats	Geopolitical
Insider Threats – Malicious or Negligent	Disgruntled
Hacktivists/ Terrorist	Ideology
Thrill Seekers	Satisfaction

www.charitylaw.ca www.carters.ca

5

- IBM Security and The Ponemon Institute's Cost of a Data Breach Report 2021:
  - The average total cost of a data breach increased significantly over 2020 (10%)
  - Canada had the third highest average total cost of a data breach at $5.4 million, a 20% increase over 2020
  - The average cost of a breach was $1 million higher when remote work was a factor
  - The top two attack vectors were compromised credentials and phishing
  - Customer personal information was the most common type of record compromised and had the highest average cost per lost or stolen record

www.charitylaw.ca www.carters.ca

6

- 2021 Palo Alto Networks Canada Ransomware Barometer:
  - Ransomware gangs are thriving in Canada
  - The average ransom paid by Canadian businesses was $458,247
  - 58% of organizations paid the ransom, 14% paid more than once
  - Ransomware attacks have long term impacts on organizations, some taking as long as 6 months to recover

www.charitylaw.ca www.carters.ca

7

C. DUTIES AND OBLIGATIONS OF DIRECTORS

- Under the *Canada Not-for-Profit Corporations Act* and the *Ontario Not-for-Profit Corporations Act,* directors and officers of charities and NFPs are required to:
  - Act honestly and in good faith with a view to the best interests of the company; and
  - Exercise the care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances
- Charitable directors are also subject to high fiduciary duties to protect and conserve charitable property and can be found personally liable for any loss that the corporation suffers as a result of a breach of fiduciary duty

www.charitylaw.ca www.carters.ca

8

- Directors of charities can be found liable in tort for negligent mismanagement if their carelessness in the oversight of the corporation's operations leads to injury
- Therefore, if directors and officers fail to put sufficiently robust measures in place to protect personal information, they could face personal liability
- In order to avoid liability, directors must be able to demonstrate that they took appropriate steps to identify, manage and mitigate privacy and cybersecurity risks
- "Business Judgment Rule" – The courts will not second-guess directors who acted prudently and on a reasonably informed basis. Perfection is not required.

www.charitylaw.ca www.carters.ca

9

- Directors can show that they met the duty of care and made an informed, reasonable decision by, for example:
  - Demonstrating that they had information available to them and how they considered it
  - Obtaining expert advice on privacy and cybersecurity
  - Ensuring that the organization is compliant with privacy laws/best practices
  - Confirming that the organization has appropriate safeguards in place to protect personal information and to prepare for and respond to privacy breaches and cyber attacks
  - Obtaining regular reports from management on cybersecurity and privacy issues
  - Obtaining insurance to cover these risks

www.charitylaw.ca www.carters.ca

10

- Directors and officers of charities and NFPs should look to *Personal Information Protection and Electronic Documents Act* ("PIPEDA") for guidance
- PIPEDA applies to any private sector organization that collects, uses, or discloses personal information in the course of "commercial activities"
- PIPEDA does not generally apply to charities and NFPs as most of the activities that they regularly engage in do not qualify as "commercial activities"
- However, the Office of the Privacy Commissioner of Canada ("OPC") recommends that charities and NFPs follow the fair information principles in Schedule 1 to PIPEDA as best practices

www.charitylaw.ca www.carters.ca

11

- Compliance with the fair information principles in Schedule 1 would likely position charities and NFPs to demonstrate that they acted in accordance with the duty of care
- Schedule 1 principles include (not exhaustive):
  - An organization is responsible for personal information under its control
  - An organization is responsible for personal information that has been transferred to a third-party for processing

www.charitylaw.ca www.carters.ca

12

- Organizations must implement policies and practices, including procedures to protect personal information and training and communicating to staff information about the organization's policies and practices
- Personal information must be protected by security safeguards appropriate to the sensitivity of the information
- Organizations must protect personal information in any format against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification

www.charitylaw.ca www.carters.ca

13

- The nature of the safeguards must vary depending on the sensitivity of the information. More sensitive information should be safeguarded by a higher level of protection
- The methods of protection should include:

(a) Physical measures; such as alarms, locked doors, locked cabinets, access cards;

(b) Organizational measures; such as policies, training, security clearances, "need to know" access; and

(c) Technological measures; such as passwords, encryption and other measures discussed today

www.charitylaw.ca www.carters.ca

14

D. CYBERSECURITY MEASURES

- Most charities and NFPs probably do not have the financial resources to implement sophisticated security systems using artificial intelligence, machine learning and automation
- However, as per Schedule 1, charities and NFPs with online operations do need to put in place appropriate measures to mitigate the risk of data loss, privacy breach or cyber attack and there are a number of measures within reach. Some examples, not exhaustive:
  - Continuous education, training and testing of staff as first line of defense
  - Identify and address vulnerabilities and gaps
  - Back up all critical data off-site/off-line/not accessible

www.charitylaw.ca www.carters.ca

15

- Have up-to-date anti-virus and anti-malware software in place
- Require strong and complex passwords for all accounts/devices and require them to be changed routinely
- Move toward "Zero Trust" approach – Treat every user inside or outside as untrusted. Implement Multi Factor Authentication for every user and provider/vendor before accessing key areas. (Castle wall vs. key to every door)
- Limit employee access to personal information on a "need to know" basis. Develop a culture of vigilance against internal threats, *e.g.* screening, access controls and data segregation, oversight and monitoring

www.charitylaw.ca www.carters.ca

16

- Carefully screen and select vendors
- Consider endpoint security solution to protect mobile/remote devices
- Have clear privacy breach and security incident response protocols in place, ensure that staff is informed of them and test and update them
- Obtain adequate cyber insurance coverage to cover costs of incident response, legal and other advice and even the cost of ransom in some cases

www.charitylaw.ca www.carters.ca

17

E. PRIVACY COMPLIANCE ONLINE

- Charities and NFPs also need to comply with privacy laws/best practices even when operating online. Some examples, not exhaustive:
  - Charities and NFPs should have a robust enterprise privacy policy explaining what personal information they collect, why, how it will be used, who it will be shared with and how it will be protected. It should be posted on the organization's website, be regularly reviewed and updated, be understandable and user friendly, and be backed up by an appropriate privacy compliance program/procedures
  - Organizations must obtain consent for the collection, use, or disclosure of personal information at or before the time of collection (privacy policy) and limit the collection of personal information to what is necessary for the purposes identified

18

- Consent processes need to be understandable, user friendly and easily accessible from all devices
- Consent should generally be express, but implied consent can be used in strictly defined circumstances. Consider "clickwrap" consent where user has to take positive action to signify consent rather than "browsewrap", where consent is inferred/deemed
- Charities and NFPs should limit/avoid collecting personal information from children and should obtain consent from parents or guardians of children under the age of 13
- The organization should have robust website terms and conditions to reinforce its privacy policy/practices, limit its liability, protect its intellectual property and other assets from loss and reputational damage and control the conduct of website users
- Organizations should have a social media policy and an acceptable use policy to control use/misuse of social media and technology resources by staff and volunteers so as to minimize risk of loss/reputational damage

19

- Organizations should have strong privacy safeguards in contracts with third parties, including the right to audit privacy compliance
- They should be transparent and open with stakeholders about use of third party vendors/ providers
  - Charities and NFPs utilizing cloud-based platforms, portals or otherwise transmitting personal information to service providers must use contractual or other means to provide a comparable level of protection for personal information being processed https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/cloud-computing
  - If personal information will be going outside of Canada, organizations must use clear and understandable language at the time of collection to advise individuals that their information may be processed in a foreign jurisdiction and may be accessed by authorities in that jurisdiction https://www.priv.gc.ca/en/privacy-topics/employers-and employees/outsourcing

www.charitylaw.ca www.carters.ca

20

KEY TAKEAWAYS

- Charities and NFPs operating online must:
  - Recognize that they are potential cyber targets
  - Empower and educate staff/volunteers to recognize and avoid attacks
  - Build a culture of vigilance against both external and internal threats
  - Identify gaps and weaknesses
  - Proactively implement and update cybersecurity measures
  - Build a culture of privacy and training
  - Abide by basic privacy law and best practices
  - Develop clear privacy policies and back them up with a strong privacy compliance program
  - Develop incident response plans
  - Obtain cybersecurity insurance

www.charitylaw.ca www.carters.ca

CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.

CARTERS PROFESSIONAL CORPORATION
TOLL FREE: 1-877-942-0001
Ottawa Toronto Orangeville
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca