CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

The Ottawa Region 2021
Charity & Not-for-Profit Law
Webinar
February 11, 2021

Critical Privacy and Security Risks in a Virtual World

Esther Shainblum, B.A., LL.B., LL.M., CRM

eshainblum@carters.ca
1-866-388-9596

A. INTRODUCTION

- Unprecedented numbers of people are working from home ("WFH") due to the Covid-19 pandemic
- The new WFH reality has exposed organizations, including charities and NFPs, to additional privacy and security risks
- Unclear what the long term impact of the pandemic will be on how people work in the future - "office centricity is over" (see https://bit.ly/34K91WH)
- Charities and NFPs will continue to face privacy and security risks associated with WFH for the foreseeable future

3

B. THE PIVOT TO WFH

- At the beginning of the pandemic, the primary threat was to the physical safety of workers
- Abrupt pivot to WFH arrangements, seemingly overnight
- Many charities and NFPs were not prepared to manage the large scale, sudden shift to WFH
- Some charities and NFPs did not have the tools or infrastructure to support a remote workforce or their remote access infrastructure could not support the increased demand
- At the same time, charities and NFPs facing declining revenues due to the pandemic

4

C. THE RISKS OF WFH

- New normal of WFH means an unprecedented risk to organizations, including charities and NFPs
- Organizations more reliant on their technology and computer systems than ever before - but
- Multiple, dispersed remote work places make it more difficult for organizations to:
  - maintain security
  - monitor and enforce employee compliance with policies and procedures
  - keep track of sensitive information and who is accessing it
  - find out about and respond to privacy breaches

5

- Employees are working outside safeguards present in the workplace environment *e.g.* firewalls, anti-virus software, face-to-face contact, and policies and procedures designed to prevent or mitigate cyber and privacy breaches
- WFH makes it more difficult for employees to communicate with one another - more susceptible to phishing and social engineering
- WFH makes it harder to reinforce the need for vigilance and strict processes

6

- Additional risk factors:
  - Lack of adequate cybersecurity awareness training for WFH
  - Stretched or inadequate IT support
  - Employees WFH setting up and managing their own remote connections
  - Employees using personal devices, such as laptops, phones and USB drives, to access core IT systems and sensitive work information
  - Organizations without secure remote access, such as virtual private networks (“VPNs”)
  - Employees accessing core IT systems or sensitive workplace information using poorly secured home internet connections

7

- Employees sharing computers, devices and workspaces with family members/roommates
- Employees installing software on corporate devices
- Relaxing the rules, not following usual processes or policies
- The use of free platforms that may not have adequate security
- No clear plan for what to do in case of an incident when WFH
- Corporate policies that do not address or reflect WFH

8

D. THE SURGE IN CYBERCRIME

- Cybercrime has surged globally as a result of the shift to WFH and home based networks
- Since Covid cyberattacks have increased at a rate of three to five times and phishing attempts have increased in both frequency and sophistication (see https://hbr.org/2020/05/)
- Coronavirus "possibly largest-ever cyber security threat" due to the total volume of cyber attacks related to the pandemic (see https://bit.ly/3oUbAxs)
  - 667% increase in cyber attacks in USA March, 2020
  - April, 2020 FBI reported a 400% spike in cybersecurity complaints

9

- The Canadian Internet Registration Authority (CIRA) reported an increased volume of cyber attacks during the pandemic (see https://bit.ly/322nQ4W)
- Canada was the most frequently targeted country for phishing attacks during the first quarter of 2020 and there was a 25% spike in ransomware attacks in Canada in the first quarter of 2020.
- In July 2020, Blackbaud revealed that it had been the subject of a ransomware attack that impacted charities around the world, including many in Canada

10

- Cybercriminals are taking advantage of the pandemic in multiple ways:
  - Leveraging the massive shift to poorly secured home networks and devices to attack and compromise organizations' systems:
    - Weak passwords, out of date or insecure devices and software and the lack of layers of authentication or protection can make an organization vulnerable to attack
  - Using deception and manipulation to bypass defenses and safeguards and to gain entry or data, including:

11

Phishing – exploiting COVID fear and anxiety by pretending to be a trustworthy entity and sending pandemic-themed phishing emails to trick people into clicking links or fake websites or downloading attachments that contain malware or ransomware

Spear phishing – similar to phishing but well-researched and targeted toward a specific individual or organization

CEO Fraud – a similar scam, impersonating senior executives to trick people into transferring funds or downloading malware

Clickbait – pretending to offer something such as free healthcare advice about COVID

www.charitylaw.ca www.carters.ca

12

E. MITIGATING THESE RISKS

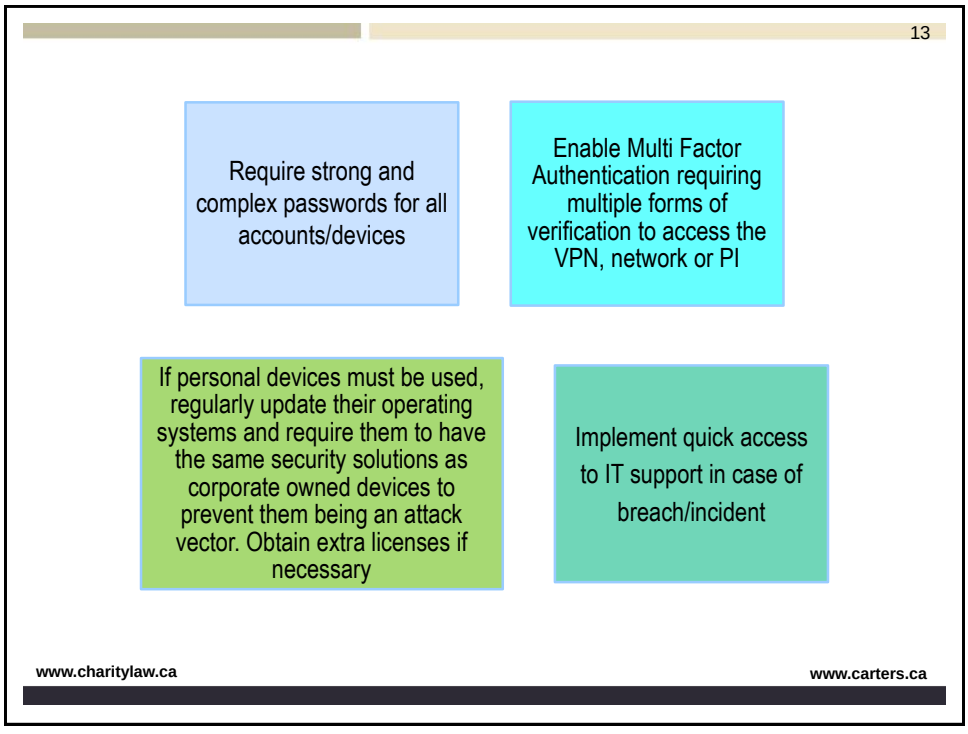
- Charities and NFPs need to consider a number of measures to mitigate the risk of data loss, privacy breach or cyber attack
- Technological measures such as:

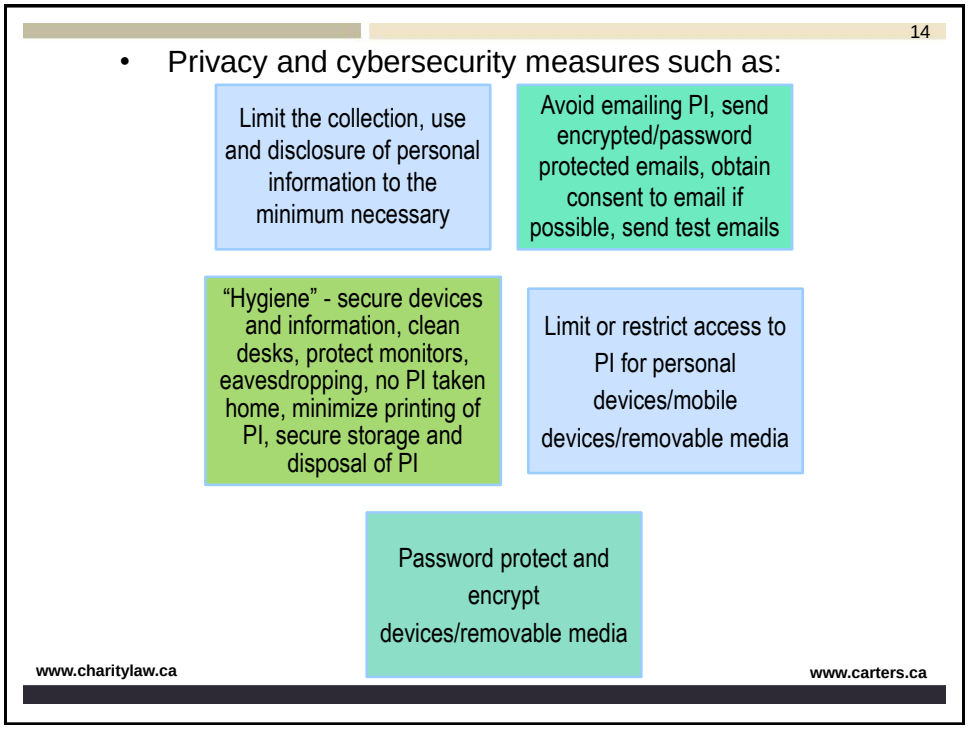
Provide employees WFH with corporate-owned devices managed and controlled by the organization

Proactively audit and test for vulnerabilities and regularly deploy updates and patches to address them

Use a VPN to create a secure connection between remote workers and the organization's network/sensitive data

www.charitylaw.ca www.carters.ca


13
Require strong and complex passwords for all accounts/devices
Enable Multi Factor Authentication requiring multiple forms of verification to access the VPN, network or PI
If personal devices must be used, regularly update their operating systems and require them to have the same security solutions as corporate owned devices to prevent them being an attack vector. Obtain extra licenses if necessary
Implement quick access to IT support in case of breach/incident
www.charitylaw.ca
www.carters.ca


14
• Privacy and cybersecurity measures such as:
Limit the collection, use and disclosure of personal information to the minimum necessary
Avoid emailing PI, send encrypted/password protected emails, obtain consent to email if possible, send test emails
"Hygiene" - secure devices and information, clean desks, protect monitors, eavesdropping, no PI taken home, minimize printing of PI, secure storage and disposal of PI
Limit or restrict access to PI for personal devices/mobile devices/removable media
Password protect and encrypt devices/removable media
www.charitylaw.ca
www.carters.ca

15

- Training and Policy measures such as:

Establish a WFH policy that sets out expectations and responsibilities for employees WFH

Review and update technology policies as needed to address WFH

Adapt and enforce privacy policies to ensure that employees WFH continue to comply with privacy law and policies

Have clear privacy breach and security incident response protocols in place

Implement mandatory cybersecurity awareness on cybersecurity threats, phishing, WFH securely and how to video conference securely

Conduct cybersecurity awareness training on a regular, ongoing basis

Obtain adequate cyber insurance coverage to protect the organization against cyber-crime and fraud

www.charitylaw.ca www.carters.ca

16

F. KEY TAKEAWAYS

- WFH is here to stay, at least for the immediate future
- Charities and NFPs should be implementing measures to mitigate the risks associated with WFH
- Takeaways:
  - Employee education and cybersecurity awareness
  - Incident response plan
  - Enable MFA
  - Eliminate/reduce personal devices
  - VPNs
  - Cyber insurance coverage
  - Home office hygiene

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