

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

**The Annual 2020
Church & Charity Law™ Webinar
Goes *Virtual* - November 5, 2020**

**MITIGATING PRIVACY AND
SECURITY RISKS IN A
VIRTUAL WORLD**

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


eshainblum@carters.ca
1-877-942-0001

© 2020 Carters Professional Corporation

CARTERS PROFESSIONAL CORPORATION
BARRISTERS . SOLICITORS . TRADEMARK AGENTS
TOLL FREE: 1-877-942-0001

Toronto Ottawa Orangeville

www.carters.ca www.charitylaw.ca www.churchlaw.ca

 <p>BARRISTERS SOLICITORS TRADEMARK AGENTS</p>	<p>The Annual Church & Charity Law™ Webinar <i>Goes Virtual</i> – November 5, 2020</p>
<p>Mitigating Privacy and Security Risks in a Virtual World</p> <p>Esther Shainblum, B.A., LL.B., LL.M., CRM eshainblum@carters.ca 1-866-388-9596</p> <p>© 2020 Carters Professional Corporation</p>	
<p>CARTERS PROFESSIONAL CORPORATION TOLL FREE: 1-877-942-0001</p>	<p>Toronto Ottawa Orangeville www.carters.ca www.charitylaw.ca www.churchlaw.ca</p>

	2
<p>A. INTRODUCTION</p> <ul style="list-style-type: none">• In the wake of the COVID-19 pandemic, unprecedented numbers of people are working from home (“WFH”)• According to Statistics Canada, 4.7 million Canadians who do not usually WFH started to as a result of the pandemic (see https://bit.ly/2HQltdm)• The new WFH reality has exposed organizations, including charities and NFPs, to additional privacy and security risks• As the pandemic drags on into its ninth month, many charities and NFPs are still dealing with the implications of the abrupt shift <p>www.charitylaw.ca www.carters.ca</p>	

- Until there is a vaccine, it is unlikely that people will be returning to the office in large numbers
- Moreover, it is also unclear what the long term impact of the pandemic will be on how people work in the future
- Many employees may choose to work remotely on a permanent basis as “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

B. THE PIVOT TO WFH

- At the beginning of the pandemic, the primary threat was to the physical safety of workers
- Social distancing requirements and mandatory closures of non-essential workplaces sprung up overnight
- In many organizations, WFH arrangements were hastily assembled
- Many charities and NFPs were not prepared to manage the large scale, sudden shift to WFH:
 - No time for risk assessments, to audit home environments for vulnerabilities or to put safeguards in place

- Could not check the security of their employees' computers or internet connections
- Many charity and NFP employees had no access to corporate-owned devices and were using personal devices to access core IT systems
- 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 and the inability to fundraise due to the pandemic

C. THE RISKS OF WFH

- The unprecedented number of people WFH means an unprecedented risk to organizations, including charities and NFPs
- These risks include:
 - Employees 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
 - Multiple, dispersed remote work places make it more difficult for organizations to:
 - maintain security
 - monitor and enforce employee compliance with policies and procedures

7

- keep track of sensitive information and who is accessing it
- find out about and respond to privacy breaches
- Stretched or inadequate IT support
- Some may require employees WFH to set up and manage their own remote connections
- Employees using personal, less secure home devices, such as laptops, phones and USB drives, to access core IT systems and sensitive work information

www.charitylaw.ca

www.carters.ca

8

- Organizations not putting in place secure remote access, such as virtual private networks (“VPNs”), to allow employees to securely access the workplace
- Employees accessing core IT systems or sensitive workplace information using poorly secured home internet connections
- Corporate policies, such as those regarding confidentiality, privacy and the use of personal or corporate devices, that do not address or reflect WFH
- Organizations not providing employees with additional cybersecurity awareness training when WFH

www.charitylaw.ca

www.carters.ca

- WFH making it more difficult for employees to communicate with one another, *e.g.* to verify email instructions, making them more susceptible to phishing and social engineering
- Employees WFH may not have a clear protocol to follow for cybersecurity incident or breach WFH, may not know how/may not be able to get help on an urgent basis
- Employees sharing computers, devices and workspaces with family members/roommates
- WFH making it harder to reinforce the need for vigilance and strict processes

- WFH relaxing or making it harder to follow the rules that normally apply at the workplace, *e.g.* not keeping devices, passwords and documents secure, not following usual processes or policies
- Increased volume of video conference calls that may discuss confidential information or make sensitive information visible, and the use of free platforms that may not have adequate security, *e.g.* Zoom Bombing
- Employees WFH potentially exposing their own personal information (“PI”) *e.g.* through video calls

D. THE SURGE IN CYBERCRIME

- Cybercrime has surged globally as a result of the shift to WFH and home based networks
- 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.
- 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

- 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:

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

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

Require strong and complex passwords for all accounts/devices

Consider 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

17

- 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

18

- 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

F. CONCLUSION

- WFH is here to stay, at least for the immediate future
- Nearly nine months into the pandemic, charities and NFPs should be implementing measures to mitigate the risks associated with WFH
- Take aways:
 - Update policies
 - Eliminate/reduce personal devices
 - VPNs
 - Phishing and cybersecurity awareness
 - Home office hygiene

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.

© 2020 Carters Professional Corporation