 <p>BARRISTERS SOLICITORS TRADEMARK AGENTS</p>	<h2>Carters Spring Charity and Not-for-Profit Law Webinar</h2> <p>March 2, 2023</p>
<h3>Preparing for a Cyber Attack and Data Breach – Why Charities & NFPs Need an Incident Response Plan</h3> <p>By Esther Shainblum, B.A., LL.B., LL.M., CRM eshainblum@carters.ca 1-877-942-0001</p> <p>© 2023 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

OVERVIEW



- Introduction
- Cyber Threat Actors
- All Organizations are Vulnerable
- Why an Incident Response Plan (IR Plan)?
- Duties and Obligations of Directors
- Framework for Development of IR Plan/Team
- Some Key Elements of an IR Plan

www.carters.ca www.charitylaw.ca

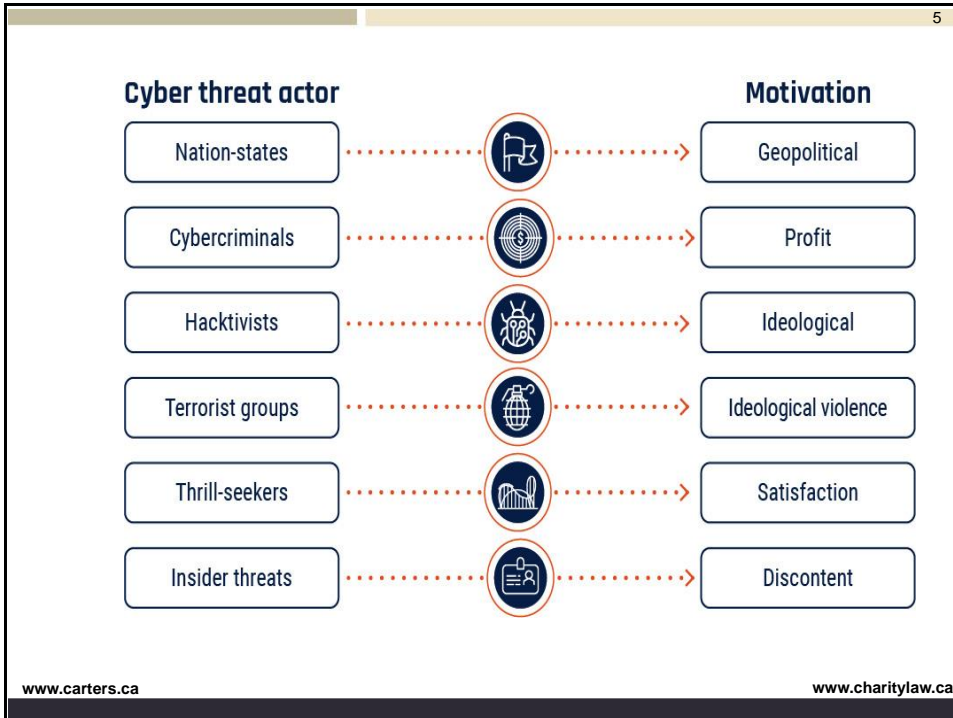
A. INTRODUCTION

- A cybersecurity incident is a matter of “when” not “if”
- Charities and Not-for-Profits (NFPs) need to be ready to respond appropriately and effectively to an incident when it occurs
- Canadian Centre for Nonprofit Digital Resilience – NFPs face many of the same cybersecurity threats as other Canadian organizations including ransomware attacks, phishing attacks, and data breaches. Other threats, including accidental or natural hazards (e.g. fires, floods), can put digital information and systems at risk
- Having a tested incident response plan (IR Plan) in place will allow a charity or NFP to better handle, respond to and recover from a cybersecurity incident
- An effective IR Plan can significantly reduce costs associated with cyber security incidents and help protect an organization’s reputation and stakeholder trust

B. CYBER THREAT ACTORS



- Canadian Centre for Cyber Security (CCCS) defines cyber threat actors as “groups or individuals who, with malicious intent, aim to exploit weaknesses in an information system or exploit its operators to gain unauthorized access to or otherwise affect victims’ data, devices, systems, and networks”
- Cyber threat actors can target vulnerabilities from anywhere in the world and can even be inside an organization
- The following slide are the types of cyber threat actors identified by CCCS



- 6
- ### C. ALL ORGANIZATIONS ARE VULNERABLE
- Cyber threat surface - Service arrangements, supply and vendor chains, the increased deployment of internet connected devices, remote working, information flow and human error can all be targeted by cyber threat actors to gain access to an organization's information systems
 - The Ponemon Institute's "Cost of a Data Breach Report 2022" reported that ransomware caused 11% of breaches, destructive malware caused 17%, 19% were caused by supply chain attacks and human error caused 21% of breaches
 - Phishing, business email compromise and third party software vulnerabilities were among the most common attack vectors
- www.carters.ca www.charitylaw.ca

- According to Ponemon, in 2022 it took an average of 207 days to identify a breach and 70 days to contain the breach – “data breach lifecycle”
- The shorter the data breach lifecycle, the less expensive the breach
- The average time to identify and contain ransomware and destructive malware attacks was significantly higher than average
- Phishing, business email compromise and supply chain attacks also took longer to identify and contain
- The global average cost of a data breach reached an all time high in 2022, with Canada being the third highest at \$5.64 million USD per data breach, an increase of 4.4% from 2021

D. WHY AN INCIDENT RESPONSE PLAN (IR PLAN)?

Ponemon 2022 - Developing and testing IR plans is one of the most effective ways to mitigate the cost of a data breach

Ponemon 2022 - Organizations that had regularly tested IR teams/plans in place reported significantly lower average costs of a data breach – average of 58% lower or \$2.66 million USD

83% organizations reported more than one cyber incident

9

E. 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 could be found personally liable for any loss that the corporation suffers as a result of a breach of fiduciary duty

www.carters.ca www.charitylaw.ca

10

- Directors of charities and not-for-profits can be found liable in tort for negligent mismanagement if their carelessness in the oversight of the corporation's operations leads to injury
- Directors and officers who fail to put sufficiently robust measures in place to protect personal information 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 cyber security risks

www.carters.ca www.charitylaw.ca

11

→

To show they met the duty of care, directors and officers of charities and not-for-profits should take steps to ensure that the organization puts in place appropriate safeguards to protect personal information and to prepare for and respond to privacy breaches and cyber attacks [not exhaustive]

→




“Business Judgment Rule” – The courts will not second guess directors who acted prudently and on a reasonably informed basis. Perfection is not required.

www.carters.ca
www.charitylaw.ca

12

F. FRAMEWORK FOR DEVELOPMENT OF IR PLAN/TEAM

- Basic principles/activities an organization can apply to develop an IR Plan team [based on National Institute of Standards and Technology (NIST) framework, SANS Institute Handbook and CCCS]
- Not “one size fits all” – organizations must customize to their own individual risk exposures and tolerances
- But provides flexible framework for developing IR Plan and teams

www.carters.ca
www.charitylaw.ca

1. Prepare

- Organizations must understand their individual business context, resources and cyber security risks

This phase includes – Inventory of data and information systems – *e.g. location of data, critical functions, resources, who has access to what, prioritize critical data assets*

Risk assessment – *e.g. identify risks and gaps*

Develop policies and procedures – *e.g. IT governance, reporting*

Develop IR Plan strategy – *e.g. how to identify and contain a breach, roles and responsibilities, communications plan*

- Establish response team – *cross functional e.g. IT, executive, communications, legal*
- Train and educate employees – *e.g. anti-phishing, testing, drills, central point of contact*
- Put in place appropriate physical, administrative and technological safeguards to limit or contain the impact of a potential cybersecurity event, *e.g.:*

- *Hardware, software*

- *Regular backups*

- *Physical security/workplace policies*

- *Identity management and access control measures*

- *Asset tracking and endpoint management of devices*

2. Detect/Identify Cyber Security Incident



- As per Ponemon, timely discovery of cyber security incidents is crucial to responding and keeping damage and costs down
- The shorter the data breach lifecycle, the less expensive the breach
- The organization must put in place functions/mechanisms/supports that will allow it to gather data from various sources to find anomalies and deviations
 - e.g. continuous monitoring, audits, firewalls, intrusion detection systems, anti-virus alerts, client complaints
- Analyze to determine whether an event is a threat – not every event is a cyber security incident
- If identified as a threat – activate IR Plan

3. Respond/Contain/Eradicate

- Implement IR Plan team to contain impact of cyber security incident and prevent further damage
- Must take proper steps and involve the right people – acting hastily or in panic can make it more difficult to contain, preserve evidence and recover
- Identify root cause, remove threats – short and long term fixes
- Includes: e.g. activating IR Plan, retaining legal counsel to preserve privilege, contacting external forensic investigators/IT security consultants, contacting insurer, isolating affected workstations/systems, disabling connectivity, shutting down employee access, restoring systems from backup


4. Recover/Understand/Lessons Learned


- Timely recovery to normal operations is essential to reduce impact of the cyber security incident.
Includes:
 - Ensure that the threat was eradicated
 - Ensure integrity of system has been fully restored
 - Determine scope of the incident, what data/information was compromised, whether there are any legal obligations (e.g. breach notification) or contractual rights/obligations that must be enforced or fulfilled
 - Take steps to patch/address/replace the vulnerability that led to the breach in the first place


- Identify areas for improvement in systems, security controls
- Preserve evidence and document the entire incident including when and how the breach was detected, all steps taken to eradicate it, what data was affected etc.
- Breach notification if legally required or if deemed advisable (legal advice)
- Analyze/discuss lessons learned – amend IR Plan as needed to correct flaws and prepare for next time


19


G. SOME KEY ELEMENTS OF AN IR PLAN

- 

Emergency contact list – who should be contacted in event of a breach and who does what (e.g. contacting forensics team, legal, consultants etc.)
- 

Technical steps such as how to do system restore from backup, process for disconnecting from the internet, who decides
- 

Diagrams/descriptions of the IT system
- 


Processes for preserving evidence such as logs and timestamps
- 

Make sure everyone has a hard copy as well as an electronic copy for obvious reasons

www.carters.ca www.charitylaw.ca

20

H. TEST IR PLAN

- Important to do regular testing exercises of the IR Plan to build “muscle memory” and resilience
- Tabletop exercise – have all IR Plan team members gather to discuss possible breach scenarios and responses
- 
 - Walk through simulation – walk through the plan to see if it works – call the different phone numbers, see how long it would take to find the appropriate people, how long it would take them to accomplish their assigned tasks
 - Realistic – create a simulated threat or interruption, see how the IR Plan works, debrief and generate feedback about how the IR team functions
 - May need outside experts/facilitators to assist with testing, debrief, feedback

www.carters.ca www.charitylaw.ca

I. KEY TAKEAWAYS



Experiencing a cyber security threat is “when” not “if”



Directors and officers of charities and not-for-profits need to ensure that the organization puts in place IR Plans to respond to privacy breaches and cyber attacks



Key steps include Prepare, Detect, Respond and Recover – there is no one-size-fits-all solution, charities and NFPs must tailor their IR Plan to their own needs and risk exposures



Regular testing of its IR Plan will allow a charity or NFP to better handle, respond to and recover from a cybersecurity incident

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.

© 2023 Carters Professional Corporation