NRC·CNRC

NRC.CANADA.CA

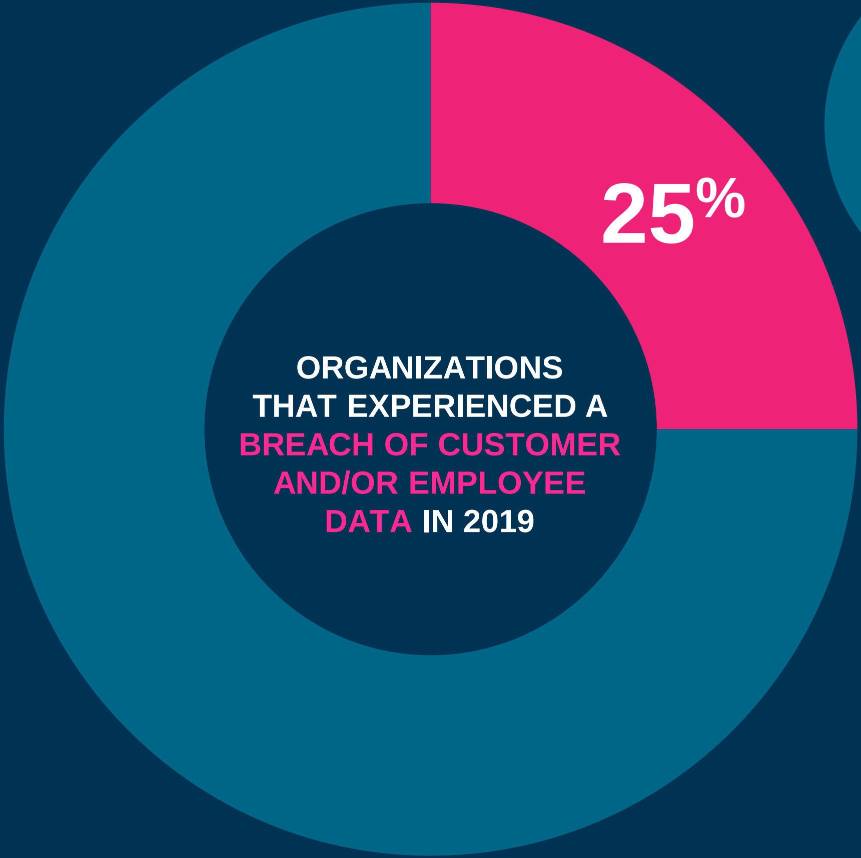
CYBER SECURITY + INNOVATION:

DE-RISKING FOR CPAS AND SMB CLIENTS

CPA Alberta Innovation, Technology and Accounting Conference Feb. 22, 2021

NRC IRAP · Author: Paul Erskine · Revision: 2.1

Canadian SMBs are a key target for cyber criminals seeking money through ransomware attacks



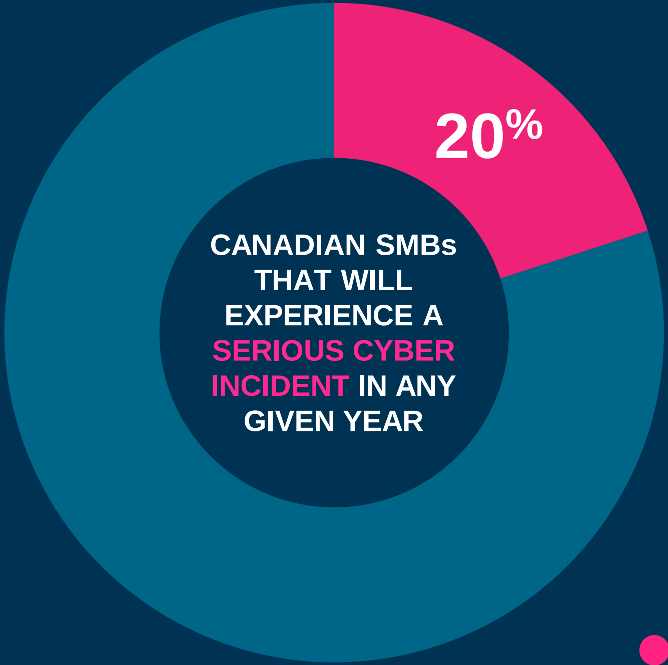
ORGANIZATIONS THAT EXPERIENCED A BREACH OF CUSTOMER AND/OR EMPLOYEE DATA IN 2019

AVERAGE COST OF A DATA BREACH:

$3.86

MILLION USD

Ponemon Institute



CANADIAN SMBs THAT WILL EXPERIENCE A SERIOUS CYBER INCIDENT IN ANY GIVEN YEAR

Cyber security is one of the most serious economic and national security challenges we face

Honourable Harjit Sajjan
Minister of National Defence

Why firms need to take cyber security seriously

- Cyber attacks on Canadian SMBs have **increased dramatically** (~300%) in 2020
- **SMBs are a prime hacking targets** — cyber criminals heavily target SMBs due to their lack of expertise in cyber security
- **Canadian SMBs are regularly targeted** because they are seen to have both IP and funding
- ~60% of SMBs who have to suspend operations after a cyber attack are **forced out of business**
- State-sponsored IP theft through cyber espionage costs the global economy **hundreds of billions of dollars annually**
- Google identified **18 million daily malware and phishing emails** related to Covid-19 in April, 2020

CYBER ATTACKS

COMMON ENTITIES INVOLVED IN CYBER ATTACKS ON SMBs

- ORGANISED CRIME SYNDICATES
- LONE WOLF HACKERS
- STATE SPONSORED HACKING UNITS
- DISGRUNTLED EMPLOYEE / EX-EMPLOYEE

THEIR GOAL/S

- $$$$$$
- IP THEFT
- DISRUPTION
- POLITICAL STATEMENT

95%

OF MALWARE IS DELIVERED BY EMAIL (PHISHING) · VERIZON

Phishing emails

Phishing is one of the most common attack vectors used by cyber criminals to deliver malware, steal IP (state sponsored actors) and hit firms with ransomware.

Many phishing emails are generic and very easy to detect.

But cyber criminals and state sponsored actors now use very sophisticated tactics. They will study your website and the website of your suppliers and clients to understand who their senior team compositions.

Phishing emails

Cyber criminals will steal logos and use email spoofing to send emails that appear to be from senior executives within your firm or a known employee at a supplier/client. The email will use the employee’s name and often their signature block. The email will use email header spoofing to appear to be legitimate (i.e. the return email address will appear to be legitimate).

The target is often lured into thinking the email is legitimate and actions the request in the email (workflow, link, attachment etc), exposing the firm to the attack.

There are ways to protect your firm against such attacks. They will be detailed in the next slide.

EXAMPLES OF SMB CYBER INCIDENTS + HOW THEY MIGHT BE PREVENTED

Cyber incident • Example 1

Firm receives an invoice from a supplier and pays it without verifying its legitimacy — it was phony.

How this might be prevented

- Make it company policy to verify all payment details and bank account changes. The verification process should include a phone call.
- Train staff in how to identify a phishing email.
- Have a phishing email escalation procedure.
- Consider disabling macros on Word, Excel etc as these are common attack vectors.

Cyber incident • Example 2

An executive assistant receives an SMS (text message) on their cell from the CEO asking to purchase online Amazon gift cards for them. The EA actions the request without realizing a hacker is using *Caller ID spoofing* to appear to be the CEO.

How this might be prevented

- Cyber security training for staff.
- Within this training, make staff aware of the Caller ID spoofing threat. It is easy to duplicate someone’s cell number on the internet, and call and SMS from what appears to be that number.

Cyber incident • Example 3

A executive has their Office365 or G Suite account compromised and sensitive information is stolen.

How this might be prevented

- All accounts should be protected using multi-factor authentication (easy to do).

Cyber incident • Example 4

**Due to poor cyber security, a firm is hit by a ransomware attack.
The firm does not backup systems, so cannot rollback to a backup.**

How this might be prevented

- Implement basic cyber security best practices.
- Ensure all systems and data are regularly backed up using an automated process.

Cyber incident • Example 5

A laptop containing confidential client information is stolen. The data is released on the web.

How this might be prevented

- Enact a policy to ensure all work systems including laptops are encrypted.
- If an encrypted laptop is stolen, the data will still be secure (provided a suitably complex password has been used).
- For an unencrypted laptop, it is easy to remove the storage drive and access the data on the drive — no password required.

Cyber incident • Example 6

A firm sold obsolete computers and mobile devices to a recycler. The recycler decided not to recycle but instead sold the devices on to customers. The hard drives had not been wiped, and confidential data was subsequently leaked on the web or to the press.

How this might be prevented

- Have a policy to ensure obsolete devices have their drives destroyed or securely wiped (not just deleted or formatted as that is easy to un-do) before being recycled or disposed of.

Cyber incident • Example 7

A firm allows employees to connect their personal cell phones to the work network. An employee connects to a compromised website which downloads malware to their phone. The malware uploads to the work network, compromising it.

How this might be prevented

- Due to security risk, move cell phones off the firm’s network to a new locked-down network that does not have access to sensitive firm info or systems.

Cyber incident • Example 8

Firm tells a client to send highly sensitive information via email using a password-protected file. The email is intercepted. The criminal entity uses a widely available password-cracking tool to crack the password and threatens to release the data on the web unless a large ransom is paid.

Also, be aware that sharing a cloud drive link can be dangerous unless multi-factor authentication is employed to ensure only legitimate recipients access the links.

How this might be prevented

- Have a policy and workflow on how to share sensitive information with an outside party in a secure manner.
- E.g. one possible option is using Box.com. Box allows for advanced security including multi-factor authentication and recipient authentication.
- Box.com allows data to be stored in Canada in either Toronto or Montreal. Ensure you configure it correctly; these options are not default. Box.com is heavily used by Fortune 500 firms.

HIGH-LEVEL BREAKDOWN OF COMMON CYBER INCIDENT CAUSES

- PHISHING EMAILS
- UNPATCHED SOFTWARE
- LACK OF CYBERSEC TRAINING FOR STAFF
- CALLER ID SPOOFING
- POOR SECURITY CONFIGURATIONS
- POOR NETWORK/ SYSTEM SECURITY
- POOR WEBSITE/ CLOUD SECURITY
- POOR MOBILE DEVICE CONFIG

RECOMMENDATIONS + RESOURCES

Top 10 recommendations

This slidedeck contains a lot of important cyber security best practice recommendations. If that is somewhat overwhelming, find a short list of some of the top recommendations below.

1. Install anti-virus/anti-malware software on every computer and mobile device (cell phones, tablets etc)

2. Have a patch policy and ensure it is followed to ensure systems/software/routers/firewalls etc are regularly patched

3. Use multi-factor authentication (MFA) as much as possible — most email systems, web accounts offer it — use it

4. Have regular cyber security training for staff — at least annual cyber security training for all staff, and mandatory cyber security training for new staff

Top 10 recommendations

5. Have a policy on how to share sensitive information to internal staff and outside parties in a secure manner, train staff on it
6. Ensure Wi-Fi routers/firewalls are used and configured for optimum security
7. Ensure remote working staff connect using a VPN (Virtual Private Network)
8. Configure your email system to add a message to flag outside emails as ‘EXTERNAL EMAIL – USE CAUTION’ (in a standout color)
9. Conduct regular phishing simulation exercises to help train staff on how to identify phishing emails
10. Implement a comprehensive automated backup process

CyberSecure Canada

CyberSecure Canada is a cyber security certification program, created by a number of Canadian federal bodies, to assist firms in achieving a solid cyber security posture.

- The program will test firms against 13 baseline cyber security controls (link) devised by the Communications Security Establishment (CSE; federal entity). The 13 controls focus on cyber security best practice for small companies.

- Complying with the controls will take considerable work, but is highly worthwhile. Consider the cost of a breach vs the cost of achieving this certification.

CyberSecure Canada

- Firms that achieve the certification can use the CyberSecure Canada certification on their website and marketing material.
- The certification lasts two years. The test needs to be retaken every two years to maintain your certification (note: there are plans to require retesting every year; please check the program’s website for updates).
- The test fee is dependent on the vendor selected to do the test.
- For further information, please see: link

Useful Cyber Security Resources

- CPA Canada's cyber security tools and resources · link
- Canadian Centre for Cyber Security · link
- CyberSecure Canada · link
- Get Cyber Safe · link
- Canadian Centre for Cyber Security — Baseline Cyber Security Controls for Small and Medium Organizations · link
- CIRA Canadian Shield · link
- U.K.'s National Cyber Security Centre - Small Business Guide to Cyber Security · link
- U.S. Federal Communications Commission (FCC) - SMB Cyber Security Planning Guide · link
- U.S. National Institute of Standards and Technology (NIST) — Information Security for Small Business: The Fundamentals · link

THANK YOU + QUESTIONS