Cyber Security Best Practices for Canadian Small and-Medium-Sized Businesses

Cyber attacks on Canadian small-medium sized businesses (SMBs) are becoming increasingly regular. SMBs are particularly attractive targets for cybercriminals often due to a lack of resources and reluctance to invest in cyber security. The Canadian economy is made up predominantly of small businesses making it particularly vulnerable.

Some important stats:

- In 2018, 58% of cyber attack victims were small businesses (Verizon)
- Around 60% of small businesses who have to suspend operations after a cyber attack never recover from the attack and are forced out of business (Hiscox)
- The average cost of a cyber incident to an SMB is $200,000 (Hiscox)
- The majority of SMB cyber attacks are phishing/social engineering based
- Many SMBs do not configure their software and operating systems for automatic updates, exposing them to multiple attack vectors through unpatched software
- One in fifty emails contains malware or is a phishing attack
- On average, IoT (Internet of Things) devices added to the internet are probed for vulnerabilities within 24 hours of being installed

It is critical Canadian SMBs understand cyber threats and implement best practices to help prevent them. A basic foundation of cyber security best practices need not take a lot of time or resources to implement, and can be done for a relatively small cost.

There is a wealth of cyber security best practice guidance available on the web, however finding the best sources can be difficult and timeconsuming. This document endeavors to simplify the process by highlighting best-in-class SMB cyber security guidance and resources.

The following links provide comprehensive solutions for your consideration and implementation. These documents, and the other free cyber security resources offered by these organisations, are described in more detail in annex.

- Canadian Centre for Cyber Security - Baseline Cyber Security Controls for Small and Medium Organizations
- U.K.'s National Cyber Security Centre - Small Business Guide to Cyber Security

- U.S. Federal Communications Commission (FCC) - SME Cyber Security Planning Guide
- U.S. National Institute of Standards and Technology (NIST) - Information Security for Small Business: The Fundamentals

Another important aspect of cyber security for SMBs to consider, is training staff to be cyber aware and know how to recognize common attacks such as phishing and social engineering.

- Workforce Management Guidebook: Cybersecurity is Everyone's Job, published by the U.S. National Institute of Standards and Technology (NIST)

Some firms prefer help in implementing the recommended cyber security foundational best practices. There are dozens of Canadian firms that offer cyber security consultancy services. A simple Google search on "cyber security firm <your province>" should produce useful results. When considering a firm, look for practitioners with industry recognized qualifications such as CISM, CISSP, GSEC, GCED.

If your budget allows for it, engaging a cyber security firm for guidance and possibly some penetration testing is a worthwhile step.

Free Cyber Security Advice

The National Research Council of Canada Industrial Research Assistance Program (NRC IRAP) offers a limited number of no-charge cyber security advisory services for NRC IRAP clients through an agreement with In-Sec-M - a national cybersecurity cluster and non-profit organization

The services offered include advice/guidance on multiple cyber security areas including:

- Operational security
- Audits to identify cyber security gaps
- Security by design and other targeted audits
- Risk analysis, intrusion detection, penetration testing
- Identity theft protection, data privacy and privacy by design - PIPEDA, GDPR etc.
- Compliance to standards or regulations including NERC-CIP, PCI DSS, GLBA, HIPPA, SOX, FISMA, ISO 17799, COBIT.

If you are interested in potentially leveraging this program, please reach out to your NRC IRAP Industrial Technology Advisor (ITA) and tell them of your interest in engaging with the In-Sec-M cyber security program (inform your ITA that the program is run by ITA Renato Rosa).

Cyber Security Resources for Canadian Small and Medium-Sized Businesses

Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security has partnered with the Communications Security Establishment (CSE) to produce a useful guide for businesses titled Baseline Cyber Security Controls for Small and Medium Organizations. It tackles key cyber security topics for small and medium-sized businesses including:

- developing an incident response plan
- enabling automatic software updates
- security software
- device configuration
- authentication
- employee awareness/training
- data backup
- securing mobile device
- perimeter defence
- cloud and outsource IT service
- securing websites
- access control.

The guide condenses key cyber security principles into a compact 18 page guide, that when implemented by organisations will give them a sound security foundation.

The organisation also offers a wide range of cyber security articles and publications.

CyberSecure Canada

The Canadian federal government is rolling out a cyber certification program called CyberSecure Canada that will assess firms based on the security baseline as detailed in the CSE's Baseline Cyber Security Controls for Small and Medium Organizations document. Firm's that implement baseline security controls will be awarded the CyberSecure Canada certification. The program is led by Innovation Science and Economic Development Canada (ISED), in partnership with the Communications Security Establishment (CSE) and Standards Council of Canada (SCC). The program is currently in pilot phase. The fee for certification has not been published at this time.

Get Cyber Safe

Get Cyber Safe is an initiative by the Canadian federal government to increase cyber security awareness and knowledge. It has a wide range of useful content including:

- Get Cyber Safe Guide for Small and Medium Businesses

- Educate Your Employees on Cyber Safety
- Make yourself more cyber secure (in five simple steps)
- Common threats to be aware of

U.K. National Cyber Security Centre (NCSC)

The U.K.'s National Cyber Security Centre published a thorough 18-page Small Business Guide to Cyber Security. The guide provides cyber security guidance on a range of topics including:

- backing up data
- protection from malware
- keeping mobile devices safe
- using passwords
- avoiding phishing attacks.

U.S. Federal Communications Commission (FCC)

The U.S.'s Federal Communications Commission (FCC) have a comprehensive Cyber Security Planning Guide (51 pages) for SMBs, written in partnership with key industry players including Symantec, Microsoft, NIST and Sophos. It gives advice on key cyber security topics including:

- privacy and data security
- scams and fraud
- network security
- website security
- email
- mobile devices
- employees
- facility security
- operational security
- payment cards
- incident response and reporting
- policy development
- management.

The FCC also offers a Small Biz Cyber Planner, an online resource to help small businesses create customized cybersecurity plans, and a wealth of SME cyber security guidance.

U.S. National Institute of Standards and Technology (NIST)

The U.S. federal organisation the National Institute of Standards and Technology (NIST), offers a wide range of cyber security guidance. They have a comprehensive Information Security for Small Business: The Fundamentals guide (54 pages). NIST offers additional guidance at their Small Business Cybersecurity Corner. Their Cybersecurity Risks section discusses key cyber risks and ways to protect your organisation from those risks.

A key part of being cyber safe is educating your workforce, NIST offers a comprehensive guide to that - Workforce Management Guidebook: Cybersecurity is Everyone's Job.

NIST's website offers guidance on nearly every cyber security topic of interest to a SMB from Recovering from a Cybersecurity Incident, to Data Breach Response: A Guide for Business. It is a tier one resource for cyber security guidance and knowledge.

NIST also publishes and regularly updates their well-regarded Cybersecurity Framework. The framework is designed to leverage standards, guidelines, and best practices for organizations to better manage and reduce cyber security risk. The downside is that the framework is time consuming and often too costly for most SMEs to consider implementing.

U.S. Department of Homeland Security

The U.S.'s Department of Homeland Security offers a useful Cybersecurity Resources for Business.

Secure Your Website and Writing Secure Code

If your firm deploys a website or develops software code, it's important your developers understand software security principles and best practices including how to write secure code by design and, how to safeguard against common attack vectors. SAFECode, SANS Institute and OWASP (Open Web Application Security Project) offer resources to assist including:

- Framework For Secure Application Design and Development (SANS)
- Fundamental Practices for Secure Software Development - Third Edition (SAFECode)
- Developers Guide [to software security] (OWASP)
- Practices for Secure Development of Cloud Applications (SAFECode)
- Managing Security Risks Inherent in the Use of Third-party Components (SAFECode)
- Guidance for Agile Practitioners [on software security] (SAFECode)
- OWASP Top 10 Most Critical Web Application Security Risks [and how to counter/prevent them]
- Top 25 Most Dangerous Software Errors (SANS)
- Testers Guide [to software security] (OWASP)
- Code Reviewers Guide [to software security] (OWASP)

Internet of Things (IoT)

On average, IoT devices added to the internet are probed for vulnerabilities within 24 hours of being installed. Key tips: only use IoT devices from the most reputable vendors, change default passwords and enable automatic updates.

IoT cyber security resources:

- IoT Security Foundation Publications,
- IoT Security for Small and Medium Organizations,

- Securing Network Infrastructure Devices

Miscellaneous

Some useful miscellaneous resources:

- FTC: Data Breach Response: A Guide for Business
- NIST: Recovering from a Cybersecurity Incident
- Ransomware: How to Prevent and Recover
- Identity and data protection for AWS, Azure, and Google Cloud – Canada-based Sonrai Security offers a solution for this difficult area.
- Backblaze – U.S. based backup solution provider.