CyberCatch

15 Minute Guide

TO

CAN/CIOSC 104

Complying with the National Standard Baseline Cybersecurity Controls for Small and Medium Organizations

MARCH 2022

TABLE OF CONTENTS

Introduction and Overview

Here are a couple of concerning facts:

- In Canada, the average cost of a data breach is $5.4 million, per IBM's 2021 Cost of a Data Breach Study. This is a significant cost, especially for a small and medium-sized business (SMB).
- 84% of SMBs in Canada are vulnerable to spoofing, per CyberCatch's 2021 Small and Medium-Sized Businesses Vulnerabilities Report (SMBVR). Spoofing involves bad code in an Internet facing web site, web server or a web application that a cyber attacker can exploit to inject malicious scripts and gain access to user names, passwords or even a database.

RECENT HEADLINES

84%

Canadian SMOs Vulnerable to "Spoofing" Cyber Attack

SOURCE: CYBERCATCH SMBVR

"A quarter of small businesses in Canada say they have already experienced a cyber attack."

SOURCE: TORONTO STAR

"Canadian SMO healthcare provider hit with two ransomware attacks at once by two different attackers who exploited missing controls."

SOURCE: SOPHOS

$5.4M

Average Cost of a Data Breach in Canada

SOURCE: IBM

Small and medium-sized organizations (SMOs), who are for profit businesses or not-for-profit organizations, are especially vulnerable to a cyberattack, because they may not know what controls to implement, how to implement or more likely have outsourced their IT to a third party who may not have implemented the necessary controls and the SMO may be unaware of the security holes. So a cyber attacker can easily exploit the control weaknesses and break in, steal valuable data or inject ransomware and walk away with a hefty ransom payment.

This is why Canada's CIO Strategy Council (CIOSC) created CAN/CIOSC 104 National Standard Baseline Cyber Security Controls for Small and Medium Organizations. CIOSC is accredited by the Standards Council of Canada (SCC) to create national standards.

CAN/CIOSC 104 National Standard prescribes up to 55 cyber security controls for a SMO to minimally implement to mitigate cyber risk. ***An SMO is considered to be an organization with less than 500 employees, and cyber risk is the risk of adverse impact to earnings, capital or reputation from a cyberattack.***

Imagine the impact to you as an SMO if a cyber attacker tricks your employees via a phishing email to divulge confidential information or wire money or the attacker exploits a vulnerability on your web site and breaks in and steals all of your customers data or your valuable intellectual property.

Or the cyber attacker also injects ransomware and encrypts all of your computers and files and shuts down your operations and you are unable to recover and resume operations for weeks or months, unless you pay a hefty ransom payment in bitcoins. And even if you do pay the ransom, what if the cyber attacker does not provide you the keys to decrypt and suddenly disappears.

Complying with Canada's CAN/CIOSC 104 National Standard is not only the right thing to do as a Canadian organization, but also a smart thing to do as an SMO, so that you can mitigate cyber risk and continue to succeed in the digital world.

Level 1 and 2 Cyber Security Controls

Cyber security controls are either a policy, procedure or a technical control (e.g. encryption, anti-malware software, etc.) to prevent, detect or respond to a cyberattack.

Under the CAN/CIOSC 104 National Standard, the requirements for cyber security controls are broken out into two Levels:

- Level 1, comprised of 22 controls.
- Level 2, comprised of up to an additional 33 controls, for a total of up to 55 cyber security controls.

Level 1 is for smaller and lower inherent risk level SMOs. For example, if you are an SMO with one or a few employees with no web site or an informational web site only.

Level 2 is for all other SMOs. So you should implement the 22 controls in Level 1, but also up to an additional 33 controls for a total of up to 55 cyber security controls. For example, regardless of how many employees you have, if you have more than an informational web site, such as a transactional web site that accepts payments or a web site that has forms and connects to a database or have web servers or web applications that are Internet-facing, you should be at Level 2 and implement up to 55 cyber security controls.

Here are the number of Level 1 and 2 Cyber Security Controls in CAN/CIOSC 104 broken out by three Control Categories and eighteen Control Requirement Types:

Cyber Security Controls	Level 1	Additional Level 2	Total Level 2
Organizational Controls (14 Controls)			
Leadership	1		1
Accountability		1	1
Cyber Security Training	1	1	2
Cyber Security Risk Assessment	1	9	10
Total	**3**	**11**	**14**
Baseline Controls (31 Controls)			
Incident Response Plan	3		3
Automatically Patch Operating Systems and Applications	3		3
Enable Security Software	1		1
Securely Configure Devices	1	1	2
Use Strong User Authentication	3	1	4
Backup and Encrypt Data	5	1	6
Establish Basic Perimeter Defences		8	8
Implement Access Control and Authorization		4	4
Total	**16**	**15**	**31**
Baseline Controls by Operating Environment (10 Controls)			
Secure Mobility		2	2
Secure Cloud and Outsourced IT Services	1	1	2
Secure Websites		2	2
Secure Portable Media	1	1	2
Point of Sale (POS) and Financial Systems	1		1
Computer Security Log Management		1	1
Total	**3**	**7**	**10**
Total Level 1 and Level 2	**22**	**33**	**55**

The CAN/CIOSC 104 National Standard also provides in the Annex an Incident Response Plan Template and a Cyber Security Risk Assessment Questionnaire to help you implement the two Controls (i.e. incident Response Plan and Cyber Security Risk Assessment).

Here are examples of Cyber Security Controls prescribed under each of the three Control Categories and how these Controls could have blocked cyber attackers in recent attacks to illustrate the value of the Controls:

ORGANIZATIONAL CONTROL: CYBER SECURITY TRAINING.

CAN/CIOSC 104 prescribes following two controls under Level 1 and 2:

- **Level 1:** Train employees on basic security practices, including a focus on the following practical and easily implementable measures: a. The use of effective password policies; b. Identification of malicious emails and links; c. Use of approved software;
  d. Appropriate usage of the Internet; e. Safe use of social media
- **Level 2:** Invest in regular and ongoing cyber security awareness and training of employees.

A small City in Canada fell victim to a phishing email resulting in the loss of half a million dollars. A phishing email was sent to the City's staff requesting change of the banking account information of an established vendor.

The City's staff had not been properly trained to look for red flags of phishing, and made the change in the system, and subsequently, the wire transfer for half a million dollars was made to the new account controlled by the attacker.

BASELINE CONTROL: AUTOMATICALLY PATCH OPERATING SYSTEMS AND APPLICATIONS.

CAN/CIOSC 104 prescribes following three controls under Level 1:

- **Level 1:** Implement up-to-date security patches for all software and hardware; enable automatic patching for all software and hardware; perform a risk assessment whether to replace systems incapable of automatic patching.

A medium-sized healthcare organization in Canada fell victim to two ransomware attacks by two different ransomware gangs. First, the Karma gang demanded bitcoin payment and no less than a day later the Conti gang

attacked. Both gangs exploited unpatched vulnerabilities in IT assets such as servers to install the two different ransomware within a short period of time.

The organization did not have in place automatic patching and was behind in patching vulnerabilities, so the attackers were able to easily exploit the vulnerabilities to infect ransomware.

BASELINE CONTROL BY OPERATING ENVIRONMENT: SECURE WEBSITES.

CAN/CISOC 104 prescribes following two controls under Level 2:

- **Level 2:** Ensure websites address the OWASP Top 10 vulnerabilities; ensure the OWASP ASVS levels needed to meet for each website.

A small maritime research organization in Canada fell victim to a cyberattack by APT40, a gang sponsored by the Chinese Government's Intelligence Agency, where APT40 exploited vulnerabilities on the organization's website to easily break into the network, and eventually exfiltrated valuable intellectual property and trade secrets.

The organization was not scanning to detect OWASP Top 10 vulnerabilities and was unaware of the vulnerabilities existing on its website, which the attackers easily exploited to break into the network.

Recommended Path

While CAN/CIOSC 104 National Standard prescribes Level 1 with 22 controls for smaller and lower inherent risk level SMOs, and Level 2 with an additional 33 controls for a total of 55 cyber security controls for all other SMOs, all SMOs should minimally implement the 55 controls.

By implementing minimally the 55 cyber security controls, your SMO will attain a stronger and more reasonable defence against cyber attackers.

You may be concerned that you have limited knowledge of the controls or the time it may take or the cost to implement the 55 controls.

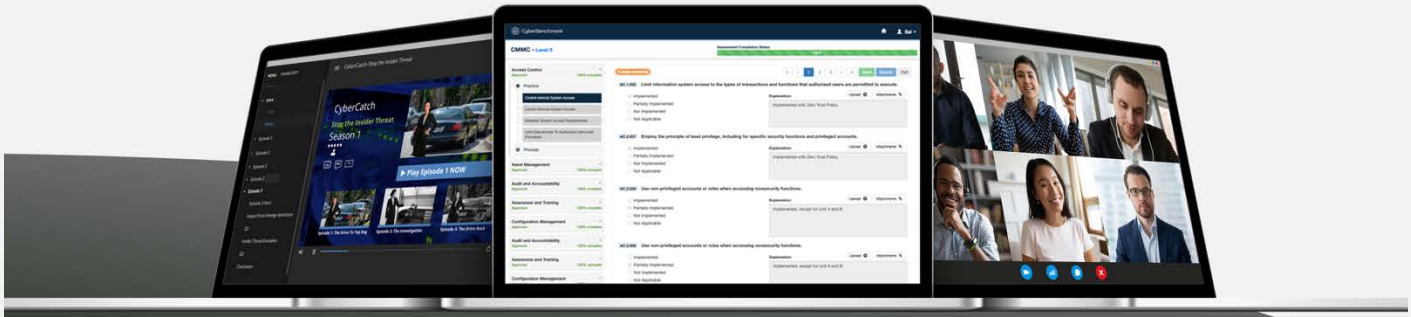
However, the key to success is to first understand the prescribed controls. Then:

- Consult with a cybersecurity expert who is knowledgeable about CAN/CIOSC 104 for guidance; or
- Subscribe to CAN/CIOSC 104 Compliance Manager.

STEP 1: COMPLIANCE ASSESSMENT

Implement up to 55 cyber security controls quickly and cost effectively with help from team of industry-leading cyber security experts.

INCLUDES IT ASSET TOPOGRAPHY, NATIONAL STANDARD CONTROLS SCORING, PLAN OF ACTION, SYSTEM SECURITY PLAN, AND MORE!



CyberThreatTV

Highly Engaging, Online Security Awareness Training, Updated Periodically

CyberBenchmark

Automated Cyber Security Assessment and Benchmarking Engine

CyberVirtualCISO

Industry-Leading Cyber Security Experts for Ongoing Consultation and Advice

AUTOMATICALLY GENERATES

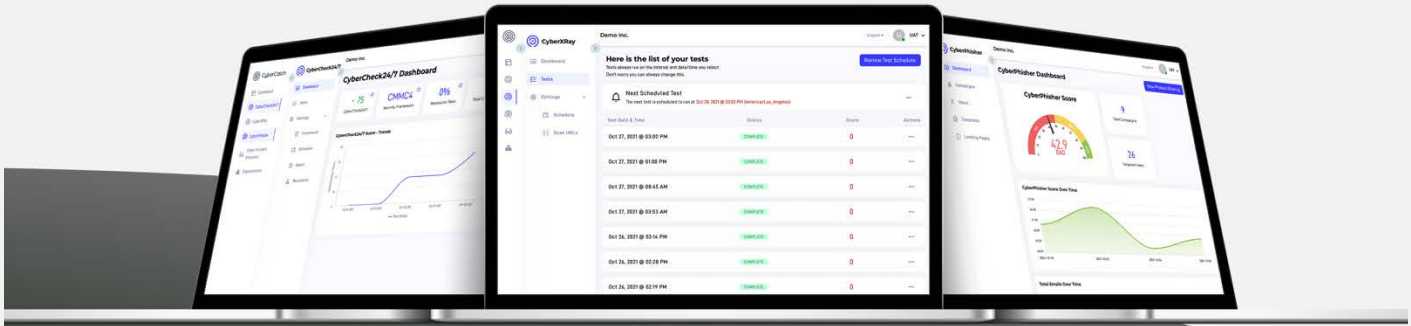
Cyber Hygiene Score

Always know your true compliance level so you can identify gaps and blind-spots to remediate promptly so you can remain fully compliant.

STEP 2: AUTOMATED CONTROLS TESTING

Automatically and continuously test the controls so you can find and fix control failures promptly and stay safe from attackers.

AUTOMATED CONTROLS TESTS UPDATED PERIODICALLY TO ADDRESS THE LATEST CYBER THREATS



CyberCheck24/7

Automated Inside-Out Testing of Implemented Controls / Practices

CyberXRay

Automated Outside-In Vulnerability Scans

CyberPhisher

Automated Phishing Susceptibility Testing

Per CAN/CIOSC 104 control requirement 4.4.3.9, you must periodically review and/or test cyber security controls to ensure effectiveness.

AUTOMATICALLY GENERATES

Cyber Breach Score

Always know your true cyber risk level and fix missing or broken security controls so you can avoid a data breach or ransomware attack.

Failing to Adopt

Cyber risk is an existential threat to SMOs. The cost of a data theft or ransomware attack may be so significant for your SMO, that you may not be able to continue operating – especially the impact from a ransomware attack.

Canada's Cyber Centre in its **Cyber Threat Bulletin: Ransomware Threat in 2021** stated "the impact of ransomware can be devastating, and the severity of the financial consequences related to a ransomware attack can be profound."

In the Bulletin, it reported it had knowledge of 235 ransomware incidents against Canadian victims from January 1 to November 16 in 2021, and stated "it is important to note, however, that most ransomware events remain unreported. Once targeted, ransomware victims are often attacked multiple times. The Cyber Centre continues to regularly observe high-impact ransomware campaigns that can cripple businesses and critical infrastructure providers."

EXAMPLE OF THE EXISTENTIAL THREAT FACED BY SMOs:

A 61-year old family owned back-office support services business comprised of 300 employees serving customers in U.S. and Canada, shut down permanently after attackers exploited flaws in website and web servers and inserted ransomware and encrypted all files and systems, and brought the operations to a complete halt. The owner decided to pay the ransom and obtained the decryption keys but the IT staff supporting the business even after several weeks could not decrypt all files and systems, and the owner and CEO decided to first suspend operations, but then ended up closing the business and laying off all employees.

EXCERPTS FROM THE LETTER SENT BY THE CEO TO EMPLOYEES:

"....Unfortunately, approximately two months ago our servers were attacked by malicious software that basically "held us hostage for ransom" and we were forced to pay the crooks to get the "key" just to get our systems back up and running. Since then, IT has been doing everything they can to bring all our systems back up, but they still have quite a long way to go. Also, since then, I have been doing my utmost best to keep our doors open, even going as far as paying your wages from my own money to keep us going until we could recoup what we lost due to the cyberattack. ....So here it is: The Company is temporarily suspending our services.....Please know that I am just as devastated as you all are, especially that we had to do this at this particular time of year.....Please know that we would have NEVER gone to this extreme if we were not forced to...."

Failing to comply with CAN/CIOSC 104 and implement necessary cybersecurity controls creates an inherent high cyber risk level for your SMO. You will have a higher chance of becoming a victim of a cyberattack with severe impact to your organization because of a weak defence. But if you adopt CAN/CIOSC 104 and minimally implement all of the 55 cyber security controls prescribed, your SMO will attain a strong defence and mitigate cyber risk.

WATCH THE DEMO

DOWNLOAD BROCHURE

Conclusion and Takeaways

As an SMO in Canada, you are increasingly vulnerable to a cyberattack. Unless you have implemented necessary prevention, detection and response controls, a cyber attacker will be able to easily exploit the control weaknesses and break in, steal valuable data or inject ransomware.

The impact to your SMO can be severe and devastating and you may never be able to recover from the cyberattack and the damage inflicted.

This is why Canada's CIO Strategy Council (CIOSC) created CAN/CIOSC 104 National Standard Baseline Cyber Security Controls for Small and Medium Organizations.

If you adopt CAN/CIOSC 104 and minimally implement all of the 55 cyber security controls prescribed, your SMO will attain a strong defence and mitigate cyber risk (i.e. the risk of adverse impact to earnings, capital or reputation from a cyberattack.)

Remember, the CAN/CIOSC 104 Compliance Manager, brought to you by Canada's CIO Strategy Council and powered by CyberCatch, is a complete solution for you as a SMO to quickly, easily and cost-effectively comply with the National Standard, including implementing all 55 controls.

Also, remember that complying with Canada's CAN/CIOSC 104 National Standard is not only the right thing to do as a Canadian organization, but also a smart thing to do as an SMO, so that you can mitigate cyber risk and continue to succeed in the digital world.

CyberCatch

About CyberCatch

CyberCatch is a unique cybersecurity Software-as-a-Service (SaaS) company that protects small and medium-sized businesses (SMBs) from cyberattacks by focusing on the root cause why SMBs fall victim: security holes. CyberCatch provides an innovative cloud-based SaaS platform coupled with deep subject matter expertise to help SMBs implement just the right type and amount of cybersecurity controls. The platform then performs automated testing of controls from three dimensions: outside-in, inside-out and social engineering. It generates the Cyber Breach Score to continuously measure cyber risk, and finds security holes and guides the SMB to fix them promptly, so attackers can't exploit any missing or broken controls to break in and steal data or infect ransomware. CyberCatch's continuous value proposition: Test. Fix. Secure.

For more information:

VISIT WEBSITE