Citizen FIRST

POWERED BY
Institute for
Citizen-Centred
Service

Cybersecurity in Government

- The Top 10 Common Cybersecurity Threats in 2021
- Lessons Learned
- Cybersecurity Strategies in Government
- Insights for a Proactive Cybersecurity Strategy: During COVID-19 and Beyond

Image Source: Wikimedia.com

JOINT COUNCILS' EXECUTIVE MONTHLY REPORT

Developed by the Research Committee

November 2021

1. Introduction

According to the Government of Canada, "**Cybersecurity is the protection of digital information stored within your cyber threat environment against cyber threats and cyber threat actors**".[1] The COVID-19 pandemic ("the pandemic") has intensified the demand for digital connectivity and digital government. Government restrictions in response to the pandemic has led to employee remote working environments and clients are predominately relying on online service delivery to access government services. The increasing dependence on digital connectivity has heightened the need for digital-first services.[2]

This ever-accelerating shift toward digital and online services has increased the importance of cybersecurity more than ever before. During the pandemic, cyberattacks have increased worldwide. According to Canada's authority on cyber security – the Canadian Centre for Cyber Security – cyber criminals are constantly adjusting their methods and using more advanced techniques to attack government systems.[3] This is predominately due to the weakening of existing cyber security measures through changes in working and infrastructure patterns caused by the pandemic.

In order to improve cybersecurity efforts during the pandemic, as well as in the post-pandemic world, it is essential for governments to examine their cyber strategies and implement concrete measures to promote a more reliable and trustworthy internet. This will help build a stronger level of digital trust and enable a robust cybersecurity environment where clients can access online government services easily and securely.

Why is this Report Important?

- Improving cybersecurity is a top priority for Canadians. According to the 2021 Edelman Trust Barometer, "65% of Canadians are worried about falling victim to a cyber-attack, a greater concern than both climate change (63%) and COVID-19 (60%)".[4]
- Jurisdictions across Canada have reported a growing number of cyber criminals and other malicious groups online that are exploiting the COVID-19 outbreak for their own personal gain.[5]
- In 2020, the Research Committee published a report titled, Cybersecurity: A look at the Canadian landscape. This report examined cybersecurity organizations and initiatives across Canada, opportunities and challenges in the cybersecurity space, and where governments should focus their efforts.

What is Covered in this Executive Report?

This report includes the following:

- Introduction
- The Top 10 Common Cybersecurity Threats in 2021
- Lessons Learned
- Cybersecurity Strategies in Government
- Insights for a Proactive Cybersecurity Strategy: During COVID-19 and Beyond

1. What is cybersecurity?
2. How Covid-19 is Dramatically Changing Cybersecurity
3. Focused Cyber Security Advice and Guidance During COVID-19
4. Cybersecurity a greater concern for Canadians than COVID-19 – here's how Canada can step up: Canadian Chamber of Commerce
5. Cyber Risks: An Increased Threat During COVID-19

2. The Top 10 Common Cybersecurity Threats in 2021

During the pandemic, the number of cybersecurity incidents reported in Canada has grown at an alarming pace. According to a new report from IBM Security, the average cost of a data breach in Canada was $6.75 million per incident in the 2021 survey year. That's up from $6.35 million in 2020 and the highest since IBM first included Canada in its survey seven years ago.[6] According to the Department of Public Safety and Emergency Preparedness and leading information security researchers, the following are the top 10 common cybersecurity threats experienced by organizations and individuals in 2021:[7]

1. **Zero-Day Exploits:** A software vulnerability discovered by attackers before the vendor or organization has become aware of it. Zero-day exploits are becoming more sophisticated and has posed a significant threat in 2021.	6. **Phishing:** A type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It has proven to be very effective in the 21st century because it is commonly deployed by means of fake emails, text messages or phony websites that seem authentic.
2. **The Internet of Things (IoT):** With the IoT, sensors collect, communicate, analyze, and act on information. Although this does create value for organizations and customers by creating and delivering a more efficient experience, it also creates new opportunities for information to be compromised. Throughout 2021, there have been more privacy intrusions from devices that utilize the IoT.	7. **Ransomware:** This is a type of malware that uses encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. In 2021, ransomware has become a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for public and private sector organizations.
3. **Botnets:** Networks of hijacked computer devices used to carry out various scams and cyberattacks. In 2021, the botnet threat grew considerably because of the popularity of smart home automation devices that connect to the internet.	8. **Crypto-Jacking Malware:** This type of cybercrime involves the unauthorized use of an individual or organization's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. In 2021, crypto-jacking attacks continue to increase.
4. **Distributed Denial of Service (DDoS) Attacks:** A method where cybercriminals flood a network with a significant amount of malicious traffic to the extent where it cannot operate or communicate as it normally would. This causes the site's normal traffic to come to a halt.	9. **Invisible Malware or Software Subversion:** Sophisticated attackers are now using "invisible malware", a new form of attack that firewalls cannot stop and anti-malware software cannot find or remove. Although this particular cyber risk may be considered a new threat in 2021, it is actually related to traditional hacking methods.
5. **Spam:** Although Canada has adopted legislation to prohibit the distribution of commercial messages without previous solicitation, spam is a global issue that continues to worsen in 2021.	10. **Man-in-the-Middle (MITM) Attacks:** This is when an attacker intercepts communication between two parties to secretly eavesdrop or modify traffic traveling between the parties. Attackers may use MITM attacks to steal log-in credentials or personal information, spy on the victim, sabotage communications and/or corrupt data.

6. Cost of data breaches in Canada hit new record in 2021: IBM
7. Common Cybersecurity Threats

3. Cybersecurity Lessons Learned During COVID-19

The pandemic revealed that preparation is key to successfully limit the risks related to cyberattacks. The ability for organizations to quickly react to unforeseen events helps reduce the impact of a cyberattack.

It is important for government to change their outlook from ***if*** an attack will occur, to ***when***, and recognize that the consequence from breaches of data privacy or ransomware can have negative financial implications.[8] It is also important to note that financial gain is not the only motive behind cyberattacks. 'Hacktivism' and its goal to damage the reputation of government organizations is an additional threat.[9]

Throughout the pandemic, a number of cybersecurity incidents have been reported across Canadian jurisdictions. According to the World Economic Forum, the following are some key lessons learned gathered during the pandemic:[10]

Foster A Culture of Cyber Resilience

Being resilient requires the highest levels of leadership to acknowledge the importance of proactive risk management and focus more on the ability of the organization to absorb and recover from a cyberattack that would disrupt essential services.

Focus on Protecting Critical Assets and Services

Organizations must have a holistic and systemic view of their critical services, applications, suppliers and assets. Leaders must prioritize resources and investments to the most essential areas to maintain operational continuity, protect critical digital assets and ensure compliance.

Balance Risk-Informed Decisions During the Crisis and Beyond

Cyber risk management needs a top-to-bottom overhaul. Traditional cyber resilience metrics have shown to be an inadequate representation of real risk. Organizations need to revise their approach to supply chains, define practical and meaningful cyber risk metrics, and focus on the risks to operations when designing new digital strategies.

Update and Practice Response and Business Continuity Plans

The COVID-19 crisis emphasized the importance of adapting and regularly testing response and resilience plans against different worst-case scenarios (including pandemics) with key suppliers and business partners. This includes equipping crisis management teams with the skill sets and experience to manage under intense pressure.

Strengthen Ecosystem-Wide Collaboration

Partnership and collaboration on cyber resilience between the public and private sector across the ecosystem is essential. This will enable transparent information sharing, collaborative awareness, and ensure sectors work together to disrupt criminal activity by creating a systemic approach to risk management as part of the broader community.

8, 9. Impact of COVID-19 on Cybersecurity
10. Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic

4. Cybersecurity Strategies in Government

As hackers continue to invent new ways to bypass security measures to steal, expose, and/or destroy sensitive data for the purpose of monetary gain, government organizations are particularly vulnerable to being targeted compared to other industries. According to Mckinsey, governments (at all levels) are more likely to experience a cyberattack for the following reasons:[11]

1. Government organizations house highly sensitive information and client data.
2. The rapid shift toward work-from-home arrangements in response to the pandemic. Employees working remotely are at a greater risk than those in offices. This is primarily because home connections are typically less secure, enabling cybercriminals to gain easier access into the organization's network.
3. Shortage of cybersecurity professionals to meet the growing demand to proactively respond to cyber risks.

Cybersecurity is a key priority across Canadian jurisdictions. The following are some examples of cybersecurity strategies across Canada.

Examples of Cybersecurity Strategies Across the Canadian Public Sector

Government of Canada

The National Cyber Security Strategy outlines the framework that guides the Government of Canada in helping to protect clients from cyber threats and supports the Government to take advantage of the economic opportunities afforded by digital technology.[12] The Strategy is designed to adapt to meet the goals of the Government of Canada as technologies and cyber threats continue to evolve.

Alberta

The Government of Alberta's Cybersecurity Strategy, *Protecting the Province's Digital Assets*, outlines the cyber threats that may impact the Government of Alberta. The document also highlights high-level strategies and principles to identify, assess, prevent, and respond to these threats in order to protect the organization's technology and information assets, or to recover these assets in the event of disasters.[13]

British Columbia

The Information Security Policy outlines the Government's corporate approach to information security management. The document acts as the framework under which all ministries must operate in order to ensure the information security practices of the Government are reasonable, appropriate, and efficient. The document aims to protect personal and confidential client information in a manner that is compliant with the security requirements of the Freedom of Information and Protection of Privacy Act and the Information Management Act.[14]

Ontario

The Ontario Cyber Security Strategy lays out the framework to modernize Ontario's cyber security program, by focusing on three areas: Enhancing collaboration across government and the broader public sector; Ensuring the continued security of government applications; and Protecting sensitive client data. As part of the Strategy, the government appointed ten members to an expert panel to help modernize cyber security across the Ontario Public Sector. The panel will submit a final report in the fall of 2022, with findings and recommendations to address common vulnerabilities.[15]

11. Cybersecurity's dual mission during the coronavirus crisis
12. National Cyber Security Action Plan (2019-2024)
13. Government of Alberta: Cybersecurity Strategy
14. BC Government: Information Security Policy V4.0
15. Ontario Appoints New Expert Panel on Cyber Security

5. Insights for a Proactive Cybersecurity Strategy: During COVID-19 and Beyond

In response to the COVID-19 pandemic, government organizations across Canada accelerated investment in digital transformation to maintain business continuity and meet the needs of clients. Many of the programs and services introduced expedited years of project planning and development into the span of a few months.[16] This increased government's exposure and vulnerability to cyberthreats.

As the pandemic progresses and alters the functioning of socioeconomic systems, cybercriminals will continue their efforts to exploit digital vulnerabilities. To remain vigilant and effective, governments (at all levels) will require new approaches to address growing cybersecurity challenges.[17] In addition to technology, the future of cybersecurity should also focus on strengthening and increasing organizational resilience.

According to PWC, the following are five key insights to ensure the development of a proactive cybersecurity strategy to meet the changing demands during the pandemic and beyond.

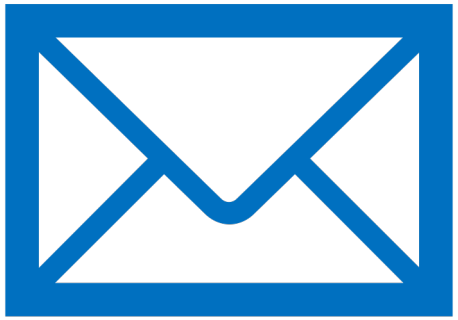
Resources to Support Your Cybersecurity Efforts:

- Focused Cyber Security Advice and Guidance During COVID-19
- The Continued Impact of COVID-19 on Cyber Threat Activity
- Ransomware: How to prevent and recover
- Developing your incident response plan

16, 17. Follow the leaders: How governments can combat intensifying cybersecurity risks
18. Canadian Digital Trust Insights 2021: Cybersecurity comes of age

Insights for a Proactive Cybersecurity Strategy: During COVID-19 and Beyond[18]

Reset your cyber strategy	• Reset your cyber strategy to adapt to the new business reality and make high-speed digital change safer. • Consider a business-driven cyber strategy that aligns with the vision and goals of the whole enterprise—not just IT.
Rethink your cyber budget	• Rethink the organization's cyber budgeting process to clearly show how cyber spending links to risk and business priorities. • Link the cyber budget to overall digitization and automation budgets. • Quantify cyber risks to enable the organization to put a dollar amount on the impact of each cyber project.
Level the playing field with attackers	• Explore innovative ways to secure the organization's cloud by fully leveraging cloud capabilities. This will reduce governance costs and proactively address emerging threats and achieve continuous compliance. • Reimagine the approach for securing industrial and IoT systems, where traditional IT security methods are ineffective. • Integrate the organization's privacy, data protection and data governance practices to inspire confidence in the use of critical data as it becomes more distributed.
Build resilience for any scenario	• Perform regular assessments and testing to identify weaknesses in the organization's defences before attackers do. • Implement a cyber hygiene program to remediate weaknesses often exploited by attackers. • Focus on enterprise-wide digital trust by orchestrating resiliency efforts across business continuity, disaster recovery, crisis management, privacy and fraud.
Future-proof the security team	• Design talent attraction and retention programs for the cyber function. • Offer upskilling to increase the expertise of current employees. • Create tailored cyber security training to help employees avoid cyber incidents and strengthen the overall cyber security culture.



For Further Reading

- Three things Canada can do to become a cybersecurity leader
- 5 cybersecurity issues that the public sector faces and how to protect it
- Cities employed new cybersecurity strategies during the pandemic
- 9 notable government cybersecurity initiatives of 2021
- Canada's fledgling cybersecurity centre must do more collaborating and educating

Other noteworthy articles:

Critical considerations for moving to the cloud

Governments look to digital ID for modern services and economic growth

The Evolution Of Voice In Elevating The User Experience

How to Address Growing Security and Privacy Challenges

How robotic process and intelligent automation are altering government performance

Research Repository

Access the Citizen First Research Repository.

Recent entries on the research repository:

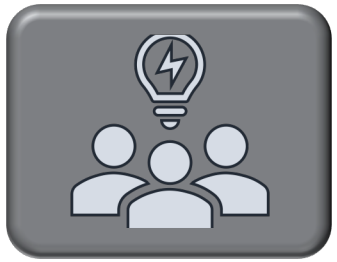
Digital Trust & Identity: Meeting New Expectations for Public Service Delivery — Joint Councils' Executive Report October 2021

This report explores: Government Adoption of Digital ID, Login Services as a Start Point, Verifiable Digital Credentials for Various Data Types, and Recommendations to Advance Implementation

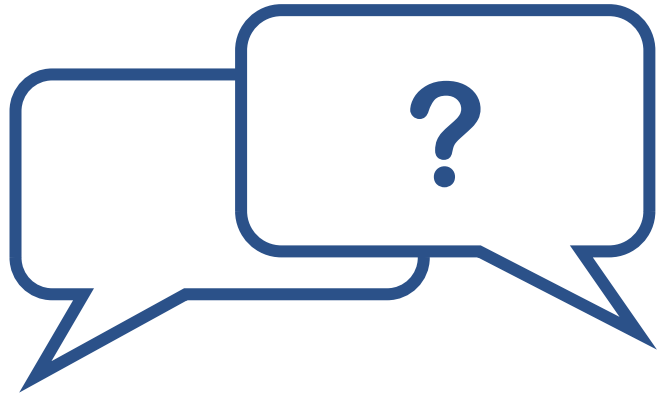
Trends in the Daily Newsletter

According to The Drum, during COVID-19, customer expectations heightened and good customer experience (CX) was no longer enough. Many organizations rushed digital transformation projects in the past year to help cater to fast-moving consumer needs. However, today we are left in a situation very different to that of March 2020. CX needs to be more smooth and personalized. Now is the time for organizations to think about the digital tools available to not only keep operations running efficiently, but to take CX to new heights.

According to GovTech, collaboration tools "proved to be critical success points" that allowed state and local governments to maintain continuity of services during the COVID-19 pandemic. Now, with more than two-thirds (67 percent) of government leaders focused on modernization over the next two years according to a CDG survey,1 it's essential to ensure these efforts support remote or hybrid working environments. Doing so, however, will require thinking about collaboration tools in a new way. This article lists seven key strategies to leverage collaboration tools to support hybrid work.



A study of four governments -- two state and two local -- illustrates how agile has evolved from a software development approach to being applied in project management, procurement and social services. Across all the organizations, three phases of agile adoption emerged: infancy, adolescence and adult. According to the report, "Agile is a mindset of organizational change. As a process of continuous improvement, Agile methods themselves could evolve over time with doing, testing, and improvement."



We would love to hear from you!

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report. If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up. Send your questions to info@iccs-isac.org.

Follow: