Board Leadership Calgary

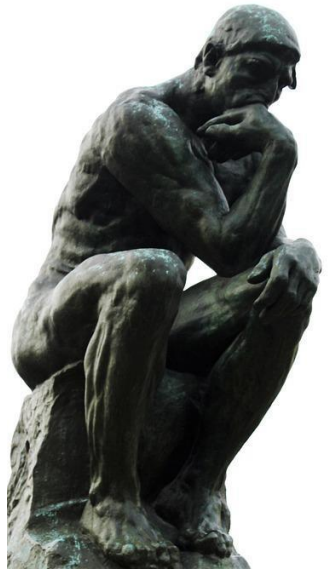
# Cybersecurity Strategies for Non-Profits

**Greg Miller**

April 25, 2026

# Welcome

Board Leadership Calgary



What brought you here today?

For Today: The Challenge. What to do. Some language and some Support & Security options

**Greg Miller**

Volunteer Board Member, HPCA for 10 years

30 years here in Calgary

A career with Microsoft, Amazon Web Servic
MSPs and many places in-between.

I’m not selling anything :-D

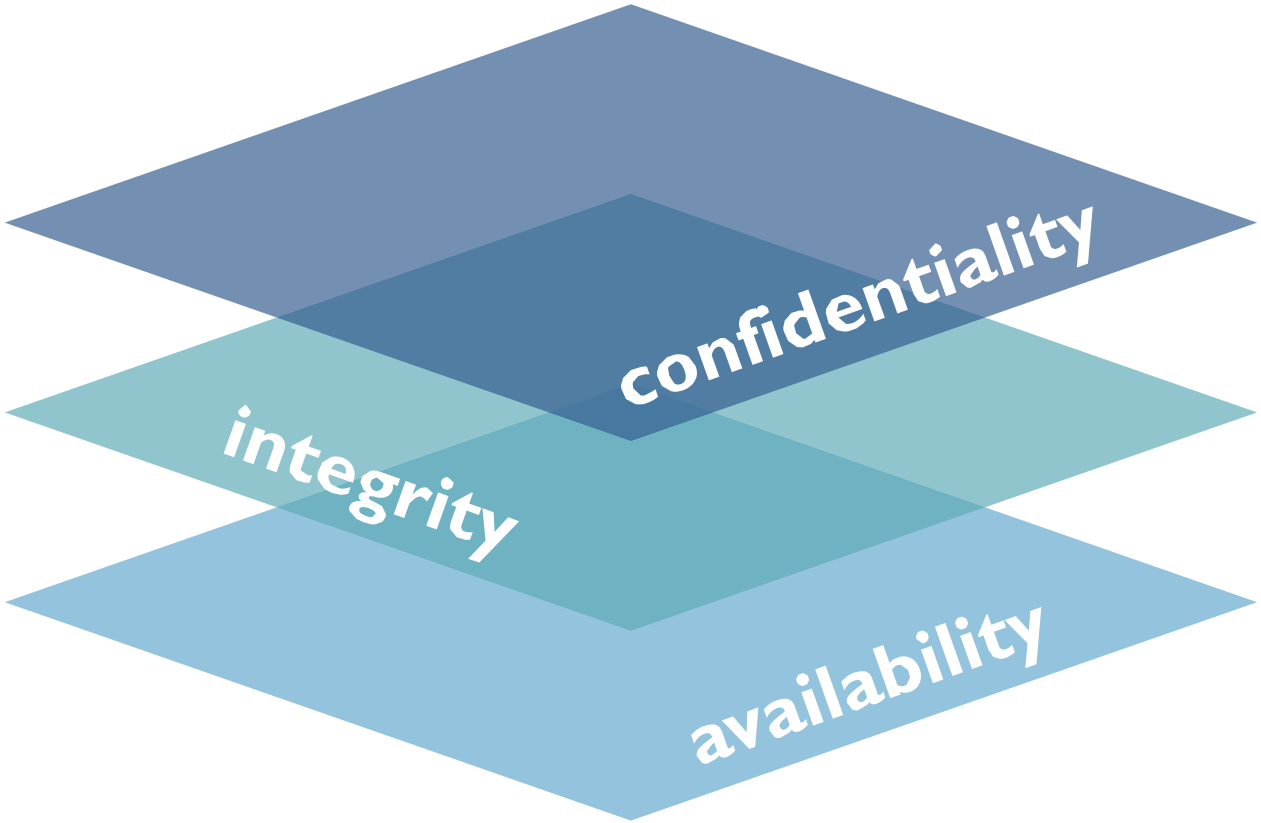
# Vocabulary

**Cybersecurity:**
The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information.

More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

**Cybercrime:**
Cybercrime includes crimes in which technology is the primary target (e.g. malware or ransomware ) or crimes that use technology as an instrument to commit crimes (e.g. money laundering or fraud).

# What are we protecting? The C.I.A. Model




Canadian Centre for Cyber Security &
National Institution of Standards and Technology (NIST)

The ability to protect sensitive information from being **accessed by unauthorized people.**

The ability to protect information from being **modified or deleted unintentionally** or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.

The ability for the **right people to access the right information or systems when needed.** Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.

## What if your Organization can't protect the CIA of its information?

# Uh Oh, Canada

## Canadian Stats:

In 2024, Canada reported over **70,000 cybercrime incidents**, a 20% increase from 2023.

**Ransomware** attacks accounted for 17% of reported cases.

*Canadian Centre for Cyber Security*

## Estimated Losses:

Canadian businesses lost **$3 billion+ annually** due to cybercrime

*IBM Cost of Data Breach Report*

Parliament of Canada


"From April 2023 through March 2024, Communications Security Establishment Canada's network-based sensors blocked about **2.4 trillion suspicious cyber security events**, which ranged from simple network scans to sophisticated cyber attacks.

From October 2023 through September 2024, Shared Services Canada's secure Enterprise Internet Service blocked about **6.6 trillion suspicious cyber security events."**


Government of Canada Gouvernement du Canada

MENU

Canada.ca › Shared Services Canada

Ministerial statement on the cyber security of federal government networks and systems

From: Shared Services Canada

Statement

October 21, 2025 – Ottawa, Ontario

*Joint statement by the Honourable Joël Lightbound, Minister of Government Transformation, Public Works and Procurement and Minister responsible for Shared Services Canada; and the Honourable Shafqat Ali, President of the Treasury Board.*

Today, following the tabling of the Auditor General of Canada's *Audit of the Cyber Security of Federal Government Networks and Systems*, our government reaffirms its unwavering commitment to protecting and strengthening the security and resilience of Canada's digital infrastructure.

Canadians expect their government to keep their personal information and the systems they rely on secure. In an increasingly complex and hostile digital environment, cyber security is not only a technical responsibility—it is a national priority and a key pillar of public trust in government institutions.

# Recent Incidents, as of April 22 2026


THE GLOBE AND MAIL

Hackers accessed personal information for up to 70,000 people in Canada Life data breach

| Organisation | Date | Incident |
|---|---|---|
| **Canada Life** | Apr-26 | Criminal group ShinyHunters accessed certain applications through a Canada Life employee account, exposing personal information for up to 70,000 people |
| **Telus / Telus Digital** | Mar-26 | Telus Digital confirmed a breach after ShinyHunters claimed a large-scale theft of data following a multi-month intrusion; Telus said a limited number of systems were accessed without authorisation. |
| **Loblaw Companies Limited** | Mar-26 | Loblaw reported that a criminal third party accessed "basic customer information" such as names, phone numbers and e-mail addresses |
| **Canada Computers & Electronics** | Feb-26 | A system supporting the retailer's website was breached, affecting customers…stolen data included personal details and credit-card information used in those transactions. |
| **Canadian Investment Regulatory Organization** | Jan-26 | A phishing-originated breach…compromising personal and financial data for about 750,000 investors, including highly sensitive identifiers and account statements. |
| **Freedom Mobile** | Dec-25 | Attackers used a subcontractor's compromised account…exposing personal details (names, addresses, dates of birth, phone numbers and account numbers) for a limited number of customers |

*Source: Insurance Business Canada*

# Fortis et Liber?

**May/July 2023 – Alberta Dental Service Corporation**
Ransomware stole personal data of 1.5 million people.

**June 2023 – Suncor**
Suspected ransomware attack impacting > 900 retail locations. Replaced laptops across the company. Estimated cost: millions.

**March 2024 – Town of Ponoka**
A breach of the system by an unauthorized external actor.

**June 2024 – Federated Co-operatives Ltd. (FCL)**
Ransomware attack disrupted service to Co-op stores in the West, including Calgary.

**June 2024 – AutoCanada – CDK Dealer System Breach**
System outage, manual transactions. Restored end of July.

**Oct 2024 – Calgary Public Library**
Ransomware attack shut down all 22 branches temporarily. No information compromised.

**Nov 2024 – Alberta Innovates**
"unauthorized access to our network by a third party"

**Late 2024 – 31 Alberta School Boards: PowerSchool Breach**
Including, CBE, Rocky View Schools, Red Deer Public. PowerSchool paid a ransom to delete stolen data.

**June 2025 – WestJet**
Reported a cybersecurity incident under investigation. Personal information compromised.

**July 2025 – Town of Devon**
Reported a cybersecurity attack

**Leduc County systems back up following cybersecurity incident**

Peter Williams

Published Feb 02, 2026 • Last updated 1 day ago • 1 minute read

Join the conversation

*"More than half of small- and medium-sized businesses in **Alberta** say were attacked by cybercriminals over the past year and*

*55 per cent [of those surveyed] paid a ransom to unlock their computers within the past three years…"*
*Oct 24 2023*

KPMG

https://www.newswire.ca/news-releases/cybercrime-strikes-more-than-half-of-alberta-based-companies-840147390.html

# New Online Business: Cybercrime as a Service

## CaaS services available online for cybercriminals to purchase

- **Malware-as-a-Service:** services to support the development and deployment of malware that can steal or encrypt victim data or gain remote control of victim systems
- **Ransomware-as-a-Service (RaaS):** a core group of developers will sell or lease their ransomware variant to other threat actors, called affiliates; the core developers will support affiliates' deployment of their ransomware in exchange for upfront payment, subscription fees, a cut of profits, or all three
- **Access-as-a-Service:** specialized threat actors gain access to victim systems and sell access to compromised systems to clients
- **Phishing-as-a-Service (PaaS):** detailed instructions, email templates, and ready-to-use tools for executing phishing attacks
- **DDoS-as-a-Service:** rented out botnets and user-friendly interfaces for clients to conduct DDoS attacks
- **Exploits-as-a-Service:** specialized actors lease or rent exploit kits and support clients on how to use exploits against software vulnerabilities

Canadian Centre for Cybersecurity: National Cyber Threat Assessment 2025-2026

# What is Ransomware

**Theft:** The criminals capture your data, encrypt it, and deny you access unless you pay them, in which case they give you a code and release it to you.

**Extortion:** the criminals don't encrypt your data. They copy it and threaten to make it public unless their demands are met.

Q: How do they do it?

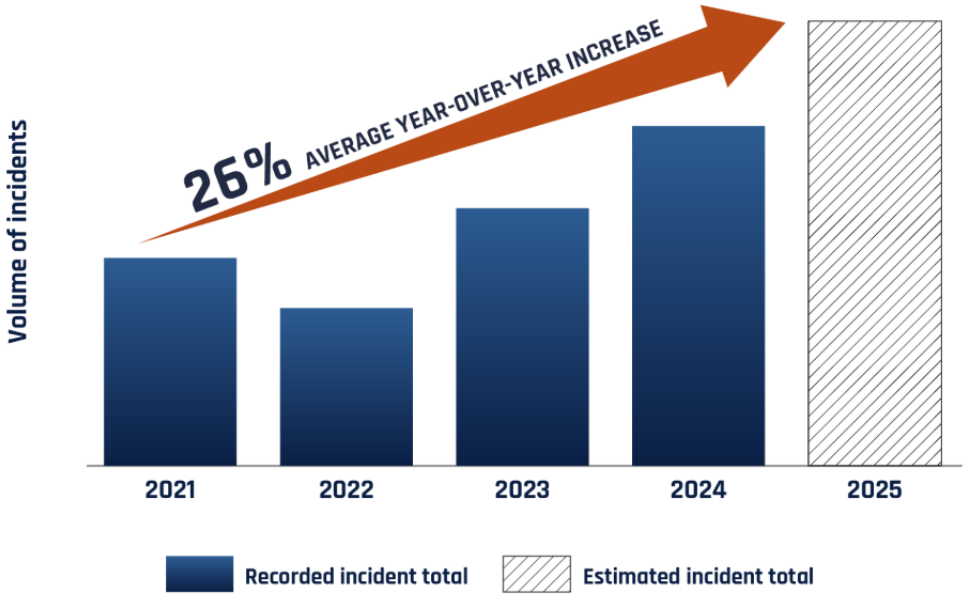
A: Through **unauthorized access to your systems**

# Ran$omware

"…**ransomware** continues to stand out as one of the most disruptive, costly, and persistent challenges facing Canadian organizations of every size."

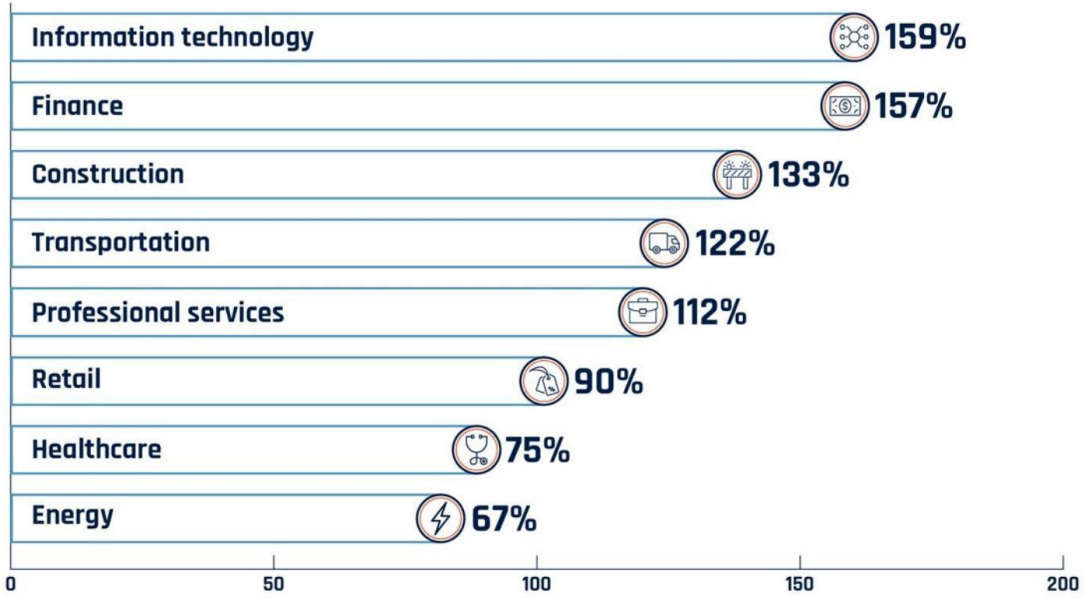
*Rajiv Gupta, Head Canadian Centre for Cyber Security*

Figure 1: Growth from 2021 of Canadian ransomware incidents known to the Cyber Centre




*Canadian Centre for Cybersecurity: Ransomware Threat Outlook 2025-2027*

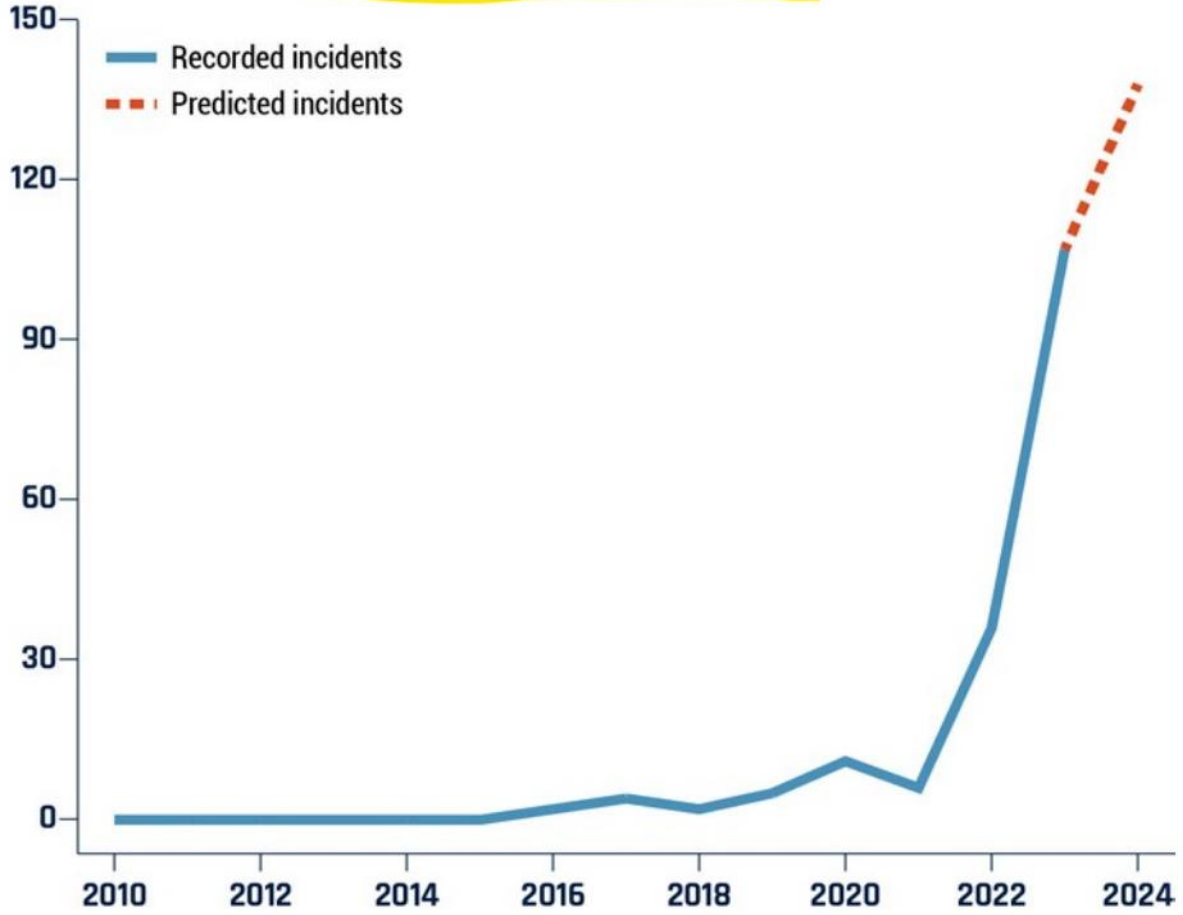
*Figure 12: Increase in Canadian ransomware incidents by sector observed by the Cyber Centre from 2022 to 2023*




**But what about Non-Profits??**

# AI makes the crooks more productive

**Figure 15: Publicly reported worldwide generative AI incidents resulting in harm or near harm**[134]




Canadian Centre for Cybersecurity: National Cyber Threat Assessment 2025-2026

*"AI technologies are almost certainly lowering the barriers to entry..."*

**...to commit cybercrime**

*"...based on recent developments in victim demography, we assess that* ***no organization is immune to cyber incidents.***

*[organizations] with* ***fewer cyber security resources may face more challenges in responding to sophisticated ransomware attacks.***"

# Who's a Target? Everyone.

Cybercriminals target organizations of all sizes — from large enterprises to small nonprofits.

AI and Cybercrime:

- AI enables attackers to automate phishing, create deepfakes, and exploit vulnerabilities faster.
- Even the smallest organizations are vulnerable due to limited budgets, outdated systems, and lack of dedicated IT staff.
- Ransomware is a big threat, enabled by the cloud and AI.

**Yikes!**

# What to do?

# What's Your Risk?

**Financial:**

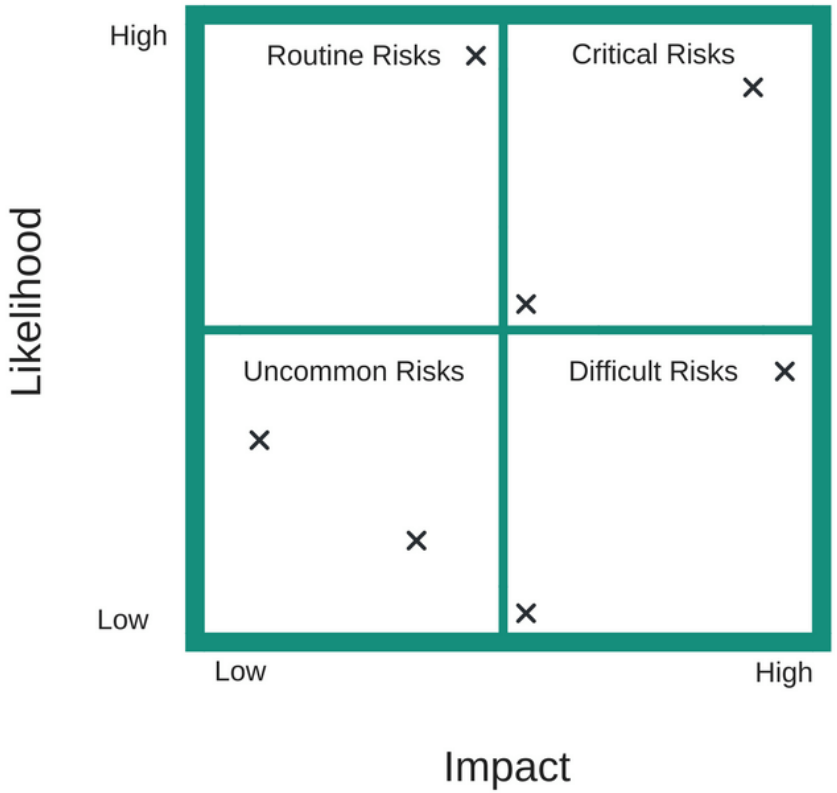
Direct monetary loss, ransom payments, recovery costs.

**Data:**

- Exposure of sensitive member, volunteer, client, user, board member, or employee information.
- Confidential meetings, minutes
- Banking, financial information

**Reputational:**

Loss of trust among members, stakeholders, and/or your community



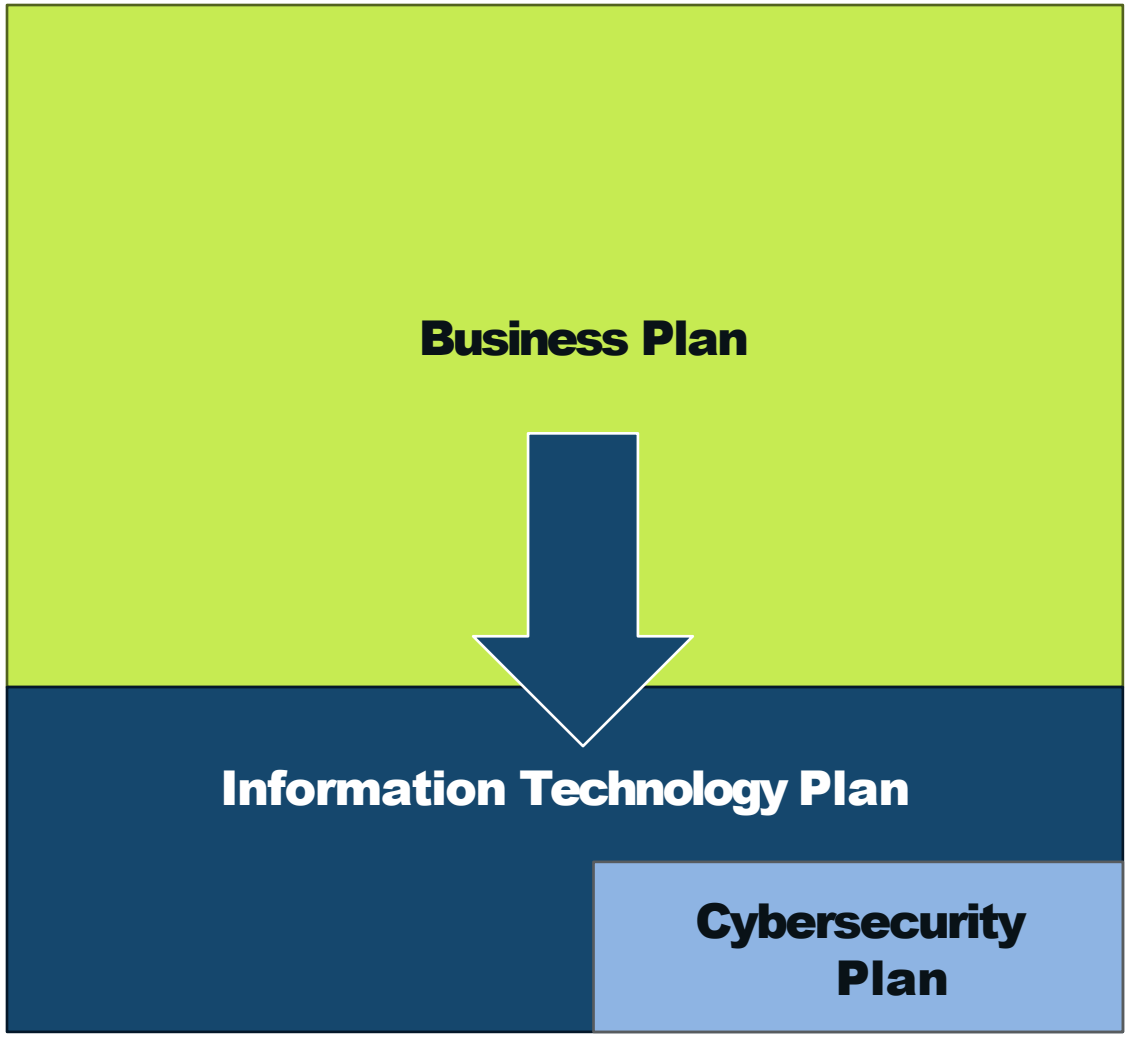

## Are these risks likely enough, costly enough, for you to mitigate?

# Mitigation: Have ~~A Plan.~~ Plans

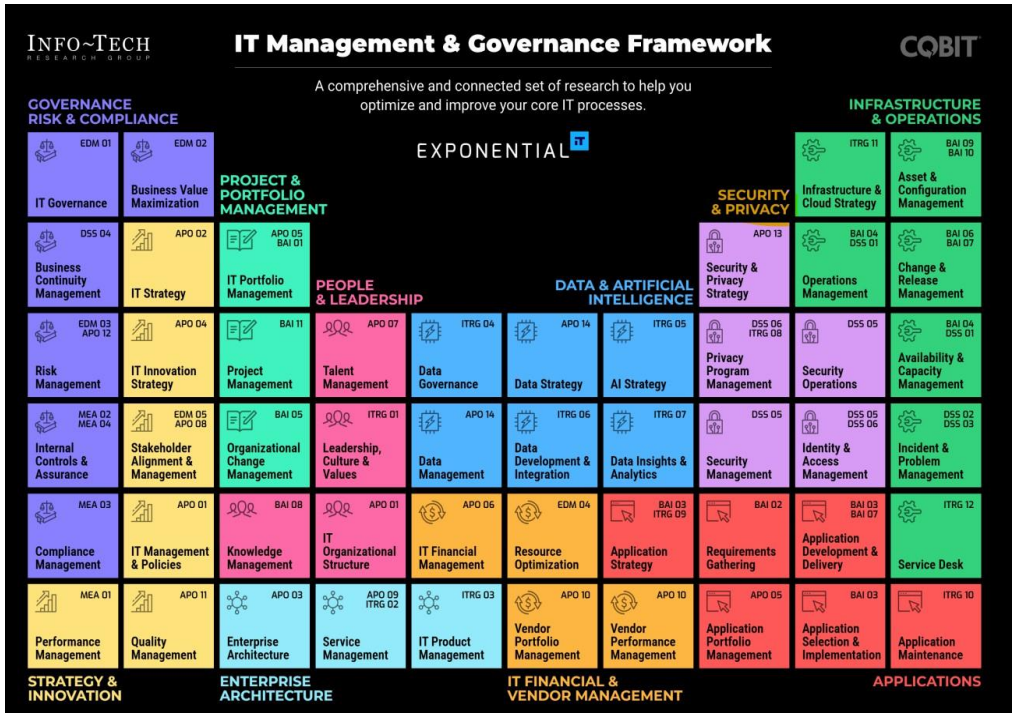
Everyone has a **Business Plan** of some kind.

You should have an **IT Plan** that supports your Business Plan.

A **Cybersecurity Plan** or Strategy lives within your IT Plan



# What should your IT Plan include?




**1. Organizational Needs:** What is your Organization's goals? Challenges? Inefficiencies?

**2. Assessment of Your Current Tech**: Hardware, software, network, IT Support, cybersecurity.

An inventory.

**3. Financial & Vendor Management**: Budget. Service Providers, applications, hardware.

**4. Strategic Goals**: How will IT support your initiatives? How do you improve security, collaboration, and operational efficiency.

**5. Roadmap**: A calendar of IT initiatives, with preliminary cost estimates and timelines.

**6. Policies, Training**: Acceptable Use. BYOD. Tech refresh.

**7. Cybersecurity:** Policies, People, Technology

# Cybersecurity Framework: Ongoing protection


NIST Cybersecurity Framework (CSF) 2.0

**Identify**

- Assess organizational assets, data, and systems to understand what needs protection.
- Define business context, risk tolerance, and cybersecurity roles and responsibilities.

**Protect**

- Implement safeguards like firewalls, access controls, and encryption to secure systems.
- Train staff on cybersecurity awareness and enforce security policies.

**Detect**

- Monitor systems continuously for anomalies and potential threats.
- Use tools like intrusion detection systems (IDS) and log analysis to identify incidents early.

**Respond**

- Develop and test an incident response plan to contain and mitigate threats.
- Communicate with stakeholders and report breaches as required by law or policy.

**Recover**

- Restore systems and data from backups and ensure business continuity.
- Review and improve recovery processes based on lessons learned.

**Govern**

- Establish oversight, accountability, and strategic alignment of cybersecurity with business goals.

# Policies, People…

**Policies:**

- Zero Trust Model
- Unique IDs, licences for all users
- An incident response plan.
- ** Cyber Insurance**
- PEN Testing – frequency?
- Keep it evergreen!

*The **Zero Trust model** is based on the principle of **"never trust, always verify."***

*Threats exist both **outside and inside** the network, so no user, device, or system is trusted by default.*

- *Verify explicitly*
- *Use least privilege access*
- *Assume breaches will happen*

**People**:

- Awareness
- Accountability, Code of Conduct
- Training:

knowbe4

Security Awareness
Gamified, Engaging Content
Simulated Phishing
Compliance and Risk Management


Fig. 3. Steps for creating and using a CSF Organizational Profile

# Technology: Detection & Response

| | EDR | XDR | MDR |
|---|---|---|---|
| | **Endpoint Detection & Response** | **Extended (or Unified) Detection & Response** | **Managed Detection & Response** |
| **What it is** | Tool | Tool | Service |
| **Purpose** | Monitors and responds to threats on user devices, laptops, workstations, servers | EDR + Network, identity, email systems. Cross-domain detection | E/XDR + People + Process |
| **Scope** | Endpoints | Endpoints + identity, email, cloud | You decide: The service operates E/XDR for you |
| **Stops known malware** | ✅ Yes | ✅ Yes | ✅ Yes |
| **Detects unknown attacks** | ✅ Yes | ✅ Yes | ✅ Yes |
| **Investigates incidents** | ⚠️ Limited | ⚠️ Limited | ✅ Yes |
| **Human analysts** | ❌ No | ❌ No | ✅ Yes |
| **Examples** | CrowdStrike, SentinelOne, Defender for Endpoint | Microsoft Defender, Palo Alto Networks, CrowdStrike | Arctic Wolf, Sophos, Red Canary |

# More Technology


| | Description | Examples |
|---|---|---|
| SIEM (Security Information and Event Management) | A technology that logs, aggregates and analyzes security data across systems. “What happened?” | Splunk, Microsoft Sentinel, LogRhythm |
| SOC (Security Operations Center) | Centralized team or service that monitors and responds to threats 24/7. It uses the tools above. | Arctic Wolf, IBM QRadar, Managed SOC providers |
| *MFA (Multi-Factor Authentication) | 2 out of 3 verification methods: Something you know, something you have, or something you are. | Microsoft Authenticator, Google Authenticator, Duo Security |
| *Password Manager | A service that encrypts and stores all your passwords in one site. | Apple iCloud keychain Google PW manager, 1Password, Bitwarden, |
| Firewall | Perimeter protection. Filters network traffic to block unauthorized access. More valuable in on-premise or hybrid environments, less so in SaaS. | Azure Firewall, Fortinet, pfSense |
| Antivirus / Antimalware | Detects and removes malicious software. *Now generally included with EDR/XDR. | Microsoft Defender, Bitdefender, Malwarebytes |
| VPN (Virtual Private Network) | Encrypts internet traffic and hides IP addresses. | NordVPN, Cisco AnyConnect, ProtonVPN |
| *IAM (Identity and Access Management) | Controls user access to systems and data. | Okta, MS Active Directory, Entra ID, JumpCloud, Google Cloud IAM |
| WAF (Web Application Firewall) | Protects web apps from attacks like SQL injection and XSS. | Cloudflare WAF, AWS WAF, Imperva |
| DLP (Data Loss Prevention) | Prevents sensitive data from being leaked or misused. | Microsoft Purview DLP, Symantec DLP, Forcepoint |

*Supports a Zero Trust Model

# Cyber Risk Insurance

**Mitigates loss, can help with recovery**

- Can provide you with a coach during an incident where time is critical and stress is high
- Data loss coverage

**Typical questions for eligibility:**

- Do you conduct regular backups?
- Do you have an incident response plan?
- Do you employ MFA? XDR? SCIEM? SOC? - ie those acronyms on the previous slide

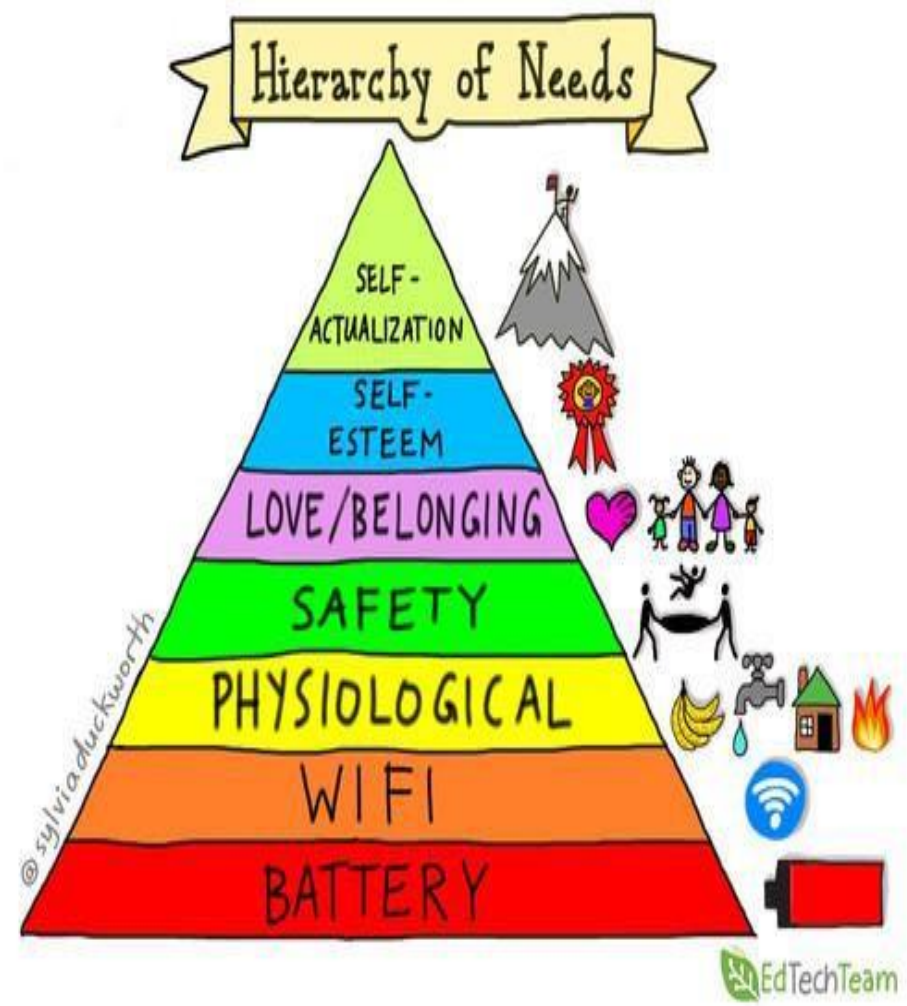
# IT Management Progression

1. **Dedicated IT Manager**, responsible to your organization. Manages 3rd party relationships

2. **Managed Service Provider**: provides both support (at least 5 by 8) and cybersecurity, (usually 24/7)

3. The contracted "**IT Guy**"

4. Someone in your organization handles IT along with their day job – **off the side of their desk.**



# IT & Cybersecurity Partner

1. IT leadership and advice at a fraction of the cost of a full-time manager
2. Continuous monitoring and management
3. Best practices, updates, and a roadmap
4. **TRUST**

**Contracting considerations:**

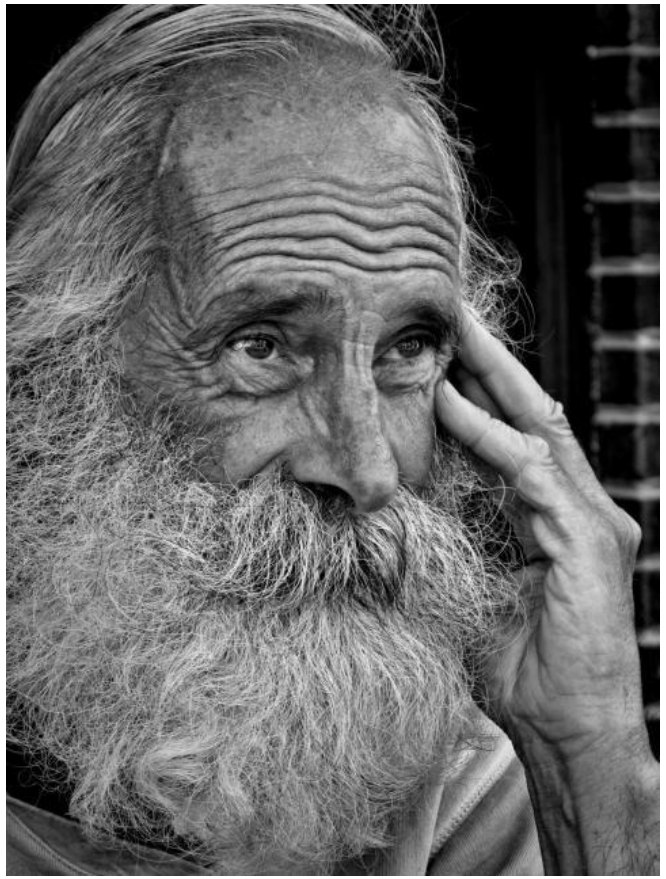
- Many reputable local providers
- Fixed Priced options.
- Base Support & Security, additional projects for a fee.
- 1 to 3 year agreements. Know your termination clause.

IMO avoid equipment leases (at least with your Service Provider)

**BUT WHY DO YOU HAVE ON-PREMISE SERVERS ANYWAY!?**

# The Last Word

***Wise***
***Non-Profit CIO***



*"Two things keep me up at night:*

1. ***Spending as little as possible*** *on our Information Technology, and*

2. ***Keeping our organization secure."***

# Thank You!

greg.miller@outlook.com

https://www.linkedin.com/in/greg-miller-936438/

403 836-0674

# Resources

- https://cyber.gc.ca Canadian Centre for Cyber Security
- https://www.ibm.com/security/data-breach
- NIST Cybersecurity Fundamentals Presentation | NIST
- https://www.insurancebusinessmag.com/ca/
  Insurance Business Canada

# Message from the Head of the Cyber Centre

At a time when cybercriminals continue to target Canadian businesses, critical infrastructure, and government systems, education on these threats has never been more important. As Canada's national authority on cyber security, the Cyber Centre is committed to helping Canadians understand, prepare for, defend against, and respond to the digital threats that impact our economy, our institutions, and our daily lives.

Among these threats, ransomware continues to stand out as one of the most disruptive, costly, and persistent challenges facing Canadian organizations of every size. This is why this report, the Ransomware Threat Outlook 2025 to 2027, provides a forward-looking view of the ransomware landscape we anticipate in the next 2 years. Our analysis draws on reporting from across Canada and around the world, classified intelligence from our foreign partners, and insights from the private sector. Together, these perspectives let us identify not only the tools, tactics, and procedures of today's most prolific cybercrime operators, but also the likely trends and evolutions that will define this threat tomorrow.

As you will read in this report, ransomware is big business. Despite some concerning trends, Canadians can rest assured that the Cyber Centre is keeping pace to address these threats and is developing new tools to defend Canadian networks and systems.

Our objectives are clear: to equip decision makers with the knowledge they need to manage their risk, to strengthen Canada's resilience, and to safeguard the trust Canadians place in our digital systems. Only by working together can we blunt the impact of ransomware and ensure Canada is secure and resilient in an ever-evolving cyber landscape.

In partnership,

**Rajiv Gupta**
Head, Canadian Centre for Cyber Security

# Basic Ransomware Tips

**BASIC RANSOMWARE TIPS**

*Even without undertaking all the measures described in this Ransomware Community Profile, there are some basic preventative steps that an organization can take now to protect against and recover from the ransomware threat. These include:*

**1. Educate employees on avoiding ransomware infections.**

- **Don't open files or click on links from unknown sources** unless you first run an antivirus scan or look at links carefully.
- **Avoid using personal websites and personal apps** – like email, chat, and social media – from work computers.
- **Don't connect personally owned devices to work networks without prior authorization.**

**2. Avoid having vulnerabilities in systems that ransomware could exploit.**

- **Keep relevant systems fully patched.** Run scheduled checks to identify available patches and install these as soon as feasible.
- **Employ zero trust principles in all networked systems.** Manage access to all network functions, and segment internal networks where practical to prevent malware from proliferating among potential target systems.
- **Allow installation and execution of authorized apps only.** Configure operating systems and/or third-party software to run only authorized applications. This can also be supported by adopting a policy for reviewing, then adding or removing authorized applications on an allow list.
- **Inform your technology vendors of your expectations** (e.g., in contract language) that they will apply measures that discourage ransomware attacks.

**3. Quickly detect and stop ransomware attacks and infections.**

- **Use malware detection software, such as antivirus software at all times.** Set it to automatically scan emails and flash drives.
- **Continuously monitor** directory services (and other primary user stores) for indicators of compromise or active attack.
- **Block access to untrusted web resources.** Use products or services that block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity. This includes using products and services that provide integrity protection for the domain component of addresses (e.g., hacker@poser.com).

**4. Make it harder for ransomware to spread.**

- **Use standard user accounts** with multi-factor authentication versus accounts with administrative privileges whenever possible.
- **Introduce authentication delays or configure automatic account lockout** as a defense against automated attempts to guess passwords.
- **Assign and manage credential authorization** for all enterprise assets and software and periodically verify that each account has only the necessary access following the principle of least privilege.
- **Store data in an immutable format** (so that the database does not automatically overwrite older data when new data is made available).
- **Allow external access to internal network resources via secure virtual private network (VPN) connections only.**

**5. Make it easier to recover stored information from a future ransomware event.**

- **Make an incident recovery plan.** Develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization, and business continuity plans for those critical services.
- **Back up data, secure backups, and test restoration.** Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.
- **Keep your contacts.** Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.

NIST Internal Report
NIST IR 8374r1 ipd

**Ransomware Risk Management:**

*A Cybersecurity Framework 2.0 Community Profile*

Initial Public Draft


Murugiah Souppaya
*Computer Security Division*
*Information Technology Laboratory*

William Fisher
*Applied Cybersecurity Division*
*Information Technology Laboratory*

William C. Barker
*Dakota Consulting*
*Silver Spring, MD*

Karen Scarfone
*Scarfone Cybersecurity*
*Clifton, VA*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374r1.ipd

January 2025


U.S. Department of Commerce
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology
*Charles H. Romine, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director*