Cybersecurity in Action

Laura Franks, BA (Ed) (Psy) MSc (IT Security) CySA+ CCAI
Stephen Franks, MSc (IT Security) C.E.T CySA+ CCAI

Lots of letters, we have been doing this for over 30 years each!

Laura Franks

A seasoned educator with over three decades of experience, I am a passionate advocate for technology-driven learning. My career spans both secondary and post-secondary education, as well as industry, where I've collaborated with learners of all backgrounds to achieve their goals. Known for creating engaging and impactful learning experiences, I am a lifelong learner committed to exploring innovative approaches and sharing my knowledge with others. I hold a Bachelor's of Psychology degree, a Bachelor's of Education degree, and a Master's Degree in Computer Security.

Stephen Franks

A passionate educator and technologist, I specialize in networking, systems, and security. With a strong belief in innovation and lifelong learning, I am dedicated to finding new and secure ways to optimize systems and networks. Committed to fostering a collaborative environment, I am driven by a desire to empower others through knowledge sharing and mentorship. I hold a CET (Certified Engineering Technologist) qualification through TechNova, a Diploma in Computer Technology, and a Master's Degree in Computer Security.

Welcome! This morning we are going to talk about…

1. The state of Cybersecurity for Smaller Communities
2. The Threat Landscape
3. Challenges, and
4. Answers and tools you can use!
5. A call to action.

The state of Cybersecurity for Smaller Communities

Cybercrime is **no longer a distant threat**. It's a pressing **issue for communities of all sizes**.

Some common targets include:

- Libraries
- Health and medical related facilities and services
- Municipal and city services

Montreal, Quebec: 2020 - Ransomware; **Gatineau, Quebec**: 2021 - Cyberattack affecting municipal services;

Understanding the Cyber Threat Landscape

Common Threats:

- **Phishing attacks** (one of the most commonly seen types of fraud):
  - Tricking users into revealing sensitive information.
- **Ransomware**:
  - Encrypting data and demanding payment for its release.
- **Malware**:
  - Malicious software that can damage systems or steal data.
- **DDoS attacks**:
  - Overwhelming a system with traffic to render it inaccessible.

Fraud, Scams, and Ransomware are the **most pressing threats across Canada** and **aided by Cybercrime-as-a-Service** are on the rise and **easier for unsophisticated attackers** to complete successfully.(From: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026)

Toronto, Ontario: 2020 - Cyberattack affecting city services; **Waterloo, Ontario**: 2021 - Ransomware;

Unique Challenges for Smaller Communities

Limited Resources: “If it ain’t broke, don’t fix it!” and “Do what you can with what you have.” **But . . . it is broken**, thus the large and increasing number of successful attacks!

Awareness: Phishing attacks (thin edge of the wedge that gives threat actors access to our environments). **Training people and raising awareness is the best way to battle this**.

Kingston, Ontario: 2021 - Ransomware on city networks; **Niagara Falls, Ontario**: 2022 - Ransomware on city infrastructure;

Best Practices for Cybersecurity

Cyber Hygiene for Leaders

Passphrases not Passwords: Use **unique passphrases for each account**.

Multi-Factor Authentication: Enable it **wherever possible**.

Phishing Awareness: **Recognize and report** suspicious emails and communications.

Software Updates: **Regularly update** all systems and software.

Secure Wi-Fi Connections: **Use encrypted connections** for sensitive data. Avoid using public networks for municipal work.

Saskatoon, Saskatchewan: - affecting municipal operations; **Victoria, British Columbia**: 2019 - attack on municipal networks;

Best Practices for Cybersecurity

Monitoring Municipal Vulnerabilities

Asset Inventory: Regularly assess digital assets and systems.

Continuous Monitoring and Vulnerability Scans: Be on the **watch**.

Data Management Review: **Data categorization and segmentation**.

Vendor Security Evaluation: **Assess security practices** of partners.

Burnaby, British Columbia: 2022 - disrupting public services; **Coquitlam, British Columbia**: 2023 - impacting local services;

Best Practices for Cybersecurity

Informed Decision-Making

Be Skeptical: Acknowledge and be aware of **things that are not what you usually expect**.

Ask questions: Ensure you are **getting a full picture**.

Medicine Hat, Alberta: 2022 - Cyberattack disrupting public services; **Red Deer, Alberta**: 2023 - Ransomware attack affecting city data;

Best Practices for Cybersecurity

Leading a Security-Conscious Culture

Awareness Training: Regularly update staff on **threats and best practices**.

Onboarding Practices: **Include cybersecurity training** in new hire orientation.

Open Reporting Culture: **Encourage reporting** of security issues and suspicious activities.

Public Communication: **Advocate cybersecurity** in community messages.

Chatham-Kent, Ontario: 2019 - Ransomware on municipal systems; **Peterborough, Ontario**: 2020 - affecting city services;

Best Practices for Cybersecurity

Strengthening Municipal Cyber Resilience

Information Security Policy: Implement a **comprehensive policy and Incident Response Plan**.

Backup Procedures: Implement **robust data backup strategies**.

Cyber Insurance Consideration: Explore options to **mitigate financial risks**.

Expert Relationships: **Build connections** with cybersecurity professionals and law enforcement.

Stay Informed: Keep up with **emerging threats and best practices**.

Burnaby, British Columbia: 2022 - Cyberattack disrupting public services; **Niagara Falls, Ontario**: 2022 - attack on city infrastructure;

Tools we all should be using that will help meet the cyber challenge. - These are just examples, there are many!

Virus Total - https://www.virustotal.com/gui/home/upload (Free)

VirusTotal is a free online service that **analyzes files and URLs** to detect viruses, malware, and other security threats. It uses a wide range of antivirus engines and scanning tools to provide a comprehensive report on the safety of the submitted item. This helps users **identify potentially harmful files or websites** before they cause any damage.

HaveIBeenPwned - https://haveibeenpwned.com/ (Free)

Have I Been Pwned (Pwned means "to own" or to be dominated by an opponent) is a free online service that allows you to **check if your email address or phone number has been compromised in a data breach**. It searches a vast database of known breaches and alerts you if your information has been exposed. This allows you to take steps to protect your accounts and personal information from further harm.

Burlington, Ontario: 2023 - affecting city data; **Cornwall, Ontario**: 2022 - Ransomware disrupting services;

Tools we all should be using that will help meet the cyber challenge. - These are just examples, there are many!

BitLocker - https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ (Free)

BitLocker is a free encryption feature **built into Windows** that **protects your data by encrypting entire drives**. This prevents unauthorized access to your files and folders, even if your device is lost or stolen. BitLocker is available on most Windows editions and can be easily activated through the Control Panel.

BitWarden - https://vault.bitwarden.com (Free and $)

Bitwarden is a freemium (It has a free and a paid-for version) **password manager that securely stores and manages your passwords, credit card information, and other sensitive data**. It offers a free plan with basic features and paid plans with additional functionality, such as secure file storage and priority customer support. Bitwarden is available as a browser extension, mobile app, and desktop application, making it accessible across all your devices.

Sarnia, Ontario: 2021 - Cyber attack on municipal networks; **Peterborough, Ontario**: 2020 - Cyber Attack affecting city services;

Tools we all should be using that will help meet the cyber challenge. - These are just examples, there are many!

1.1.1.1 (Secure DNS) - https://one.one.one.one/ (Free)

1.1.1.1 is a **free Domain Name System (DNS) service provided by Cloudflare**. It functions as a directory for the internet, translating domain names (like NSCTC.ca) into IP addresses that computers understand. 1.1.1.1 **emphasizes privacy and speed**, promising not to log user data and often providing faster resolution times than default DNS servers.

Warp+ - https://blog.cloudflare.com/warp-for-desktop/ ($)

Warp+ is a paid **upgrade to Cloudflare's 1.1.1.1 service**. It **routes your internet traffic through Cloudflare's global network**, aiming to improve connection speed and reduce latency, particularly for geographically distant servers. It also provides an **additional layer of security by encrypting your connection**, making it harder for third parties to snoop on your data.

Chatham-Kent, Ontario: 2019 - Ransomware on municipal systems; **Nanaimo, British Columbia**: 2023 - impacting city operations;

Tools we all should be using that will help meet the cyber challenge. - These are just examples, there are many!

NordVPN - https://nordvpn.com/ ($)

NordVPN is a **paid Virtual Private Network (VPN) service** that **encrypts your internet traffic and routes it through a server in a location of your choice**. This masks your IP address, making it appear as if you're browsing from a different location. NordVPN is often used to access geo-restricted content, protect privacy when using public Wi-Fi, and enhance online security.

These tools can be used to monitor and secure your information and your municipality's information.

Lethbridge, Alberta: 2022 - Cyber attack disrupting municipal functions; **Red Deer, Alberta**: 2023 - Ransomware affecting city data;

A Call to Action, What can you do.

Some simple statements first.

If you use bad password hygiene at home, stats say that you will bring those bad habits to work.

Cisco's 2021 Cybersecurity Study found that employees who do not follow best password practices at home are less likely to adopt secure habits at work. The study revealed that 77% of security professionals believe that personal cybersecurity habits heavily influence an employee's behavior at work.

If someone sees a person "higher up" than them in an organization doing something, they are likely to emulate it.

Leadership Influence: Senior leaders and managers have a significant impact on the behaviour and decisions of employees. Employees are likely to emulate behaviours they see in their leaders, whether good or bad.

Medicine Hat, Alberta: 2022 - Cyber attack disrupting public services; **Kamloops, British Columbia**: 2021 - Ransomware on city systems;

"Follow the Leader" Effect on Compliance and Risk

Employees typically take cues from higher-ups when deciding whether to report issues, follow protocols, or take risks. **If the higher-ups display risky behaviour**, **employees are more likely to do the same**, and this **can ultimately lead to legal or financial risks for the organization**.

Coquitlam, British Columbia: 2023 - Ransomware Impacting local services; **Burnaby, British Columbia**: 2022 - disrupting public services;

Thank you, and please **don’t hesitate to contact us!**

Stephen Franks - smfranks@nsctc.ca

Laura Franks - ldfranks@nsctc.ca

Thank you for joining us today!