So, You Think You Are Safe?
how libraries can be cyber aware
who we are

Krista Robinson
Systems Librarian

STRATFORD
PUBLIC LIBRARY

Lesa Balch
Director of Innovation and Integration

KITCHENER
PUBLIC LIBRARY

Sherry Fahim
Director of Digital Technology and Creation

HAMILTON
PUBLIC LIBRARY
today’s agenda

- Cyber Attacks
- Stratford’s Experience with Cyber Attacks
- Kitchener’s Cyber Assessment
- Hamilton Public Library's Security Program
what is the threat?

A **Cyber Attack** is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks.

A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.

Cybercriminals use a variety of methods to launch a cyber attack, including social engineering, malware and denial of service attacks.
what is the threat?

**Social Engineering** the art of manipulating someone into divulging secret information. These attacks usually exploit human psychology and susceptibility to manipulation in order to trick victims into disclosing sensitive data or break security measures that will allow an attacker access to the network.

Employees are the first line of defense — and they’re also the weakest link. All it takes is one employee clicking on a suspicious link to cost the company thousands of dollars.
what is the threat?

**Phishing** uses disguised email as a weapon. The goal is to trick an email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.
what is the threat?

**Malware** is any piece of software that was written with the intent of damaging devices, stealing data, and generally cause chaos.

Viruses, Trojans, spyware, and ransomware are among the different kinds of malware.
what is the threat?

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
what is the threat?

**Denial of Service (DoS)** is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
some “fun” facts

7 trillion threats stopped by Cisco in 2019, 20 billion a day (Cisco)

20 billion annual ransomware damage cost worldwide by 2021 (CV)

90% successful hacks stem from phishing scams

180 thousand average cost of downtime in Canada in 2019 (Datto Inc)

28 million Canadians were exposed to a data breach in 2019 (not including LifeLabs) (OPC)

5 most attacked industries include: healthcare, manufacturing, financial services, transportation, and government
why municipal services?

• The increased reliance on Internet delivered services present more opportunity

• The data held is attractive

• Less prepared

• Many municipal services pay
what could possibly go wrong?
it’s happening.

**Fraudster hits City of Saskatoon for $1M**

Ottawa

City treasurer tricked into wiring $100K US to fraudster

**Foreign crime group’s cyber attack shuts down networks at libraries, Syracuse schools**

Woodstock library feels impacts of ongoing cyber attack

**Wasaga Beach pays cyber criminals thousands to regain access to town servers: staff report**

**City of Burlington falls for $503,000 phishing scheme**

**Contra Costa County Cyber Attack Snarls County Library Network**
It’s not a question of IF you will get attacked but WHEN
well... it happened to Stratford

City of Stratford managing apparent cyberattack on its systems

‘Days, not hours’: Stratford still dealing with effects of cyber-attack

Cyber attack that cost Stratford city hall $75K ransom should be wake-up call: Expert
Stratford Public Library

- Population 30,000
- 8,600 active cardholders
- In-house IT:
  - staff computers
  - file / web / email servers
  - Internet / wifi
  - 3 IT staff
- Connected to Municipality:
  - file / email services for admin
  - payroll
  - thermostat controls
2019

The City of Stratford is managing what appears to be a cyber attack.
The Cyber “Incident”

- Access gained prior to April 14, 2019
- **April 14 at 8:01am**, encryption of City’s systems began
- April 14 at 1pm, City disconnected from the Internet to contain the incident and workstations are all disconnected
- April 15, the City’s lawyers engaged Deloitte to provide cyber incident response services
- April 17, began negotiations with the attacker on the ransom
- April 19-22, the City’s servers are backed up to prevent loss due to decryption errors
- April 25, decryption of files completed after receiving decryption keys from the attacker
- April 26, Deloitte completed their scan of the City’s endpoints and servers, clearing them for use
- April 29, the City of Stratford returns to “normal” business operations
$15,000
Impact on the Library

• Cut off from the City as of 1pm, April 14
• No access to:
  • Outlook Exchange for senior staff (email & room bookings)
  • File deives for senior staff
  • Financials including payroll
  • Thermostat controls

Not impacted:
• Internet and wifi
• Library owned servers (email / web / file)
• ILS (SaaS)
• Phone system
Impact on the Library

• Gained access to webmail on April 26
• Accessed a copy of our files on a portable drive on May 2
• Reconnected to the network **May 24**
• Still do not have access to certain shared drives with City staff
• STILL cannot control our thermostat
WHEN THE IT DEPARTMENT IS

“WORKING ON IT”
Post Cyber “Incident”

• Additional security measures for drive access
• Mandatory to use a City VPN to access City resources
• Monthly security bulletins
• Security Training & Awareness Session
• No external webmail access from non City managed devices
Lessons Learned

1. Have a Cyber Incident Response Plan
2. Get Cyber Insurance
3. Have an IT team you can trust
Next Steps for SPL

2020 will be revamping our security procedures
  • Improving backup procedures
  • Staff training & awareness
  • Security assessment
thank you!

Krista Robinson
krobinson@stratford.ca
@lilmisslibrary
Kitchener Public Library

- 5 locations, with centralized network and server management at Central Library
- 485 PCs / laptops / tablets / servers + many networked copiers and printers
- Separate networks for staff and public
- Independent of City of Kitchener
- IT Manager + 3 FT IT staff

Where community connects.
Cyber Attacks

Nov 27 2019: **Significant malware attack hits Waterloo Catholic District School Board**

Nov 21 2019: **Waterloo Brewing bilked of $2.1 million in cyberattack**

**Public Libraries:**

Jan 3 2020: Contra Costa County Library, California
Jul 17 2019: Onondaga County Public Library, New York
Jan 29 2018: Spartanburg County Public Library, South Carolina
Cybersecurity Training

• Serene Risc basic cybersecurity online training
• https://cybersec101.ca
1. Internet Concepts
2. Security Concepts
3. Setting Security & Privacy
4. Going Out onto the Internet
Cybersecurity Training, Con’t

5.  Checking the Mail
6.  A Healthy Computer
7.  Have a Backup
8.  Identifying Yourself
9.  Behaving Yourself
10.  Others’ Behaviour
11.  Addressing Online Hate

Where community connects.
Security Measures

January 2018:  Microsoft Office 365 Advanced Threat Protection


April 2019:  Upgraded firewall to increase malware detection & prevention

June 2019:  End-point vulnerability scanning

November 2019:  Sierra – personal logins versus group logins

Where community connects.
Canadian Cyber Resilience Review

• Public Safety Canada  <rrap_perr@ps-sp.gc.ca>
• “ability to manage cyber risk to its critical services”
• Requested Jan 10, 2019 / Conducted Nov 29, 2019
• First identify critical services:
  • Library management system
  • Accounting
  • Payroll
  • Facilities and energy management
Cybersecurity Practices for Critical Services

1. Asset management

• Identify, document and manage assets to support critical services

• People
• Information and data
• Technology – hardware and software
• Facilities
Cybersecurity Practices for Critical Services

2. Controls management

- Identify, analyze and manage controls of the operating environment of a critical service
- People only have access to what they need to do their job
- Regularly audit and review controls
Cybersecurity Practices for Critical Services

3. **Configuration and change management**

- “Disruptions are mitigated and benefits are optimized” when hardware or software or people are added, changed, or removed
- Define who can authorize, and who can make, changes
- Define how to un-do a change, if necessary
- Includes documentation updates
Cybersecurity Practices for Critical Services

4. Vulnerability management

- identify, analyze and manage vulnerabilities for a critical service
- Test for vulnerabilities
- When find a vulnerability:
  - Implement technology tools
  - Train staff regarding expectations
Cybersecurity Practices for Critical Services

5. Incident management

• “mitigate the impact of a disruptive event”

Develop and implement processes to:
• Detect events
• Analyze events
• Respond to and recover from events
• Improve response to future events

• Internal and external communication is key
Cybersecurity Practices for Critical Services

6. Service continuity management

“predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents”

- Business continuity plan
- Technology recovery plan
- Pandemic plan
- Facility recovery plan
Cybersecurity Practices for Critical Services

7. Risk management

• Identify risks to which the operation is exposed

• Analyze / categorize risks and determine action:
  • Avoid, accept, monitor, transfer, or mitigate

• Control risk to reduce probability of occurrence or minimize impact
Cybersecurity Practices for Critical Services

8. External dependency management

• “ensure the protection and sustainment of services and assets that are dependent on the actions of external entities”

• Vendors, including internet provider
• Agreements
• Oversight, reporting and correction of performance
Cybersecurity Practices for Critical Services

9. Training and awareness

Staff understand:
• Issues and concerns
• Policies
• Plans
• Practices – how to perform their responsibilities within organizational guidelines
• On-going
Cybersecurity Practices for Critical Services

10. Situational awareness

Goal: Prevent disruption of a critical service or restore a service to proper function

- General awareness
- Collect and analyze data from external threats
- Identify suspicious behavior
- Communicate threat information
- Participate in threat-sharing communities

Where community connects.
Canadian Cyber Resilience Review

- Comprehensive report with scores
- Comparison to industry peers
- Recommendations to improve cyber resilience
Top 10 Security Actions to Protect Networks and Information

1. Consolidate, monitor and defend internet gateways.
2. Patch operating systems and applications.
3. Enforce the management of administrative privileges.
4. Harden operating systems and applications. Disable all non-essential ports, services, and accounts.
5. Segment and separate information.
Top 10 Security Actions to Protect Networks and Information

6. Provide tailored awareness and training.
7. Protect information at the enterprise level. Implement mobile device management.
8. Apply protection at the host level. Deploy an intrusion prevention system to protect against viruses and malware.
9. Isolate web-facing applications.
10. Implement application whitelisting.
Data Breach

November 1 2018:

• “breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals”

1. report breach to the Privacy Commissioner of Canada
2. notify affected individuals of breach
3. keep record of breach
Next Steps at Kitchener Public Library

- Implement recommendations from Public Safety Canada.
- Conduct staff training and awareness.
- Upgrade facilities and energy management solution.
- Review backup strategy.
- Investigate a centralized intrusion prevention system.
- Implement a VPN (Virtual Private Network) for external access.
- Investigate cyber insurance.
3 Take-Aways

1. Conduct **staff training** – and continue to conduct training.
2. Conduct a security audit – and **implement recommendations**.
3. Develop **continuity and recovery plans**.
So You Think You Are Safe!
OLASC January 2020
Welcome to Hamilton

- Located in the Golden Horseshoe on the westernmost tip of Lake Ontario.
- Hamilton is one of the largest cities in Ontario, and home to 550,000 residents.
- Hamilton Public Library operates 22 branches and 2 bookmobiles across 1137 km².
- Hamilton Public Library has a close relationship with the City of Hamilton by sharing services for firewalls, networks, facilities and ERP system.

The Digital Technology Team consists of 2 managers and 20 staff that manages traditional IT as well as Makerspace services, training and digital literacy.

Sherry Fahim
Director, Digital Technology and Creation
sfahim@hpl.ca
905 5463200 x 3557
Vulnerabilities

• Backdoor access and Privilege escalation
• Denial-of-service and Direct-access attacks
• Eavesdropping, Phishing
• Spoofing and Tampering
• etc ...

DDoS attacks have increased overall in the past 2 years

90% of data breaches could have been prevented

Potential Risks

• Financial systems and impact
• Library and Customer devices
• Privacy Breaches
• Denial of service
• Loss of Data
• etc...

Data Sources: Juniper research and KnowBe4
It happens to us too?

- Every week we successfully block more than 9000 attacks on our website.
- Daily we block over 100 phishing emails with a large portion being malware.
- We receive email scams from what looks like the CEO asking staff’s assistance.
- 6:00 am April 12th, 2018, HPL website was intermittently down for 2 hours due to an attack from multiple IP addresses.
Over 100 phishing emails on a daily basis. The orange line indicates emails with malware.
Our Security Journey

- Protection – Countermeasure Controls
- Policies and Governance
  - Information Security Culture
  - Security Programs Development
  - Security Testing and Assessment
  - Incident Response planning
Protection and Controls

**Security by Design**
- Limit collection of information
- Security architecture
- Security measures

**Vulnerability Management**
- Reducing Vulnerabilities
- Hardware protection
- Network protection e.g. firewalls
- Segregated Networks – staff and public, library and city
- Secure operating Systems - applying patches

**Access Controls**
- Manage access rights
- Alert systems – password complexity and changes
- Security controls - physical space as well as network access
Controls and Protection Measures

High Level Network Controls

Internet → Firewall → Web Filtering → Antivirus
Strategic Approach

Policies and Governance
- Access and Security Policy
- Privacy Policy for Library Customers
- Technology Use Policy for Library Customers and For Staff
- Technology Innovation and Security Steering Committee

Security Program Development – w/ Infotech
- Security Assessment - Gap analysis
- Security Initiative Priorities -
- Security Program Plan

Information security culture
- Security Awareness Training – Staff & Public
- Announcements on Intranet
- Reporting of Spam – phishing emails - controlled email testing
Major and detailed initiatives were identified, with assistance of Info-Tech Research Group, to improve specific security domains, and HPL’s overall security posture. Many foundational security initiatives were identified as necessary to lay the ground work for further advanced work.

1. Current State Evaluation
   Often identified ways to improve

2. Determine Target State
   Decided what is a necessary and expected level to mature to

3. Identified Initiatives to Reach Expected Level

Security Program Development - Maturity Gap

Security Strategy Dashboard

Initial Snapshot - size of gap between initial and target state

Legend and Customization
- Maturity gap of 0
- Maturity gap between 0 and 1
- Maturity gap between 1 and 2
- Maturity gap greater than 2

Assessment of current state
Security Program Development - Maturity Gap

Security Maturity Level Gap Analysis

Assessment against target state
Security Program Development

• A total of 118 potential initiatives were identified
• High level costs and effort are estimated
• Initiatives are prioritized considering level of risk and costs
• Similar initiatives are grouped together to develop a Road Map

The information security charter includes the expectation and requirements of interested parties and necessary business stakeholders.

The information security charter includes a statement describing the scope (including data, systems, locations, and organizational units).

The information security charter includes the vision and mission for the security program.

The information security charter includes the objectives for the security program.

High-level responsibilities for the security program are outlined and assigned by role or group in the security charter (e.g., using a RACI chart).

Governing security principles (either custom to the organization or following recognized best practices) are included in the security charter.

The information security charter is communicated to the organization.

The information security charter is regularly reviewed, evaluated, and updated.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Doing Now</th>
<th>Initiatives that are already underway and/or are part of IT projects in progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 0</td>
<td>Next 6 Months</td>
<td>High priority – actionable immediately</td>
</tr>
<tr>
<td>Phase 1</td>
<td>6 Months – 1 Year</td>
<td>High-value extended controls, key documentation, and investigation of value and relevance</td>
</tr>
<tr>
<td>Phase 3</td>
<td>2021</td>
<td>Lower value/higher customer impact/longer-term controls – defer for immediate term includes low benefit documentation</td>
</tr>
<tr>
<td>Phase 4</td>
<td>2022 and Beyond</td>
<td>High cost/value controls or initiatives deferred for other reasons</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phases</th>
<th>Example of initiatives into buckets:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 0+1</td>
<td>Phase 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content and Leadership</th>
<th>Information Security Charter</th>
</tr>
</thead>
<tbody>
<tr>
<td>The information security charter includes the expectation and requirements of interested parties and necessary business stakeholders.</td>
<td>The information security charter includes a statement describing the scope (including data, systems, locations, and organizational units).</td>
</tr>
<tr>
<td>The information security charter includes the vision and mission for the security program.</td>
<td>The information security charter includes the objectives for the security program.</td>
</tr>
<tr>
<td>High-level responsibilities for the security program are outlined and assigned by role or group in the security charter (e.g., using a RACI chart).</td>
<td>Governing security principles (either custom to the organization or following recognized best practices) are included in the security charter.</td>
</tr>
<tr>
<td>The information security charter is communicated to the organization.</td>
<td>The information security charter is regularly reviewed, evaluated, and updated.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current State</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Context and Leadership</td>
</tr>
<tr>
<td>2.0</td>
<td>Information Security Charter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current Maturity</th>
<th>Current Average</th>
<th>Current State</th>
<th>Target Maturity</th>
<th>Target Average</th>
<th>Gap Description</th>
<th>Common Gap Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>0.0</td>
<td>1 - 4 Define scope, vision, mission &amp; objectives with business stakeholders to get buy-in.</td>
</tr>
<tr>
<td>2</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>0.0</td>
<td>2 - 3 Document and define an information security charter.</td>
</tr>
<tr>
<td>3</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>3.0</td>
<td>0.0</td>
<td>3 - 4 Define scope, vision, mission &amp; objectives with business stakeholders to get buy-in.</td>
</tr>
<tr>
<td>4</td>
<td>4.0</td>
<td>4.0</td>
<td>4.0</td>
<td>4.0</td>
<td>0.0</td>
<td>4 - 5 Sign-off on charter document and provide dedicated resources to support implementation of the charter.</td>
</tr>
<tr>
<td>5</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
<td>0.0</td>
<td>5 - 6 Assign high-level responsibilities and roles to support implementation of the charter.</td>
</tr>
</tbody>
</table>

Current Maturity: 3.0, Target Maturity: 5.0, Common Gap Initiatives: 1 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.
Security Program Awareness

- Training campaign launched on Staff Day 2018
- Training to understand and protect against Malware
- Use silly videos and real life examples to train
- Staff Tech Benchmark plan include security module
- Train staff over 1 year and refresh every 2 years
- Offer security awareness program to the Public
- ...more to come .. such as Controlled email testing; Intranet did you know and security tips