

# Cyber Security Update

Ryan Parker, CISSP CISA  
Information Security Manager

# Presentation Overview

- Cyber Security Trends and Challenges
- Approach and Strategy
- Recent Improvements & Priorities
- Resourcing
- Strategic Alignment

# What is Cyber Security?

*Cyber Security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.<sup>1</sup>*

- Cyber crime is one of the fastest-growing criminal activities in the world and has surpassed illegal drug trafficking as a criminal money maker <sup>2</sup>
- The average financial cost of downtime to a Canadian business following a ransomware attack is 7.5 times higher than the average ransom requested per incident <sup>3</sup>
- 6.4 billion - The number of fake emails sent worldwide — every day <sup>4</sup>
- 550 million - The number of phishing emails sent out by a single campaign during the first quarter of 2018 <sup>5</sup>
- 1,946,181,599 The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018 <sup>6</sup>

1. Cisco Systems [<https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>]

2. Symantec Corporation [[https://www.symantec.com/about/newsroom/press-releases/2009/symantec\\_0910\\_01](https://www.symantec.com/about/newsroom/press-releases/2009/symantec_0910_01)]

3. Scalar 2019 Scalar Security Study: The Cyber Resilience of Canadian Organizations

4. Dark Reading, August 27, 2018. [<https://www.darkreading.com/endpoint/64-billion-fake-emails-sent-each-day/d/d-id/1332677>]

5. Dark Reading, 26 April 2018. [<https://www.darkreading.com/vulnerabilities---threats/new-phishing-attack-targets-550m-email-users-worldwide/d/d-id/1331654>]

6. Chronology of Data Breaches, March 2018. [<https://www.privacyrights.org/data-breaches>]

# Cyber Security Trends

- Common Methods of Attack
  - Malware i.e. Ransomware
  - Exploited Vulnerability
  - Social Engineering
  - Human Error
- Recent Municipal Experiences
  - Ransomware
  - Privacy Breaches
  - Fraud

# Recent Municipal Experiences

Kitchener-Waterloo

## City of Stratford managing apparent cyberattack on its systems

Recovered from backups. Estimated downtime was two weeks.



Phone system, online forms also down Monday morning

Jackie Sharkey - CBC News - Posted: Apr 15, 2019 12:19 PM ET | Last Updated: April 15

## Midland servers hacked, attackers demanding ransom

NEWS Sep 04, 2018 by Andrew Mendler Midland Mirror

## Ransomware costs continue to climb for Wasaga Beach

NEWS Aug 27, 2018 by Ian Adams Wasaga Sun

\$35K ransom paid. Estimated recovery cost was \$250K.

CBCnews | Kitchener-Waterloo



Home Opinion World Canada Politics Business Health Entertainment Technology & Science

Canada Kitchener-Waterloo

## Guelph fires deputy CAO after privacy breach

CBC News Posted: Feb 09, 2017 12:44 PM ET | Last Updated: Feb 10, 2017 8:15 AM ET

53K emails accidentally released

## Some Brampton Residents Affected by Serious Privacy Breach

by Rajpreet Sahota on May 23, 2019 in News

Personal information of 13K residents exposed by a misconfigured system

CRIME June 13, 2019 5:23 pm

## City of Burlington defrauded out of \$503,000 due to phishing scam



By Lisa Polewski  
News Anchor 900 CHML

CANADA April 8, 2019 3:37 pm

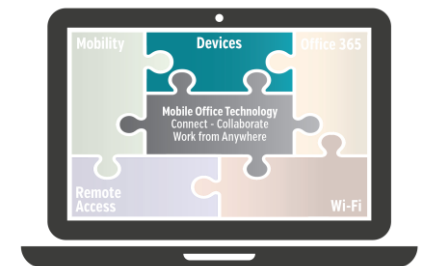
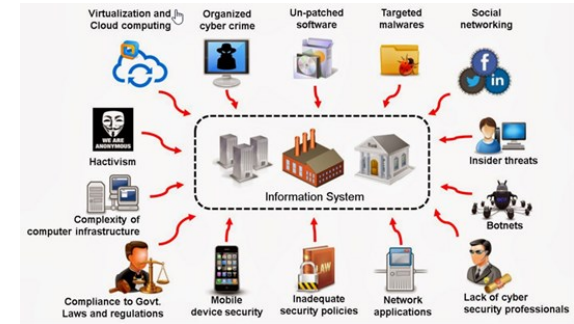
Updated: April 10, 2019 7:29 am

## Scam email impersonating Ottawa city manager tricked treasurer into wiring \$128K to fraud supplier

By Beatrice Britneff Local Online Journalist Global News

# Cyber Security Challenges Facing The City

- Changing threat landscape
  - Targeted Malware
  - Monetized Threats
  - IT Infrastructure Complexity
- Emerging Technology Demand
  - E.g. Mobility, Cloud, Remote Access, Internet of Things
- IT Inventory Asset Management
  - We need to “know” what we “don’t know”
  - Managed vs. unmanaged



# IT Security – Our Approach



# IT Security - Our Program





# Recent Improvements



- ✓ Build on existing strong foundational practices
- ✓ Have upgraded all safeguards in the past two years
- ✓ Strengthened security language in procurement practices
- ✓ Cyber Insurance - purchased in 2018
- ✓ Information Security Framework Implementation
  - ✓ ITS Security Maturity Assessment – *Completed 2018 Q4*
  - ✓ Maturity Assessment Remediation Plan – *Developed 2019 Q2*
    - ✓ Developed 5 Year Workplan
    - ✓ Strategic approach to strengthening administrative and technical controls
  - ✓ Staff Security Awareness and Training Program – *Implemented 2019 Q3*
    - ✓ Mandatory foundational security training for all staff with a City email address
    - ✓ 2019 will focus of security basics and social engineering

# Priorities

- Implement the Information Security Framework
  - Pragmatic approach to build effective layers of control
  - Build detection and prevention techniques in equal measure
  - Work towards optimizing and enabling growth
  - Focus on a long-term alignment with NIST Cyber Security Framework
- Information Security Policy redevelopment – *In Progress, to be completed 2019 Q4*
- Corporate Incident Response Plan – *In Progress, to be completed 2020 Q1*
- Continuation of the Corporate Security Awareness and Training

# IT Security - Resourcing

- Staffing
  - 1 FTE (IT Security Manager)
  - Some responsibilities distributed among other ITS staff
- Previously Approved Capital Budget (\$100k)
  - Information Security Framework
  - Awareness Training
  - Policy Development
- Future - 10 year Capital (\$600k)
  - Annual IT Security Enhancements
  - 2020 Mobile (endpoint) Security
- Operating Budget (~\$195k)
  - Security Safeguard Tools and Assessments (includes backup/recovery)
  - Assessment of additional needs being considered annually

# Strategic Alignment

- IT strategic vision statement: *Innovative city services powered by tech-savvy people, modernized technology and meaningful information*



Tech Savvy Culture



Information as an  
Asset



Technology Systems  
Modernization



IT Service  
Modernization



Enterprise Systems

- Vision to Focus Alignment
  - Delivering Customer Centric Services with a Focus on Efficiency and Technology Transformation
  - Increasing corporate resilience to cybersecurity threats through effective and proactive IT security management practices



Focus Area 5

# Questions?