are you

FUTURE READY?

Cyber Security Audit
City of Markham

Date:

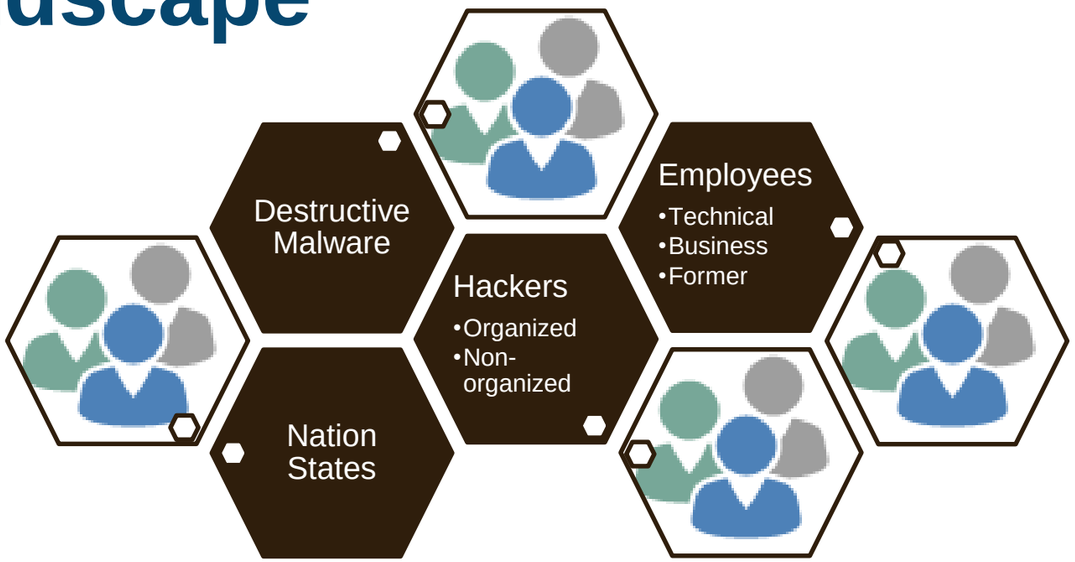
March 26, 2018

Agenda

1. Background and Landscape
2. Approach
3. Overall Results
4. Industry Comparison
5. Auditor General Recommendation and Management Response
6. Questions

Background and Landscape

- **Attackers find value in sensitive information**
- **Organizations are finding it challenging to protect against threats**
- **Attacks can originate from various sources**
- **Avenues of attacks continue to evolve**

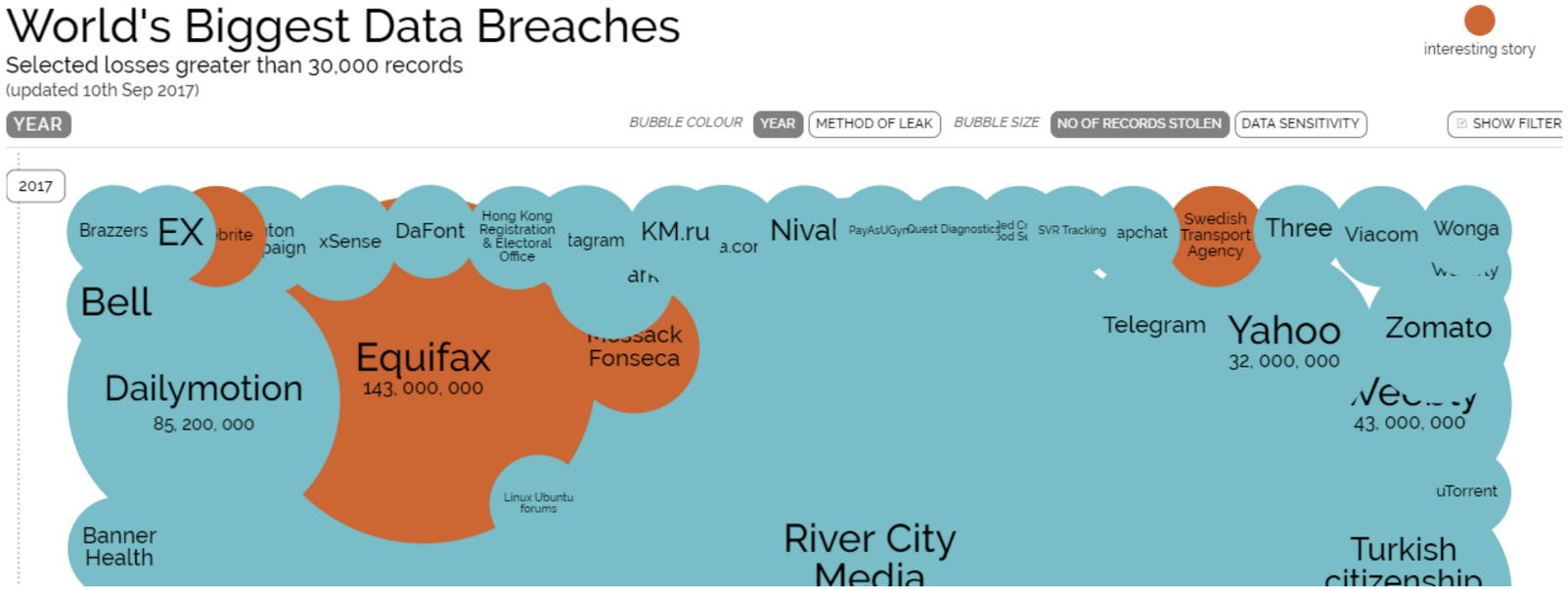


Business Information

Personal | Proprietary | Credit Card

Client | Employee

Background and Landscape



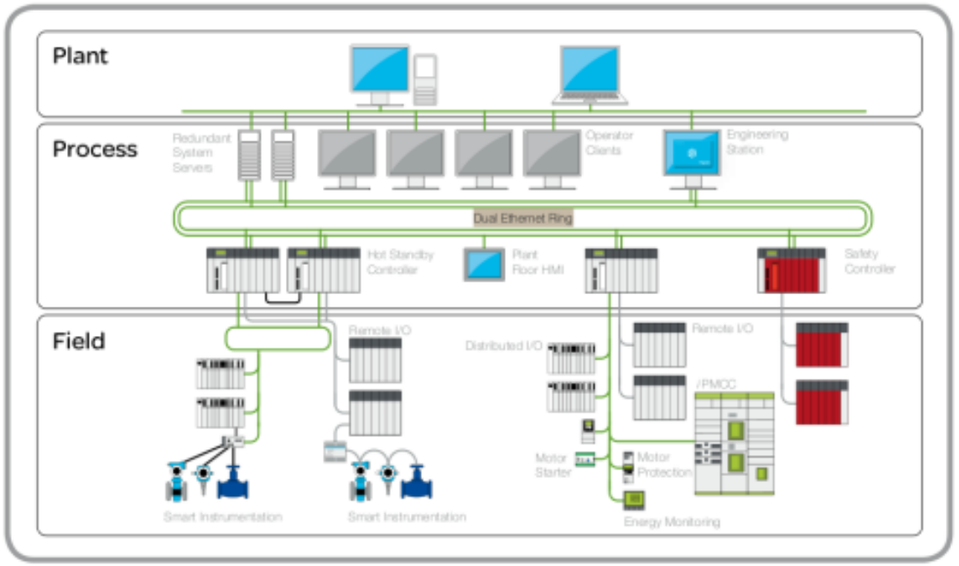
- **The Verizon 2017 Data Breach Investigations Report describes public sector organizations as having the third highest number of reported breaches (and increasing)**
- **Unreported (or undetected) breaches may be even worse**

Background and Landscape

Attackers are targeting industrial control systems

- Water treatment and pumping
- Electrical control systems
- Traffic control systems

These systems are converging with corporate IT systems



Source: Schneider Electric

Audit Objective

- **MNP evaluated the effectiveness and reasonableness of the City's logical security and management/monitoring controls relating to cybercrime prevention, detection and incident management processes, policies, procedures, and security governance activities**
- **Focused on the following elements:**

Security policies, planning, risk management	Security training and awareness	Physical and logical security access controls	Operational security practices
Information sensitivity classification	Security assessment practices	Security monitoring and incident management	

Approach

1. Project Planning

- Define objectives and scope
- Confirm project duration and schedule
- Define team members and structure
- Define deliverables
- Obtain understanding of systems environment
- Develop audit work program
- Draft Audit Planning Memo
- Distribute to City and Council

2. Project Execution (Controls Assessment)

- Conduct interviews and discussions
- Review policies, standards, and procedures documentation
- Observe IT systems and configurations
- Evaluate and assess current state against best practices and security frameworks

3. Project Reporting

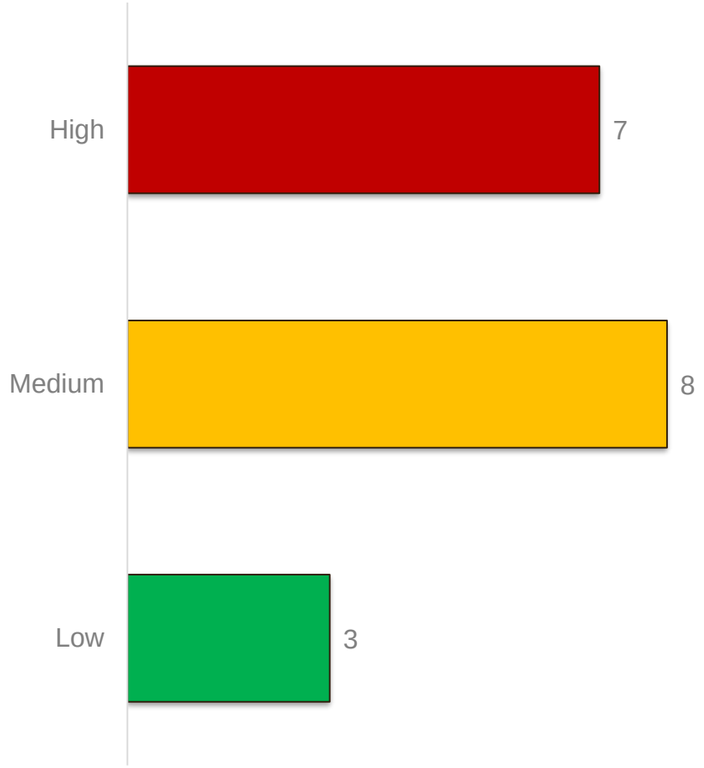
- Identify improvement opportunities
- Draft report with findings and recommendations
- Validate observations and present recommendations
- Issue final report

Overall Results – Strengths

- **The City has implemented good practices to protect the security and confidentiality of information on its IT systems**
- **Strengths noted include:**
  - ✓ Perimeter network defenses
  - ✓ Anti-malware software
  - ✓ Hard drive encryption
  - ✓ IT system backup
  - ✓ Administrative access
  - ✓ Vulnerability assessments
  - ✓ Mobile device management security

Overall Results – Risks

- **Notwithstanding the efforts and investment in security**
- **We identified several areas for improvement**
- **Gaps expose the City to a malicious attacker and unauthorized access to systems**
- **18 observations in total**

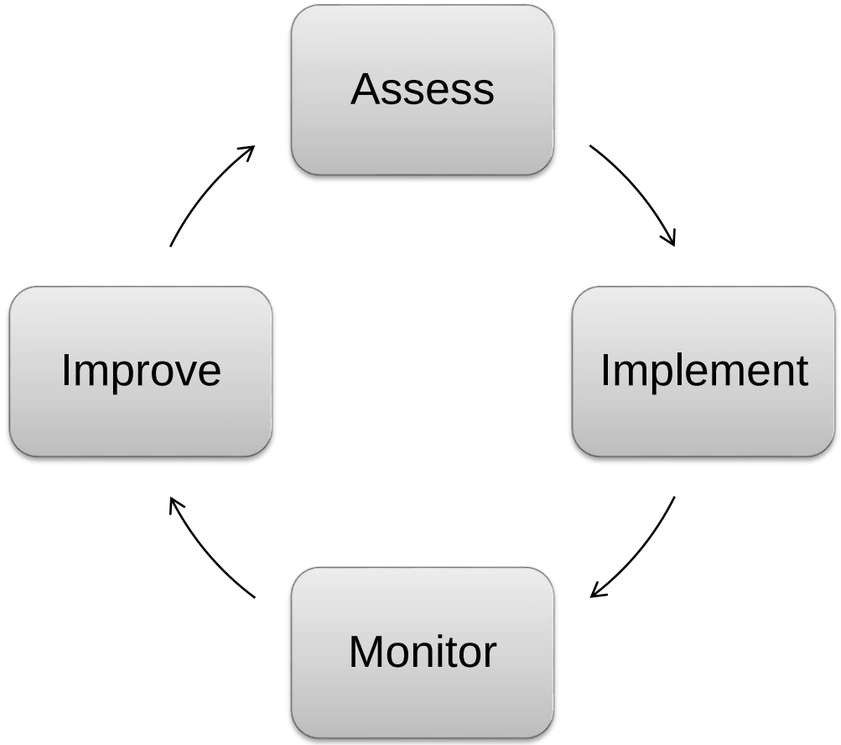


Overall Results – Security Program

- **Most notably, the City has not formally and sufficiently defined its overall security program**
- **For example, there is no:**
  - Strategy
  - Roadmap
  - Policies
  - Dedicated security resources

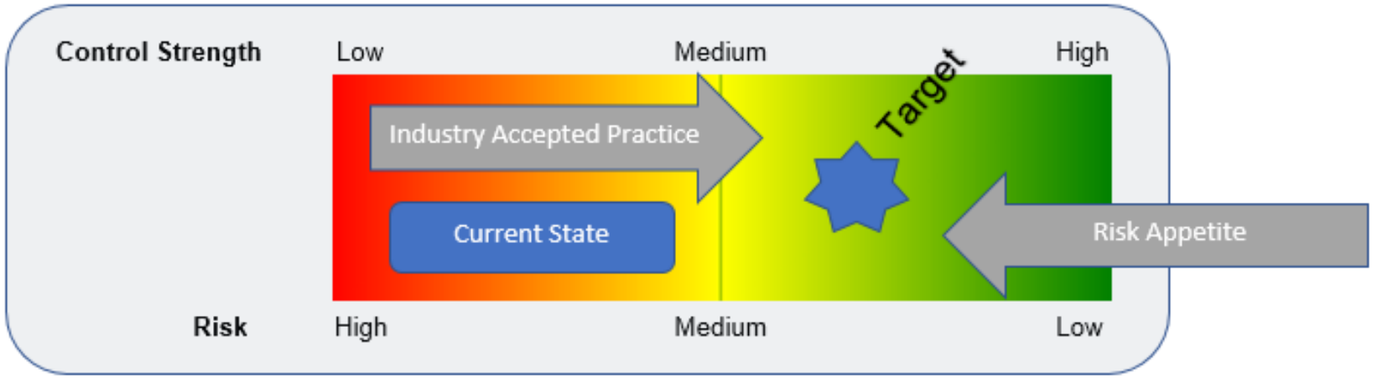
Overall Results – Security Program

- **An effective and comprehensive security program:**
  - Forms the foundation for security practices
  - Structured and tailored plan to manage security risks
  - Continually monitored and maintained
  - Addresses business requirements
  - Changes to the security threat landscape
- **Proactive vs re-active approach**



Overall Results – Security Program

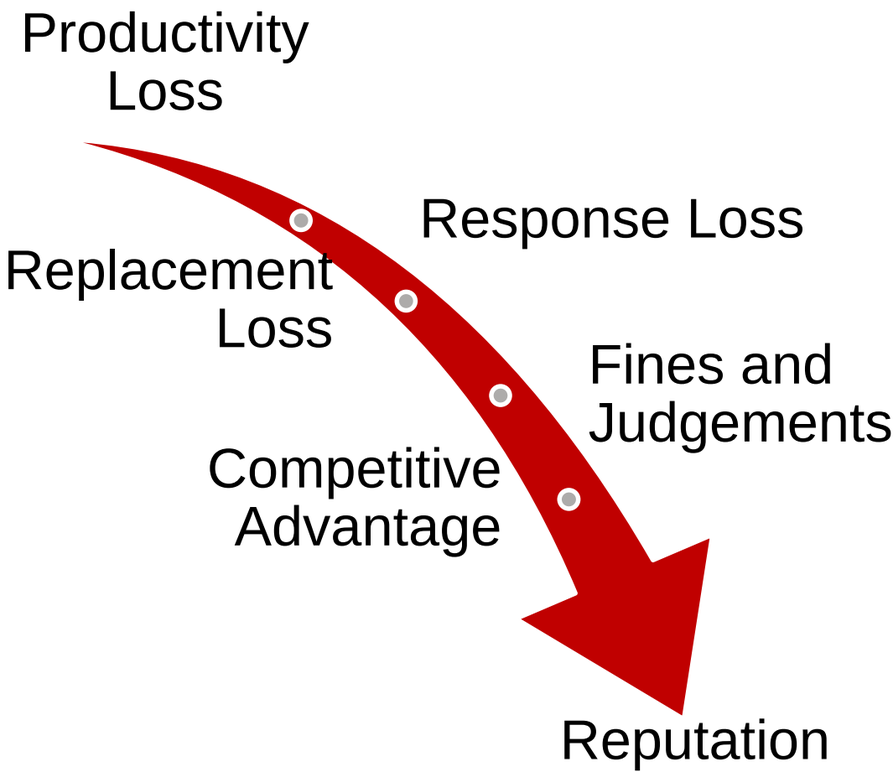
- **No one-size-fits-all approach to managing cyber security risk**
- **Security program should be based on:**
  - ❑ Risk appetite
  - ❑ Industry accepted practices
- **City should define their risk appetite and target state that they want to achieve:**
  - ❑ Implement the program
  - ❑ Address high and medium risks



Overall Results – Impact

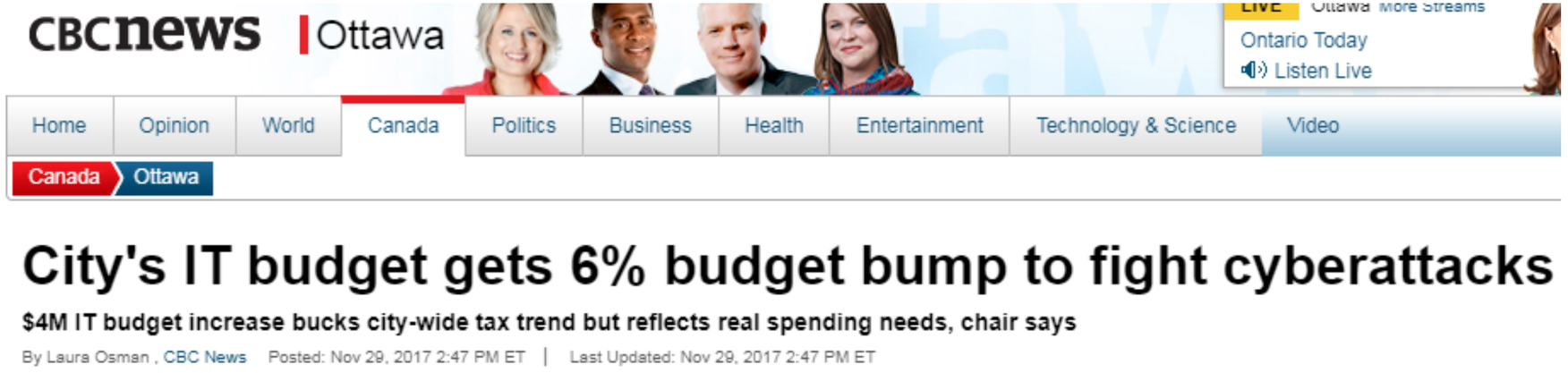
- **Weaknesses identified increase the risk of an information security incident or data breach**
- **May have a significant and negative impact on the City**
- **Difficult to assess the actual cost of a data breach**
  - Value and loss of information is challenging to measure
  - Many considerations
  - Cost of a breach ranges:

    $10,000 - $10,000,000



Industry Comparison

- **Many organizations struggle to implement and sustain strong security practices**
- **Many municipalities are starting to assess their cyber security posture and build their own security program**



Auditor General Recommendation and Management Response

- **The Auditor General's overall recommendation is for the City to enhance the current security program by formalizing efforts and priority for cyber security. The City should determine the level of security that they wish to achieve, improve their existing practices, and monitor progress towards its security objectives.**

- **The City supports the Auditor General's recommendation and will enhance its current cyber security practices by:**
  - Developing a comprehensive security program which will provide a sustainable approach to enhance the City's cyber security posture based on accepted levels of risk tolerance (deemed appropriate by the City), including:
    - Security strategy and roadmap;
    - Security policies and procedures; and,
    - Identification of budget and resources required.

Recommendation

The Auditor General recommends that:

1) The Cyber Security Audit Presentation be received.

Questions?