Cybersecurity:

Protection of City of Saint John information system hardware, software and data

September 23, 2021

SAINT JOHN

Investing in Cybersecurity

Cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains

Cybersecurity involves the measures taken to protect a computer or computer system from an unauthorized access or attack

Cyber Threats

People are often the prime target for a cyberattack

Cost of CSJ Cyberattack

- Phishing email
- Reconnaissance
- Administrative Rights
- Lateral Movement
- 13 Nov 2020 Attack
- All Windows Servers Impacted
- Temporary Network – Days
- Core Network – 14 Weeks
- Back-Up System – 18 Weeks
- Application (60+) Restores 2022

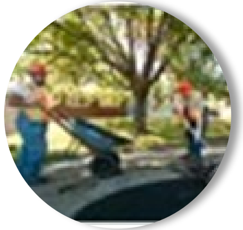
Event Management	$34,421
Recovery Consultants	$902,683
Forensic Consultants	$295,955
Third Party Vendors	$460,098
Equipment	$1,189,141
Overtime	$43,198
Response	$10,681
Business Continuity	$14,234
Estimated Total 6 Apr 2021	$2,950,409

Intangible Costs of Cyberattacks

Workforce Balance

Pride In IT Customer Service

Confidence in IT Service Delivery



Productivity

Opportunity

Data Loss

Security Investment Since 2019

- ✓ Risk Threat Assessments
  - ✓ Security Information and Event Management (SIEM)
  - ✓ Cyber Insurance
  - ✓ Enhanced Antivirus Solution
  - ✓ Vulnerability Scanning and Penetration Testing
  - ✓ Cybersecurity Expertise
  - ✓ Patching
  - ✓ Employee Education - Cybersecurity 101
- ✓ Firewall Upgrades
- ✓ Payment Card Industry (PCI) Compliance Process*
- ✓ Security and Recovery Plans

SIEM and SOC

Security Information and Event Management

Security Operations Centre

- Alert to Suspicious Activity
- Containment of Damage
- Partnership in Rebuild

Continuous Improvement of Cybersecurity

- Access (MFA)
- Enhanced Security in Network Design
- Robust Back-up System
- Documentation of Network, Applications, Data Governance
- Policy and Standard Operating Procedures (User)
- Enhanced Education of the User
- Continuous Upgrading of IT Team Skills

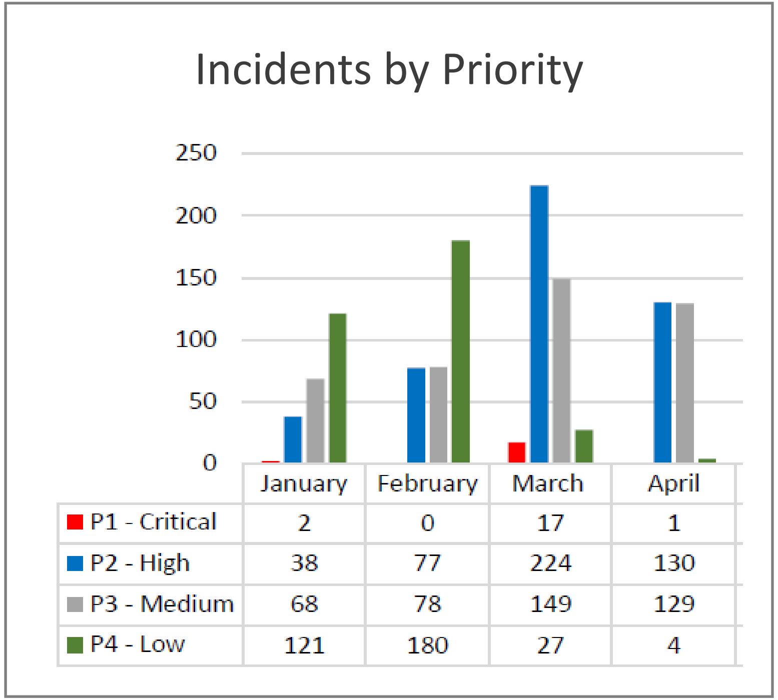
Long-Term Impacts on City Services

- The City has continued to deliver all required services throughout the event.
- Security and stability of systems have been enhanced through the recovery process.
- Operating costs have increased to enhance security management and management of capital equipment cost has increased.
- In the short-term, the City is leveraging workarounds as services are restored and some services are being delivered manually until full restoration. Data availability is allowing for restoration of applications.
- The City does not see any long-term negative impacts on the City's ability to deliver services.

Assume You Are Already Hacked

Incident Response Preparation

Security Operations Centre


Incidents by Priority

	January	February	March	April
🟥 P1 - Critical	2	0	17	1
🟦 P2 - High	38	77	224	130
▨ P3 - Medium	68	78	149	129
🟩 P4 - Low	121	180	27	4

April Analysis

- 698.4M Security Events
- 470 Security Alerts
- 275 Incidents Investigated
- 2 Incidents Escalated

Implications on GNB Municipal Sector

- More awareness that attacks are taking place and it is not “if” but “when” the next attack will take place.
- Majority of municipalities in NB are small with limited resources to respond to attacks of this magnitude. GNB should consider investing in a strategy to help smaller municipalities with cyber security event management.
- Enhanced collaborative discussions between municipalities pertaining to such events would be beneficial.
- Need for a shared emergency vendor procurement vehicle shared across municipalities.

Cybersecurity:

Protection of City of Saint John
information system hardware, software and data

September 23, 2021

SAINT JOHN