CYBER SECURITY KNOWLEDGE EXCHANGE

Moderated By:
Monday, August 21, 2023

Association of
Municipalities Ontario

Cyber Governance Strategies for Mayor's and Councillor's

August 21, 2023

AMO Conference 2023

MISA Ontario

Municipal Information Systems Association, Ontario (MISA Ontario)

- We are a community of experts and practitioners who provide leadership, guidance, and resources for anyone interested in using technology to improve municipal services.

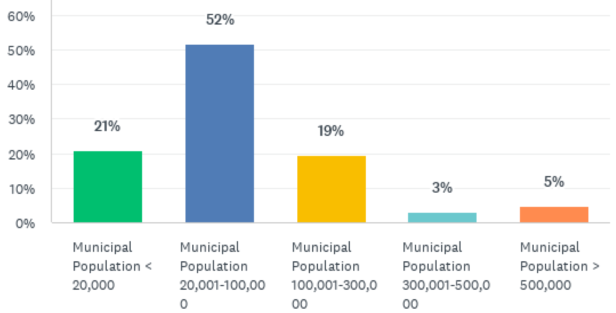
- We provide technology-focused online resources, directories, and events targeted to municipalities of all sizes and represent 1400+ dedicated professionals working towards a more effective government.

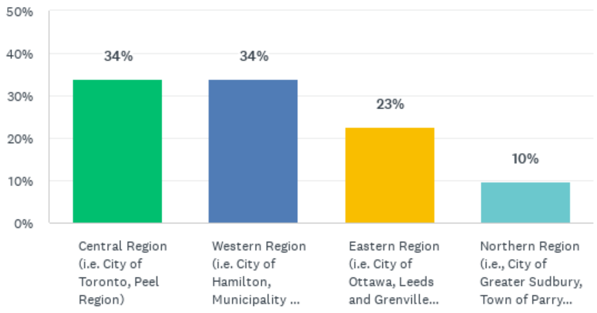
- Considering cybersecurity is key risk to Municipalities, MISA Ontario has a dedicated program for members consisting of several initiatives:
  - Annual InfoSec Conference and Trade Show
  - Annual Cyber Security Outlook Survey
  - Cyber-focused webinars and content from municipality members and industry experts
  - Building partnerships with academia, governments and the private sector to provide benefits for members

https://www.misa-asim.ca/page/ON_Homepage

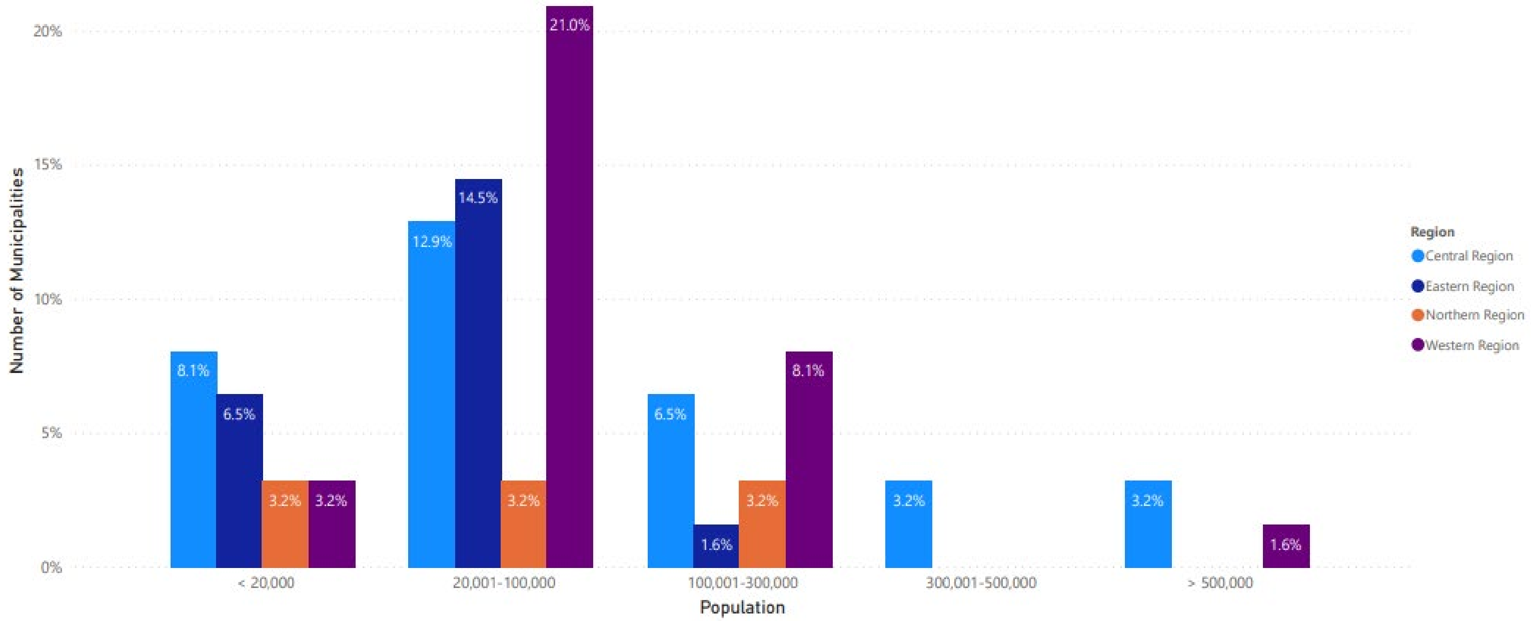
Cybersecurity Outlook Survey 2022

Positive response representing a diverse cross-section of Municipalities from a Population and Region perspective:

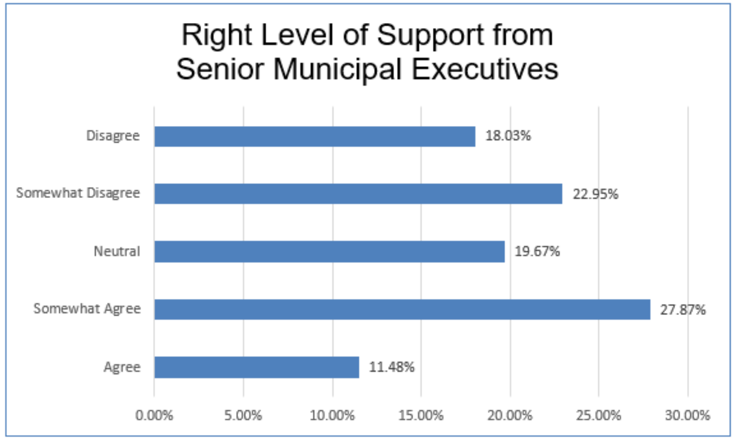




Respondent By Region and Population



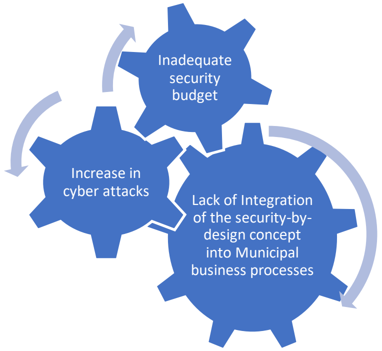
Cybersecurity Outlook Survey 2022



100%

Top 5
Priority

Top 3


Inadequate security budget

Increase in cyber attacks

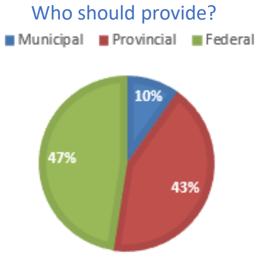
Lack of Integration of the security-by-design concept into Municipal business processes

84%
Should have
dedicated role

75%
Centralized
function

67%
No dedicated
role today

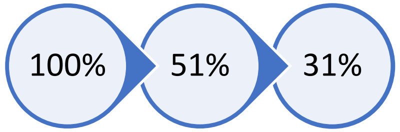
71%
Cyber Services
to Citizens



MISA Ontario

Cybersecurity Outlook Survey 2022

Cyber Response Plan



Investment should be made

Have a Plan

Plan: Test yearly

Critical Infrastructure & Business Apps

92%
Focus First

97%

Integrate cybersecurity & privacy by design principles into all transformations, initiatives, projects and procurements

Priority
Dedicated Funding

What is cybersecurity?

CYBERSECURITY

- Protection of assets:
    - People (staff, citizens, etc.)
    - Processes (IP, etc.)
    - Technology (devices, servers, networks, data, etc.)
- Response to those assets being breached

CYBER GOVERNANCE

- Strategic view of how an organization controls its security
- Defining its risk appetite
- Establishing accountability and decision-making frameworks
- Effective governance will also ensure that cybersecurity supports Municipal strategic goals

What is cybersecurity **not**?

DIFFICULT

I don't understand, it's too complicated

- Educate yourself
- Similar to managing finances (we don't know every detail regarding all accounts/invoices)

COMPLEX

We can't stop cyber attacks, there's just too many

- Take the first step
- Most attacks exploit known vulnerabilities (simplicity, cost effective method)

TARGETED

I'm a Municipality, why would someone attack me?

- Many attacks are opportunistic and financially motivated (untargeted)

**Adopted from the National Cyber Security Centre: Cyber Security Toolkit for Boards: 2019*

Good Governance Considerations

Embed into Organization Structure / Objectives

- Have we defined individual and collective cyber responsibilities?
- Who currently is responsible for cyber?
- How do we assure that our Municipality's cyber measures are effective?
- Do we have a process the integrates cyber risk with business risk?

Build Cybersecurity Skillsets

- What cyber skillsets do we have? Need?
- What is our plan to develop skills we don't currently have?
- Do I have the right level of knowledge to make cyber decisions on behalf of the Municipality?
- Are we building a workforce with DEI principals?

Develop a positive Cybersecurity Culture

- Do I lead by example?
- Do we have the right policies in place?
- What skills are a priority?
- Do we have a good cyber culture?
- What do we do to encourage a positive cyber culture?
- Do we have an environment in which staff feel confident, safe and comfortable raising cyber issues?

**Adopted from the National Cyber Security Centre: Cyber Security Toolkit for Boards: 2019*

Good Governance Considerations

Establish Baseline / Define High Value Assets

- Do we have a clear understanding of how systems/applications, processes, assets are contributing towards Municipal objectives?
- Have we clearly communicated Municipal priorities, and do we have assurance that cyber is guided by these?
- How do we identify and keep track of systems/applications, data or services?

Understand Threats

- Which threats do we assess?
- Which threats are relevant to our Municipality? Why?
- How do we stay up-to-date with the latest cyber threats?
- How do we use threat intelligence to inform business as usual? (e.g., educating staff, change procurement approach)

Define & Manage Cybersecurity Risk

- Do we have a process that ensures decision makers are well informed?
- Do we have a process that ensures cyber risk is integrated with business risk?
- Do we have an approach to manage cyber risk?
- Have we clearly set out what types of risks we would be willing to take? Those that are unacceptable?

**Adopted from the National Cyber Security Centre: Cyber Security Toolkit for Boards: 2019*

Good Governance Considerations

Implement Cybersecurity Measures

- Do our measures align with industry frameworks like ISO/IEC 27002 or NIST?
- How do we assure that our measures are effective?
- What measures do we take to minimize the impact an attacker can have?
- Do we implement cyber controls to defend against the most common attacks?

External Collaboration (Suppliers, Vendors, etc.)

- How we mitigate the risks associated with sharing data and systems with third parties?
- How do we ensure that cyber is considered in business decisions? (e.g., procurement)
- Are we confident that our third parties (e.g., suppliers) are adhering to cyber standards?
- Do we have a clear strategy for using suppliers? Has it been communicated?

Establish & Test your Incident Response Plan

- Do we have an incident management plan? Do we test it for effectiveness annually?
- Do we know where we can go for help during an incident?
- Do we learn from incidents or near misses?
- How would we know when an incident occurred?
- Do we know who leads incident response? Who has authority to make decisions?
- Do I understand what's required in my role during an incident? Have I had training?

*Adopted from the National Cyber Security Centre: Cyber Security Toolkit for Boards: 2019

Kush M Sharma

Director, Municipal Modernization & Partnerships

Municipal Information Systems Association, Ontario

kush@misa.on.ca

https://www.misa-asim.ca/page/ON_Homepage

https://www.misa-asim.ca/page/CA_Membership

Panel Roundtable Question:

How much will a cyber incident cost a municipality?

Ontario Canada

St. Marys

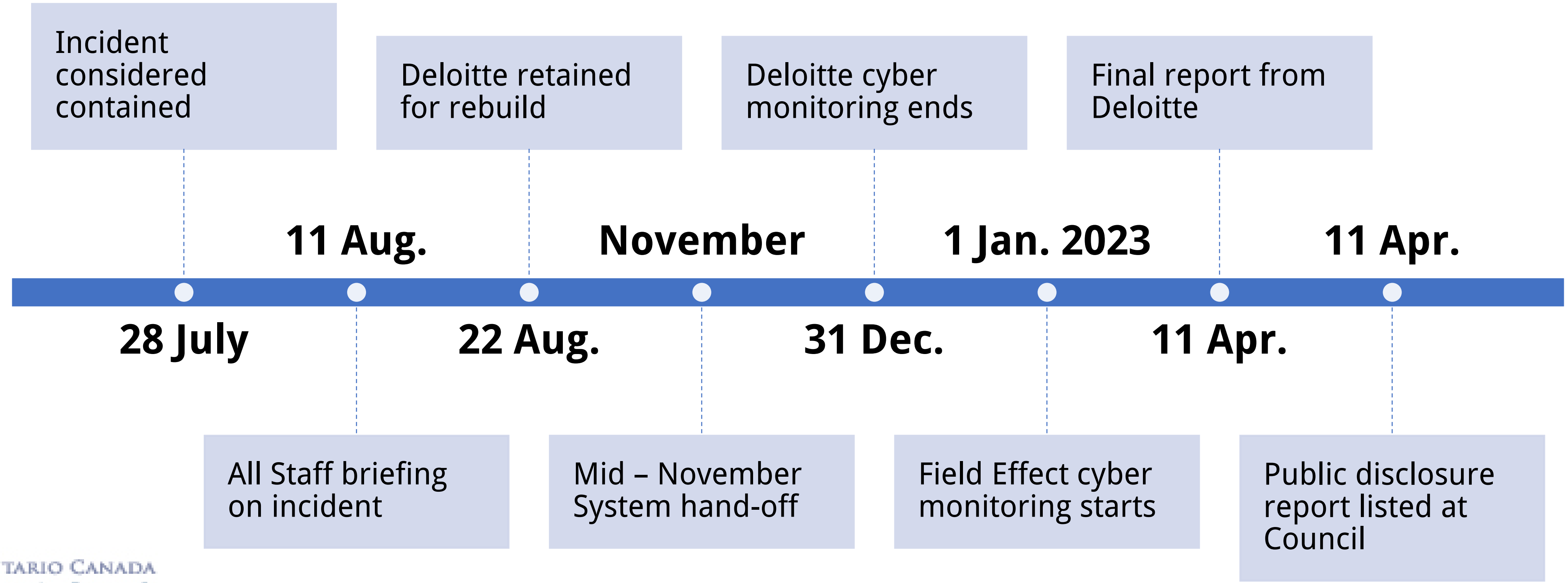
- Located in Southwestern Ontario between Stratford and London
- Situated at the junction of the Thames River and Trout Creek
- Unique architecture featuring locally-quarried limestone

- Single Tier Municipality – 7,400 pop
- Council of 7, elected at large
- 65 FT employees, 90+ PT/Seas.
- $27M Annual Budget
- $14M Tax Levy

ONTARIO CANADA
ST. MARYS

CYBER INCIDENT – JULY 20, 2022

- Lockbit 3.0 Ransomware
- Internal Network Compromised



28 July

Incident considered contained

11 Aug.

All Staff briefing on incident

22 Aug.

Deloitte retained for rebuild

November

Mid – November System hand-off

31 Dec.

Deloitte cyber monitoring ends

1 Jan. 2023

Field Effect cyber monitoring starts

11 Apr.

Final report from Deloitte

11 Apr.

Public disclosure report listed at Council

Ontario Canada St. Marys

CYBER INCIDENT COSTS

SOLUTION	COST
Incident Management/Investigation	$860,000
Network System Rebuild	$440,000
TOTAL	**$1,300,000**

External Assistance

- **Cyber Insurance**
  - Call Insurance Company
- **No Cyber Insurance**
  - Follow your incident response plan

ONTARIO CANADA
ST. MARYS

External Assistance

- Current IT/Legal Consultants may **NOT** be able to assist
- Police will want information, but **NOT** able to assist
- Provincial/Federal cyber agencies will inform of the breach, but **NOT** able to assist

ONTARIO CANADA
ST. MARYS

EXTERNAL ASSISTANCE - RECOMMENDATION

- Create a cyber response plan
- Know who your technical and legal supports are and how to contact them in an emergency

ONTARIO CANADA
ST. MARYS

INTERNAL SUPPORT

- **IT Team**
  - High stress levels
  - Expectation of being blamed
  - Extremely high level of extended hours required over long period of time

ONTARIO CANADA
ST. MARYS

INTERNAL SUPPORT

- **Senior Staff**
  - High stress levels
  - Feelings of helplessness
- **General Staff**
  - Frustration as work cannot be performed

ONTARIO CANADA
ST. MARYS

INTERNAL SUPPORT - RECOMMENDATION

- **What Can Council and Senior Staff Do?**
  - Be good leaders
  - Support your teams
  - Communicate
  - Do not lay blame
  - Let the experts perform their work

ONTARIO CANADA
ST. MARYS

COMMUNICATIONS

- **Work quickly to control the message**
  - Media outlet from the US called with interview request minutes before putting out a media release
  - Establish key message quickly and distribute through channels early to maintain control of information

ONTARIO CANADA
ST. MARYS

COMMUNICATIONS

- **Prep your spokesperson**
  - Most media calls ever received
  - List of key messages prepared for spokesperson during interviews
  - If time allows, debrief after each interview to determine areas of improvement

ONTARIO CANADA
ST. MARYS

COMMUNICATIONS

- **Stick to the facts**
  - “In the absence of evidence, the imagination soars.”
  - Provide as much information as possible without speculating
  - Draft an FAQ document that is available to all staff and public

ONTARIO CANADA
ST. MARYS

COMMUNICATIONS

- **Empower your people**
  - Equip front-line staff with information for basic questions
  - Designate one trusted person to handle in-depth or difficult questions
  - Ensure consistency in information

ONTARIO CANADA
ST. MARYS

In Summary

- **Invest in Being Prepared**
  - Cyber Security best practices
  - Data management and governance
  - Incident response
  - Staff Training
- **Support your Staff**
- **Be ready to receive a lot of Attention**

ONTARIO CANADA
ST. MARYS

Panel Roundtable Question:

Where should a municipality start to prepare for a cyber incident?

LAS

AMO
Business
Services

Who am I?

- **Shannon Devane, Program Manager – Municipal Risk Management**

- New role at LAS - June 2022
- Risk Manager, City of Vaughan 2017-2022
- VP, Risk Management – JLT Canada (now Marsh)
- Director of Risk – OMEX – 2010-2015
- Previous roles at OMEX and other municipalities

LAS

Cyber Insurance Market

Fewer insurers willing to take on municipal risk

Higher premiums

Higher deductibles/self insured retentions

Stringent underwriting

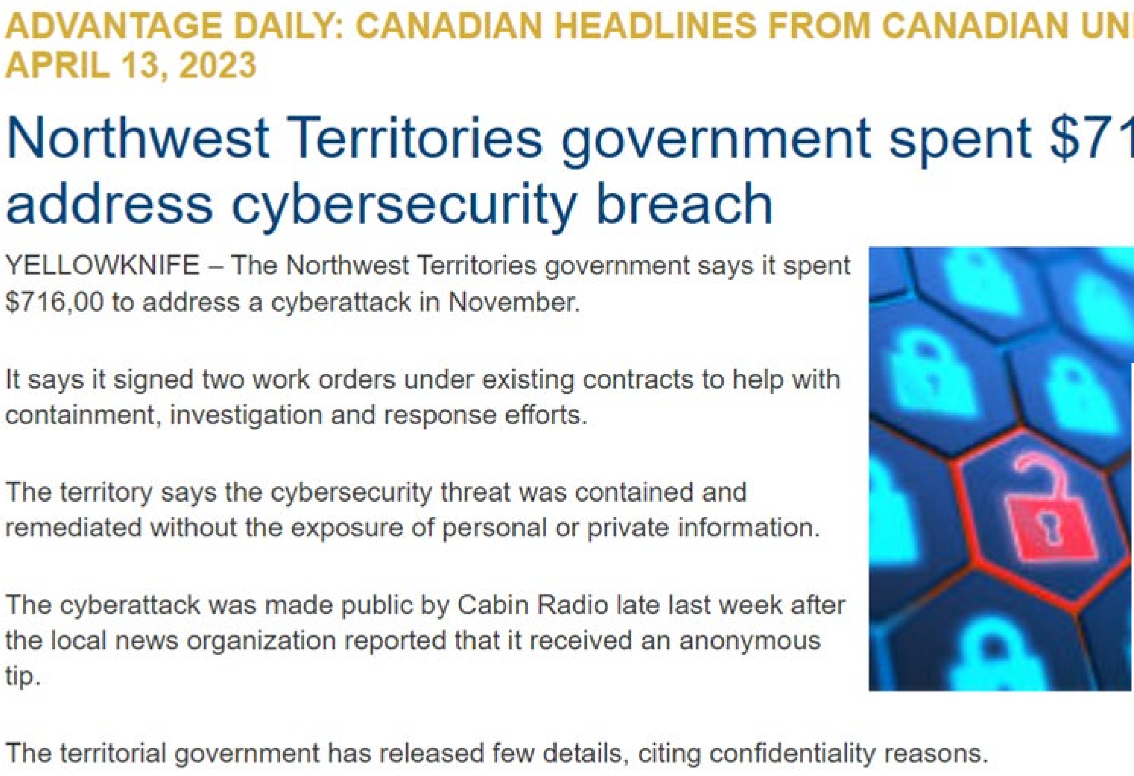
11%

of cyber attacks in Canada last year targeted the public sector

Source: PwC threat intelligence sources

LAS

In the News



ADVANTAGE DAILY: CANADIAN HEADLINES FROM CANADIAN UNDERWRITER - APRIL 13, 2023

Northwest Territories government spent $716,000 to address cybersecurity breach

YELLOWKNIFE – The Northwest Territories government says it spent $716,00 to address a cyberattack in November.

It says it signed two work orders under existing contracts to help with containment, investigation and response efforts.

The territory says the cybersecurity threat was contained and remediated without the exposure of personal or private information.

The cyberattack was made public by Cabin Radio late last week after the local news organization reported that it received an anonymous tip.

The territorial government has released few details, citing confidentiality reasons.

CONSUMER

Cyberattack prompts closure of Gateway Casinos locations in Ontario

By Jacquelyn LeBel • Global News
Posted April 18, 2023 11:49 am · Updated April 18, 2023 2:13 pm

SECURITY

Ontario school board trying to recover from cyber incident

HOWARD SOLOMON

NOVEMBER 29, 2022

LAS

RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lost.
Time Left
02:23:59:06

NEW PROGRAM ANNOUNCEMENT

Cyber Incident Management for Ontario Municipalities - CIMOM

Development of the Program

- Financial recovery is one main component of a cyber insurance policy - Assistance in the event of a breach is the other critical piece.

- If a municipality cannot procure cyber insurance, how will that impact their Incident Response Plan? Who will they contact?

- The concept of CIMOM was born and an RFP was issued in summer 2022.

The RFP

- Eight (8) responses received

- Consensus evaluation -

  Three (3) LAS staff

  Three (3) Municipal experts in IT, Risk and Legal

LAS

The Successful Proponent

ISA CYBERSECURITY

- ISA Cyber Security Inc.
- Canadian Company with over 31 years experience

LAS

The Program

3 Retainer Hour Tiers

Level 1 = 20 hours

Level 2 = 50 hours

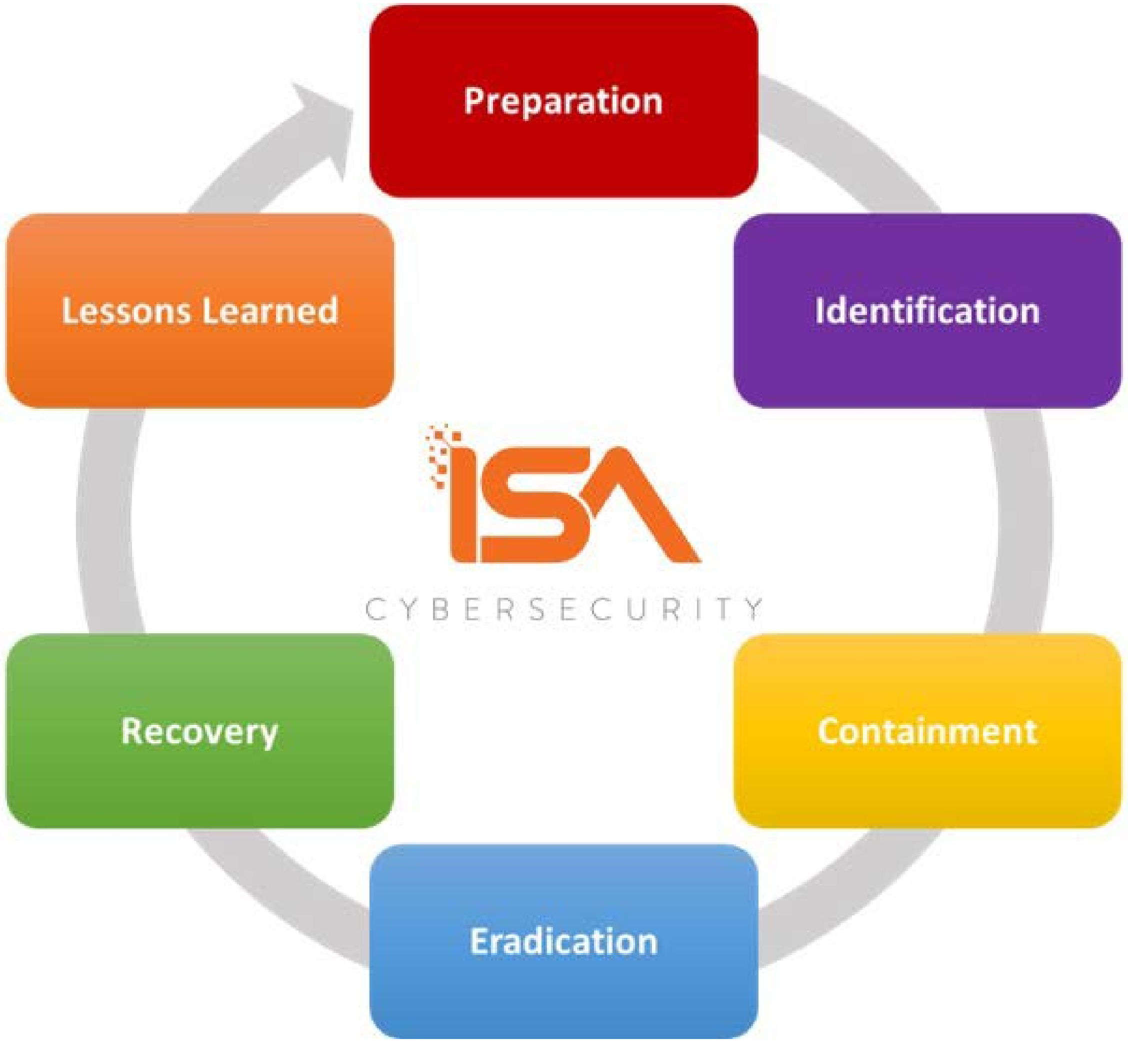
Level 3 = 80 hours

60% of hours can be used in Year 1 for additional incident response work

100% of unused hours from Year 1 can be used for additional incident response work upon renewal

LAS

The Program



LAS

The Program – Adhoc Hours

The program also allows for municipalities to buy hours for cyber incident response related work

The opportunity for block purchasing has been negotiated

Focus is on those municipalities currently without insurance in this initial rollout phase

LAS

LAS and Municipal Risk Management

Working Groups

Municipal Risk Management Working Group

Technical Working Group

Cyber Risk Financing Feasibility Study

Led by Technical Working Group

Board approved next steps in creating a Protective Association at the May 2023 Board Meeting

LAS