Municipal Cybersecurity Best Practices

Supporting Canadian Municipal Resilience

TECHNATION CA

About

TECHNATION

TECHNATION is the industry-government nexus for technology prosperity. As a member-driven not-for-profit, TECHNATION unites Canada's technology sector, governments, and communities for Canada's future. TECHNATION champions technology prosperity by providing advocacy, professional development, and networking opportunities across industry and governments at all levels; connecting Canadian scale-ups with global tech leaders; engaging the global supply chain; and filling the technology talent pipeline.

TECHNATION has served as the authoritative national voice of the $210 billion ICT industry for over 60 years. More than 43,200 Canadian ICT firms create and supply goods and services that contribute to a more productive, competitive, and innovative society. The ICT sector generates more than 666,500 jobs and invests $7.5 billion annually in R&D, more than any other private sector performer.

www.technationcanada.ca

TECHNATION Future Workforce Development

Canada's prosperity relies on a digital workforce with the skills to keep our companies and our country competitive in a constantly changing global market. TECHNATION develops digital talent from both inside and outside the industry through a mix of up-skilling and re-skilling programs. As a strategic arm of TECHNATION, Future Workforce Development focuses on creating the workforce that Canada needs for leadership in the digital economy. This includes inspiring young people to pursue technology careers; advising on technical education requirements and learning outcomes; guiding those in non-technical fields or underrepresented groups to attain needed skills to transition into technology careers; supporting increased diversity within the industry; and helping shape public policy to support, expand, and enhance Canada's tech workforce.

Acknowledgements

Cybersecurity Industry Professionals

TECHNATION wishes to express its sincere appreciation to the cybersecurity professionals and stakeholders who directly or indirectly contributed to this best practices document through interviews, consultations and informal discussions. While too numerous to individually mention, we sincerely appreciate the interest and expertise that the engaged members of the cybersecurity community have provided throughout this project. Their insights and perspectives were essential to the outcomes. We thank them for sharing their time, knowledge, research, and experiences with us. We also look forward to their future contributions in the review process to keep the Municipal Best Practices Guide current and relevant. Please see Appendix A for a full list of industry participants.

Municipal Leaders, Staff, and Municipal Associations

TECHNATION would also like to thank the attendees of our Municipal Cybersecurity Best Practices events for their participation and engagement with these events. Their feedback was crucial in shaping the content of this document. We would particularly like to thank the Municipality of Stratford, the Association of Municipalities of Ontario (AMO), the Canadian Association of Municipal Administrators (CAMA-ACAM), the Federation of Canadian Municipalities (FCM), and Municipal Information Systems Administrators Canada (MISA/ASIM) for their support in communicating the importance of cybersecurity to municipal leaders across Canada.

Government of Canada

This project is funded in part by Public Safety Canada under its Cyber Security Cooperation Program. The opinions and interpretations in this publication are those of the author and do not necessarily reflect those of the Government of Canada.

Canada

Municipal Cybersecurity Best Practice Guidelines

In recent years, municipal governments have faced increasing threats from cybercrime.

Unfortunately, small and medium municipalities are most likely to face cyber threat activity as a result of cybercrime. Municipalities may be targeted for information on their residents, access to payment and government services, or through ransomware and other disruptions. These Guidelines are intended to help municipal leaders understand the actions they should be taking in advance of any cyber incident to prepare for the possibility, as well as the steps they can and should take after an incident occurs.

It is not technical in nature, and organizations seeking guidance on appropriate technical measures should reference *Baseline Cyber Security Controls for Small and Medium Organizations* or other publications to determine the appropriate technical measures and cyber controls.

The following is a draft set of best practices developed through a collaborative effort at two TECHNATION events (2020 and 2021) and supported by industry subject matter experts from our industry and government partners at Bennett Jones, CyberNB, Douglas Communications Group, eSentire, the Ontario Provincial Police, RSA, and Tenable.

Pre-Incident Planning

Threat and Risk Assessment

Threat and risk assessment is the primary activity that will help ensure that you wisely invest in cybersecurity, putting money and resources where it can have the greatest effect.

1. **Identify what is critical to your municipality.** Identify critical information, information systems, and operational systems upon which your municipality relies. If the information or system isn't critical, it doesn't mean that it shouldn't be protected, it just means that it should not be your priority to protect.

2. **Identify threats (accidental and deliberate) to your information and information systems for your municipal context.**

   - Participate in industry/sector cybersecurity events.
   - Leverage security vendor information related to your industry.
   - Consider Canadian Cyber Threat Exchange membership.
   - Regularly check in on government cybersecurity websites and alerts such as the Canadian Centre for Cyber Security Alerts and Advisories or the Canadian Anti-Fraud Centre.

3. **Identify the risks that the cyber threats pose to your critical information, information systems, and operational systems.** This will allow you to prioritize your risks and guide you to where you should invest your funding and resources available.

4. **Get help**. If you don't have the expertise or resources, consult with cybersecurity managed services or other third-party services to help.

Planning and Governance

1. **Optimize awareness & training**. There are a variety of training and awareness activities that you can do within your organization that will help your leadership and employees to prevent and be better prepared for cybersecurity incidents. This includes online awareness courses, phishing exercises, security policy training, and specific role-based training (e.g. incident handling or business continuity training).

2. **Develop critical cybersecurity policies & protocols**. Merely having a policy does not ensure that appropriate activities are in place; you need protocols that ensure compliance to the protocols. All employees should be familiar with the policies and capable of following the protocols for which they are responsible. You should have an overarching security policy with organizational responsibilities and specific policies or protocols for key cybersecurity requirements such as access controls, patch management, and incident response.

3. **Establish internal alignment on cybersecurity requirements**. A default position in many organizations is that cybersecurity is an 'IT issue'. However, cybersecurity is very much an operational issue for municipalities. Consequently, there should be good internal alignment about municipal priorities and how cybersecurity protects information and systems that support the municipality.

A good way to ensure this is to ensure that both government and technical professionals are 'speaking the same language'. This should also include educating municipal leaders and administrators on cybersecurity as a municipal concern.

4 **Manage third-party risk**. Most small and medium organizations do not have the need for an IT infrastructure. There are several practical and economic advantages to leveraging third-party services including moving to the 'cloud' and using 'security as a service'. A few key things to consider are:

- Vetting suppliers to understand what they offer relative to your cybersecurity needs – ensure you understand your needs and that they are documented.
- Including third-party providers in your cybersecurity planning.
- Understanding third-party risks – those that may hold and those you are asking to help mitigate.
- Establishing clear communications, and ensuring and building trust with the supplier contractual provisions – safeguard info, cyber controls...don't make assumptions. Don't use standard form contracts.
- Any relationship between the provision of third-party services and insurance.

Communications and Readiness Planning

1 **Develop a list of the people who need to be involved in managing a cyber attack.** Make sure that you have their contact information.

This list should include:

- Decision-makers
- Communication Teams
- Legal Teams (and possibly outside cyber insurance provider)
- Technical Experts
- Vendor Management
- Vendor Relationship Managers

2 **Hold a planning exercise for best-case and worst-case scenarios.**

- Identify stakeholders who could be affected
- Assess processes and transactions to determine which are most critical and develop procedures to perform them manually. If possible, train staff on these manual processes.
- Determine which vendors will have to be engaged.

3 **If practical, identify a single person who will manage crisis communications.** This person will be responsible for making sure that everyone in your municipality is able to deliver a consistent message to stakeholders.

4 **Determine when frontline managers should escalate issues.**

- Is there or is there likely to be damage to health or property?
- Is there evidence of a criminal act or other wrongdoing?
- Is there considerable public interest?
- Is the issue affecting a mission-critical part of our operation?
- Have errors or mistakes in organizational response occurred?

5 **Define a protocol to determine who needs to be informed of issues and when.**

- Remember that your computers may be inaccessible in a worst-case scenario. Ensure that all contact information is kept in hard copy. Include multiple means of contact for each person on the list: landlines, cell phones, email that doesn't rely on municipal infrastructure, and any other contact points such as a cottage phone.
- Establish a physical location for the team to meet in person during a crisis.
- Determine what kinds of external professional help may be needed.
- Include senior political leaders, law enforcement, and provincial staff such as privacy commissioner in the list.
- Plan messaging for internal stakeholders. Internal stakeholders will be asked questions regarding any cyber breach and should be able to respond to the concerns of constituents.

6 **Perform a stakeholder analysis.** Remember that your stakeholders will talk to one another, so ensure that the information you provide is consistent. For each major audience, identify and define:

- The primary relationship manager.
- What you want that stakeholder to do.
- The primary messages you will communicate to that stakeholder.
- Your communications tools, channels, and rollout.

Incident Management

1. **Have a plan**. Refer back to your threat and risk assessments, know where your critical information resides, and establish values relative to the information that will help you gauge the level and urgency of your response. There are numerous online resources and the *Canadian Centre for Cyber Security Baseline Security Controls for Small and Medium Organizations* is a good place to start, as are other cybersecurity resources aimed at organizations of comparable size.
2. **Create a playbook**. The playbook supports the plan and identifies your organizational incident management processes, key roles and responsibilities. This includes contact lists, third party arrangements and responsibilities, and guidance on reporting and record management during an incident.
3. **Exercise the plan**. You'll never know if the plan will work unless you test it out. You should do this regularly. One good way to exercise the plan is through tabletop exercises—this is a powerful way to manage and practice with applicable scenarios with those in your organization who have responsibilities during incident response.
4. **Improve the plan**. Your organization evolves and so do the threats. Regularly review, exercise and take actions to improve the plan so that your organization is prepared to respond quickly to a cyber security incident.

Communications

It is vital that the news of the breach reach key stakeholders from you and not through a leak. It is equally important that you not say more than is necessary or make statements in a way that may inflame the situation.

1. **Quickly develop holding statements.** These statements provide a response that municipal spokespeople and staff can provide to the public, press, and other stakeholders while the breach is being investigated and you are determining what action to take. These statements will provide you with time to determine next steps.

SAMPLE HOLDING STATEMENT:

"We are currently investigating a potential cyber incident that has affected our municipal systems. At this time, there is no evidence that any personally identifiable data has been accessed, although investigations are continuing. We have locked down all affected systems to prevent any further incidents and are working with our information technology partners to resolve the incident. We have notified law enforcement officials and will fully cooperate with their investigation."

2. **Do not speculate**. Do not say more than you know or provide false assurances—it's OK to say that the incident is still under analysis. These statements must not contain incorrect assumptions that can damage credibility later. Legal teams and law enforcement should be consulted as these statements are developed to ensure that you are not increasing your legal exposure or providing information helpful to criminals.

3. **Ensure that you describe the incident with precise language.** Consult with your experts as to the proper language to describe the incident. For example, you should not describe the incident as a data breach unless you have confirmed that there has been unauthorized access to or loss of data. This will help you avoid providing incorrect information or making statements that may be used against you at a later date.

4. **Maintain an ongoing dialogue with stakeholders.** Whenever possible, reach out to them rather than waiting for them to contact you—it will increase your credibility and help make them confident that you are responding appropriately.

   Internal communications should occur first, wherever possible. This:

   - Allows leaders to lead.
   - Builds employee confidence.

5. **Arm your employees with responses to typical questions so that they know how to respond to stakeholder concerns.**

6. **Consistent messaging creates allies.** Your stakeholders want you to succeed in containing the attack and protecting your municipality.

Legal Issues and Risk

Be aware that your exposure from any incident will include potential exposure to regulatory action or litigation. In addition to your exposure from the incident itself, you may face additional exposure from how you handle your response. Having legal counsel in place is advised to mitigate your risk.

Legal counsel may assist with:

- Management of the breach response.
- Preservation of evidence.
- Advice on legal implications of your response, including communication strategy, reporting, notification, and litigation risk.
- Identification of affected third parties.

Preservation of Privilege

It is important to ensure that certain categories of forensic work remain legally privileged to avoid litigation risk.

- Communication regarding the source of the attack and remediation actions is unlikely to be covered by legal privilege.
- Forensic analysis regarding the scope of potential compromise, or areas of defense that could be strengthened, may be protected.
- Communications with third parties will only remain privileged as long as both parties share a common interest. Privilege will be lost if there is likely to be legal action between the parties, or if any statements are made that indicate that blame is being assigned (e.g. to a vendor).

Reporting and Notification Obligations

In general, if any personal data may have been affected, a report to the privacy commissioner and notification to affected individuals must be made as soon as it is practical.

Other notifications may be required by law or advisable to mitigate risk. This may include notification for affected employees, financial organizations (particularly if banking or credit card information may have been compromised), and police.

Working with Law Enforcement

1. **Safety is priority number one.** If there is a risk to people's safety, taking steps to protect or warn those people must come first.

2. **If safety is not a concern or has been managed, act to protect your systems and data.**

    - Isolate infected systems or even the entire network from the internet and third party connections if practical.
    - If unauthorized access is ongoing, it may be helpful to monitor that activity to collect evidence towards motives, techniques, and attribution.

3. **If the originating system can be identified, a RAM capture or suspension of an affected VM service will assist in analysis and investigation.**

4. **Wherever possible preserve digital evidence, including:**

    - Log files
    - Screen Captures of any messages or unusual activity
    - Suspicious and malicious files and processes (Sysinternals)
    - Unknown or newly created user accounts
    - Activity through suspicious IPs
    - Ransom notes
    - Monikers/Email addresses
    - Tor site addresses
    - BTC Wallet IDs
    - Any communications with the threat actor

Reporting Cybercrimes to Police

If you have reason to believe that a crime has been committed, report the incident to police as soon as possible. Bringing police into the situation during the investigation will allow them to help you take the appropriate steps to protect your constituents and investigate the crime.

Many cybercrimes go unreported, because victims are concerned that the incident will become public or that police will hinder the response to the attack. This attitude increases the risk of cyberattack as criminals believe that they can avoid any risk of prosecution for their actions.

Examples of cybercrime include:

- Unauthorized access to systems, such as data breaches, hacking, data theft, and taking over of email and social media accounts.
- Mischief to Data, including alteration, deletion, or otherwise rendering it useless.
- Attacking web services, via Denial of Service (DDoS) attacks, web page defacement, SQL injections, cross site scripting, cross-site request forgery, and other methods.
- Use of malware.

During the Investigation

Law enforcement will work along IT admins and third-party security companies to identify the attackers and collect digital evidence.

Investigators will need to speak to your staff to gather information about the incident and collect digital evidence. They will understand that a response may be ongoing and will work with you to avoid negatively affecting that response.

- Expect interviews to take about 1-2 hours per person.
- Questionnaires may be provided to fill out in advance.

As the target, you need to focus on:

- Stopping the attack and preventing further exposure.
- Cleaning systems.
- Installing security measures.
- Getting operations back up and running.
- Communications, both external and internal.

Preservation of Evidence

Preservation of evidence should be guided by the source of intrusion and the extent of compromise.

- Understanding the source of the intrusion is necessary to enable you to close the gap in security.
- Understanding the extent of the compromise will determine what reporting and notification obligations you may have and allow counsel to advise you on risk reduction strategy.

IT teams may accidentally destroy evidence in efforts to contain the breach and remove the intruder. Legal or police advice can be critical in managing the breach response in such a way as to preserve evidence that may one needed to determine the extent of the breach and to support future prosecution.

Conclusion

Unfortunately, no set of best practices or cybersecurity measures will make your municipality immune to potential attack. However, ensuring that your municipality makes the effort to put appropriate controls in place, and develops a plan to respond if and when an attack occurs, lowers the chance that you will be attacked and may reduce the severity of any cyber incident.

Appendix A

Content Contributors

Ruth Promislow, Bennett Jones LLP

Bob Gordon, CCTX

Randy Purse, CD, PhD, CTDP

Ashley Lukeeram, CISSP, CEH, CRISC, Tenable

Tyson Johnson, CyberNB

John Douglas, Douglas Communications Group

Eldon Sprickerhoff, eSentire Inc.

Imran Bashir, KPMG

Paul Sammut, KPMG

John Weigelt, Microsoft

DS Vern Crowley, OPP

Ben Smith, RSA

And a special thanks to the Industry Cybersecurity Advisory Group for their contributions.

TECHNATION^CA

Funded in part by the Government of Canada

Canada