A Municipal Cyber Security Toolkit

Best Practices to Guide and Improve Cyber Security Readiness

SEPTEMBER 2020

Executive Summary

At the 2019 AMO Conference in Ottawa, cybercrime and municipal cyber security emerged as key topics with delegates. The experiences of several AMO members effected by cyberattacks made it clear that in this age of ever-expanding use of digital technology and systems connectivity, municipal governments are prime targets for cyber criminals. The message received at the Conference was clear: how can AMO assist the membership in addressing potential cyber threats?

To that end, AMO reconstituted its Digital Government Task Force to explore opportunities in municipal cyber security. With the technical implications associated with municipal IT infrastructure and systems, membership on the reconstituted Task Force included several Directors, Managers and Leads of IT, including several representing municipalities that experienced a cyberattack. These members provided invaluable advice to the Task Force as recommendations and a path forward was developed for AMO on municipal cyber security.

The Task Force met four times in late 2019 and early 2020. Delegations were received from police services, insurance, cyber security specialists, the Province of Ontario, MPAC, municipal auditors, and media relations to discuss municipal interests in cyber security.

The culmination of the work of the Task Force is this Municipal Cyber Security Toolkit that highlights key considerations brought forward by delegations, provides advice and critical information for members to consider when thinking about municipal cyber security, as well as recommendations on how AMO and LAS can assist the membership in addressing potential cyberattacks.

AMO's Digital Government Task Force consists of elected officials and municipal staff with expertise in municipal IT systems, government services, reporting, and digital initiatives. Chief Information and Technology Officers, CAOs, Clerks, directors and managers in information and technology systems, business planners, risk managers, and legal staff participated at Task Force meetings.

Cathy Downer, Councillor, City of Guelph and Robert Foster, Councillor, Region of Niagara, co-chaired AMO's Digital Government Task Force during its meetings on municipal cyber security.

Contents

Background

Cyber security is how individuals and organizations work collaboratively to reduce the risk of a cyberattack. The core function of cyber security is to protect devices and technology we use (smartphones, laptops, tablets, computers, complex IT systems, etc.), and the services we access online from theft or damage. It is also about preventing unauthorized access to the vast amounts of personal information and data that we store on these devices, and online.

Cyber security is important because the technology we use daily is critical for how individuals, families, governments, and businesses interact with the world. From banking to shopping to the operation of a municipal government, it is vital that both council members and municipal staff take appropriate steps that can prevent cyber criminals accessing accounts, data, and devices. With cyber criminals becoming savvier with their methods, it is not a matter of if a municipality will experience a cyberattack, it is a matter of when.

In 2018 and 2019, several municipal governments in Ontario experienced data breaches resulting from cyberattacks. As delegates at the 2019 AMO Conference learned, cyber criminals do not distinguish their targets and no municipality – whether urban, rural, small urban, northern – is immune from a potential attack. Small, rural, and northern municipalities face the same cyber security threats as their larger urban counterparts but with fewer resources and capacity to confidently address a potential attack. Smaller municipalities are targeted as low hanging fruit because they are often underfunded, underprepared, and do not have the capacity internally to implement effective cyber security measures. Residents rely upon accessing municipal programs and services daily, as such municipalities are more willing to pay ransom to regain access to data to maintain local operations and service delivery.

Why are municipalities targets? Municipalities possess and maintain large amounts of sensitive data connected to both personal information of their residents (property tax information) and the infrastructure that they operate (traffic cameras, water systems, etc.). This data held by municipal governments is considered valuable to cyber criminals. Many municipalities are also connected to an upper tier municipality where the data cache is even larger. As a result, as municipalities become more high-tech, using internet-connected systems, and offering more municipal services online, they increase their vulnerability to a cyberattack. As seen with the recent attacks on the City of Stratford, Town of Wasaga Beach and others, administration, operations, and service delivery can be crippled if municipalities cannot access their data and systems.

Planning a cyber security strategy is a good first step towards hardening municipal systems from cyber criminals. There is no one size fits all approach to prevent a cyberattack, and there are strategies of varying costs to manage cyber security risks. Council members and municipal staff should note that cyber security is always evolving to address new risks and there is no one simple fix.

Effective cyber security measures are built around a combination of technology measures to protect systems, but even more importantly around education and training. The weakest point to your systems is often human error or misjudgment and it is vital to appropriately educate and train council members and staff periodically about recognizing a potential cyber threat/crime before it happens. As with most risk management practices, it is better to be proactive than reactive when it comes to the cyber security of municipal governments.

Cyber security is a shared responsibility across a municipality. It is not limited to the sphere of IT staff but requires buy-in from all council members and municipal staff for it to succeed. Councils are the custodians of the data within a municipality and they need to ensure that the sensitivity and security of that data is maintained. It is important to know the threats that exist and the potential impact (cost, reputational and political consequences, etc.) to your municipality. Cyber security must become a priority of municipal governments as managing the risk of a potential cyberattack helps preserve public trust and minimizes financial consequences. That is why it is vital that council members and senior municipal staff champion robust cyber security measures within their municipalities.

This paper is designed as a toolkit to help build the knowledge of council members and senior municipal staff on cyber security as well as help municipalities manage the risk of a potential attack.[1]

Municipal Policies and Procedures

Cybercriminals exploit human and technical weaknesses. To manage those risks, municipal governments should consider developing written cyber security policies and procedures for council members and staff to follow. All cyber security policies should be shared with everyone with access to municipal systems, devices, and networks to ensure that they are adopted and followed. Developing an effective cyber security policy requires proactive planning by all municipal departments, identifying risks, explaining roles and responsibilities. Documented policies provide the foundation for effective governance of any cyber security program and provide clear guidelines and processes.

To protect municipal networks and systems, it is important to establish and enforce data security policies and procedures that address acceptable use of:

- Email
- File sharing
- Internet
- Laptops
- Remote access
- Social media
- Personal mobile devices used for work

Another way municipal government can improve cyber security is by having an access management policy, granting access to confidential data and critical IT systems only to those employees who need it as necessary to fulfill their job responsibilities. This allows you to classify your data, know where it is (both internally and externally), and protects your vital data by limiting access to it.

[1] A special thanks to the New Hampshire Municipal Association for the report by Lisa N. Thompson "Cybersecurity Best Practices for Municipalities" that is included throughout this report.

It is important to keep in mind that as technology and cyberthreats change, security policies and training should be updated on an annual basis. Also, municipal governments should periodically review their policies to ensure compliance with all applicable laws and regulations.

Cyber Security Assessment

Key to improving a municipality's cyber security is recognizing vulnerability. Most local governments do not have a complete picture of the security gaps in their systems and networks. To develop a cyber security program, municipalities must first conduct a comprehensive risk assessment across all departments, identifying potential risks, exposures, and areas for improvement. If a municipality cannot identify its cyber vulnerabilities it cannot expect to effectively defend against them. The risk assessment should identify the categories of risk that apply to the municipalities' people, processes, systems, and vendors.

Once the risk assessment is finalized and potential vulnerabilities are identified, municipalities can create actionable and appropriate solutions to address weaknesses in their system and direct resources to bolster security. Municipal governments should use their assessment as a focal point to bring together stakeholders and partners to develop a comprehensive cyber security strategy. For any cyber security initiative to be effective it must be integrated throughout all departments of an organization.

Incident Response Planning/Data Breach Protocol

Municipalities should approach cyber security policies and procedures as an expansion to emergency preparedness. A common refrain in the cyber security industry is "it's not if, but when" a cyberattack will occur. Just as municipal governments routinely prepare plans for the continuity of operations in the event of a natural disaster, they must also prepare plans to restore critical computer systems and networks as quickly as possible in the event of a cyberattack.

The time to develop an incident response plan is not in the wake of a cyberattack. Prior to a cyberattack, municipal governments must proactively develop a comprehensive written incident response plan. Only with a documented incident response plan can consistent action and mitigation measures be taken. An incident response plan is a set of procedures designed to identify, investigate, and respond to a cyberattack in a way that reduces the impact and allows the municipality to return to normal operations as quickly and efficiently as possible. An effective incident response plan should include a step-by-step plan to determine the nature and extent of the incident, specifying the actions to be taken, and identifying the roles of key employees, vendors, and other stakeholders for each step in the plan.

Every municipal government relies on critical services and communication systems, that would significantly impact its ability to function if compromised. Communication is crucial during any disaster or emergency, including a cyberattack. In the event of a cyberattack that knocks out municipal servers, electronic communications such as email, instant messaging, and texting may be shut down, potentially impacting the delivery of critical public safety services such as emergency medical personnel, fire and police, which rely on access to computer systems and networks to communicate. Municipal governments need to be prepared to communicate using different forms of communication during a cyberattack. It is critical that, as part of their incident response planning,

municipal governments include procedures on how the organization will communicate and coordinate after a cyberattack, including:

- How to contact council and staff e.g. through Gmail or similar web-based email accounts – this may include designing a policy to permit external email accounts for the purposes of maintaining work during the event of an attack
- How to connect with the Government of Ontario where provincial systems are linked
- How to inform residents which services may be impacted
- How to contact third parties that work with municipal governments e.g. MPAC, vendors, etc.

Other areas within incident response planning in the event of a cyberattack that may require policy changes include:

- Procurement – to allow for cryptocurrency procurement and engagement with dark web consultants without going through a full RFP process
- Business Continuity Plans – including but not limited to paying staff, issuing building permits, issuing marriage licenses, ensuring field work complete, etc.

Municipal IT Policies and Procedures

IT Infrastructure Asset Management

Within municipal governments, your IT infrastructure is just as critical as many of the hard infrastructure services that you deliver such as roads and bridges. Your IT systems are needed by your employees in the workspace to deliver local services effectively and efficiently, as well as allow residents to interact with their municipality to access those services in a timely manner. Protecting those assets is essential.

Municipal governments that do not assess their security weaknesses on a regular basis are most vulnerable. Often hardware, network equipment, software, and wi-fi access points are soft spots. At a minimum, a cyber security assessment should identify the types of sensitive information that each department collects, where it is maintained, and who has access to that information within the organization. The assessment should also entail conducting an inventory of all hardware and software components to determine the types of hardware and software the organization is currently using and identifying any risks to data and existing hardware and software. In addition, before committing to new hardware, software or e-government program, municipal governments should ensure that all cyber security issues have been considered before implementation. Municipalities should also understand what third-party organizations, such as short-term consultants or IT trouble-shooters, potentially have access to that information to protect internal IT infrastructure and systems.

Password Management Policy

Passwords to accounts are high value targets for cyber criminals. One of the most important steps a municipality can take to prevent a data breach is to establish and enforce a password management policy for council members and staff. For each account, computer, mobile device, or wireless network, passwords should be unique, hard to guess, and should have a minimum of 10 characters,

containing a mix of upper and lower case letters, numbers, and symbols. The same or similar passwords should never be used for different accounts or applications and sharing of passwords should be prohibited. In addition, it is essential that that all personal mobile devices that access municipal networks and systems be password protected. For added security, passwords should be changed regularly (e.g. every 60-90 days) and never repeated.

Also, imposing strict session timeouts so that if a user leaves an account or application unattended for an extended period of time while logged in, the session will automatically time out and log the user off, requiring the user to reenter their password to log back on. All municipal government computers and systems should have a lockout feature, which after a certain number of successive attempts of entering the incorrect password the user is automatically locked out.

Multi-Factor Authentication

Since passwords are easy for cyber criminals to crack, a password alone is not enough to protect municipal networks and systems from being breached. Implementing multi-factor authentication is a simple way to keep municipal networks secure. Multi-factor authentication is a security enhancement that requires a user to supply additional information besides a username and password before being allowed to login to an account or gain access to a network or system. Even if a password is cracked or stolen, access is thwarted because of multi-factor authentication. For the authentication to be complete, a user must enter their login/password and then when prompted provide a passcode or security code, usually a temporary code sent by email or text to gain access. Multi-factor authentication is highly recommended whenever employees request remote access to municipal networks and systems. While many apps and programs such as Office 365 already support multi-factor authentication, it is important not to overlook other critical software programs that are used by various departments. Municipal governments can install multi-factor authentication apps or hire a third-party vendor that offer cloud-based multi-factor authentication services.

Encryption

Municipal governments are tasked with safeguarding sensitive government data and personal information. Many council members and staff routinely use laptops, USB drives and mobile devices to store and transmit sensitive data through e-mail, instant messaging, and other forms of digital communication. Lost or stolen laptops, USB drives and mobile devices that contain unencrypted data are a main cause of data breaches. While a password can prevent someone from logging into a lost or stolen laptop or mobile device, other means can be used to access and copy stored files and data. Encryption safeguards against unauthorized access to confidential data when a laptop, USB drive or mobile device is lost or stolen or when a message is intercepted by a third party. Encryption is a vital security control for municipal governments and should be enabled on all computer systems, USB drives, files stored in the cloud, laptops, and mobile devices. Encryption is where readable text, documents, or other data are converted into unreadable, scrambled code that can only be read by those authorized to access it with a password or security key.

When developing a cyber security strategy, municipal governments should consider encryption to protect sensitive data. Data stored on hard drives, laptops, mobile devices, servers, USB drives and stored in the cloud, known as “data at rest,” can be a vulnerable target for hackers. Municipal governments should consider what is called “full-disk” encryption, which can be used to encrypt data at rest. Full disk encryption protects data if a laptop, USB drive or mobile device is lost or

stolen. Most newer desktop computers, laptops and mobile devices come with operating systems that offer ways to fully encrypt stored data. For example, both Apple and Microsoft offer built-in encryption software which allows for full encryption of an entire drive. Some operating systems have encryption enabled by default and others require users enable encryption on an individual file, directory, or drive basis. In addition, there are third-party cloud-based, hardware and software encryption solutions that can be used throughout an organization on servers, desktop computers, laptops, and mobile devices.

Software Updates

Routinely installing security updates as soon as they are released is an essential component to any cyber security program and can greatly improve a municipality's cyber resilience. Municipal governments that do not regularly install security patches and software updates on all devices, hardware and applications (e.g., antivirus software, browsers, desktop computers, laptops, mobile devices, operating systems, printers, routers, etc.) are vulnerable to attack. For example, a ransomware attack that exposed the City of Atlanta in 2018 was due to the exploitation of a system that had not been updated. It only takes a single computer or device that has not been updated or patched for an entire network to be compromised. Cybercriminals are constantly scanning for security vulnerabilities to exploit so that they can gain access to critical systems that have valuable data. Municipal governments should prioritize raising awareness about importance of installing updates and require all employees that have access to municipal networks and systems to regularly update all personal devices and apps as soon as they are available. In addition, software that is no longer supported with updates and security patches present weaknesses that can be easily exploited and should be disabled or deleted (e.g., Windows XP, Internet Explorer versions 10 and older).

Backup Data

A backup of municipal networks and systems is the best way to avoid data loss and can be invaluable if a catastrophic event such as a ransomware attack, fire, theft, natural disaster, server crash, or user error occurs. Municipalities can protect their networks from ransomware by keeping regular backups of their systems offsite. Regular backups are one of the easiest and least expensive cyber security precautions that a municipality can take to mitigate the risks of an incident involving data loss. A backup is a stored copy of important municipal data and systems, which can be recovered if the original data is lost or corrupted. Municipal governments should ensure that all important data and systems are routinely backed up. Backups should be encrypted so that they are protected from ransomware.

Municipal governments should also maintain their backup at a secure off-site location and make sure to backup all data that is stored in the cloud as well. Also, just as important as the backup itself, is the periodic testing of backups to ensure that data can be restored. Backup systems can be stored on-premises using an external hard-drive or flash drive, or off-site using a cloud provider. Having one back-up copy is not sufficient – to be safe it is advised to enable two backup options with at least one copy off-site or on a different server in case of an on-premise disaster or outage. It is important to note that while most municipal governments regularly back up their systems, employees are less likely to back up their local drives or mobile devices. To prevent the loss of data in the event of a cyberattack, municipal governments should require employees that use mobile devices such as smartphones, tablets, and laptops to routinely perform full backups of data and program files.

Municipal Communications

Municipalities must be prepared to have an effective communications strategy should they be faced with a cyberattack. Coordinating a response with consistent messaging is both helpful internally and when addressing the public. In addition to having a contingency and business continuity plan in place, a municipality's communications should also have plans in place to respond to a cyberattack. Should your municipality choose to role play/simulate a cyberattack, your communications team should be brought in as part of that exercise as they will have to manage public messaging during the attack.

A quick communications assessment of potential issues that may emerge from a cyberattack will help the municipality when communicating with the public, especially at the early stage of the attack:

- How can we communicate trust/credibility to the public in the wake of the attack?
- What are the costs?
- Is there a safety issue?
- How are we showing that we are doing our due diligence?
- How can we emphasize transparency, especially if key data may have been breached?
- Is there a plan in place to communicate next steps to the public?

Best practices in terms of key principles, objectives, strategic approaches, and internal and external tactics when managing a cyberattack from a public communications perspective include the following:

Key Principles

- Acknowledge and communicate quickly – providing basic, accurate information
- Focus on what you know and be open about what you do not know
- Anticipate public needs and concerns
- Set reasonable expectations
- Identify best sources for information and assistance
- Leaders make promises the organization can meet, or beat
- Simple, plain language that can ripple through the community

Objectives

- Maintain confidence in the municipality: responsible, trusted organization equipped to deal with threats to cyber security now and in the future
- Reassure residents that essential local services are still operating as usual (or that back-up plans are rolling out as expected)
- Balance the need to share timely information publicly with ongoing legal and other considerations until the security issue is resolved

Strategic Approach

- Ensure clear and consistent communications through all internal and external communications channels
- Use existing media networks and the website to provide timely, accurate and appropriate information

Internal Tactics (Council and Staff)

- Basic customer service message for public and customer service facing staff, e.g. the Clerk's office
- Email updates and face-to-face staff communications as needed

External Tactics (Public and Media)

- Customer service: special phone line set up and messaging/Q&A provided
- Media relations protocol: designated spokesperson conducting interviews as needed
- Media materials: media updates issues daily
- Website: update as needed
- Social media posts: regular updates as needed

Having a communications plan in place before a cyber incident occurs will help your municipality navigate the attack better.

Digital Initiatives

More than ever, municipalities are harnessing the power of technology to help them digitally transform internal operations and service delivery so they can work better. When implementing various digital initiatives, proper security protocols should be observed to protect both IT and the privacy of residents. During procurement, in the RFP process, municipalities should build in strong requirements for vendors to prove how they will secure data from potential cyber threats.

Many municipalities often outsource functions and rely on third-party service providers and other vendors for a range of services such as credit card processing and payroll services. To combat cyber security threats municipal governments must conduct adequate due diligence and risk management assessments on all third-party vendors that have access to any confidential data and that interact with municipal networks and systems, verifying that they are capable of complying with all relevant data security laws. This can be accomplished by having vendors complete a comprehensive due diligence questionnaire. Municipalities should also require all vendors to provide security documentation. Furthermore, municipalities should impose contractual obligations on vendors, requiring up to date on-time patching of vulnerabilities, prompt reporting of potential cyber incidents, cooperation in investigating an incident and preserving relevant evidence, etc.

As part of ongoing third-party due diligence, municipal governments should evaluate vendors for compliance and risk on an annual basis. To effectively manage vendor risk, municipal governments should consider creating a vendor database to collect and store due diligence information, risk ratings, and monitoring information. The database could also include current and past versions of

contracts as well as exceptions to vendor policies and procedures. By constantly maintaining and updating vendor records, municipalities can further minimize their cyber security risks.

Legal Considerations

Municipalities will also need to prepare and mitigate for potential civil litigation resulting from a cyberattack. Lawsuits are being brought forward across multiple sectors globally for failing to have adequate cyber security systems in place to counter cyberattacks. In short, being unaware of the risks of cyber threats will not protect an organization from both the attack as well as the potential fallout of civil litigation which could further tarnish the brand of your municipality.

Municipalities are required by law to honour security obligations to protect the data that has been impacted by a cyberattack. Under the *Municipal Freedom of Information and Protection of Privacy Act* s.3(1) of Regulation 823, municipalities must ensure that reasonable measures are defined, documented and put into place, taking into account the nature of the records to be protected to prevent unauthorized access to records in their control or custody.

Being proactive to cyber threats and continually implementing cyber security best practices, policies, procedures, and plans may help alleviate the risks of civil litigation.

Audit Considerations

The best time to negotiate the scope of work in event of a cyberattack is before the cyberattack. If a cyberattack occurs, municipalities should specify the scope of work to quantify and prove the extent of damage that occurred because of the incident e.g. what will be the scope of a digital forensic audit? Auditors want to see what organizations have done to recover, how an organization has tightened controls (disclosure), financial impacts (loss of business, lawsuits, etc.) and make provisions when quantifying the loss. An organization should disclose if they have been exposed by a cyber incident but there is no accounting standard that requires reporting.

Annual internal cyber security audits may also ensure that your municipality meets or exceeds cyber security policies and procedures in place, confirms that those policies are being enforced, and identifies potential weaknesses that may exist. The audit would act as an internal checklist to the state of your municipality's readiness in the event of a cyberattack.

Insurance Considerations

As cyberattacks become more sophisticated, despite preparation, education, and training, municipal computers and networks can still be compromised by an unforeseen vulnerability. One way that municipalities can offset some of the risks and limit their exposure is through cyber liability or cyber security insurance. Municipal governments across the country are purchasing cyber insurance policies to cover losses resulting from a cyberattack. It is important to note that cyber insurance is intended to complement, not replace, a municipal cyber security program. Furthermore, cyber insurance will not remove the threat of a cyberattack, but it can help cover the costs arising from a cyberattack, including breach notification, regulatory fines, forensics, legal fees, and other expenses. Not all policies are created equal and will vary, but cyber insurance can also cover the cost of

restoring data affected by a cyberattack and for legal liabilities such as the cost of claims made against the municipality for failing to protect personal data.

Insurance companies that offer cyber insurance often perform evaluations of an organization's security practices and policies to determine whether adequate procedures are in place to mitigate potential cyberattacks. Municipal governments that do not meet certain standards will pay higher premiums for a cyber insurance policy – premiums are higher for municipalities that have not implemented safeguards to protect themselves from a cyberattack.

Specific cyber insurance policy "must haves" include:

- Multimedia liability – social media
- Security and Privacy Liability
- Privacy Notification and Crisis Management
- Extortion/Ransom Coverage
- Business Interruption
- Loss of Electronic Data
- Court Hearing Costs

Cyber insurance policy "nice to haves" include:

- Network and Data Sharing Coverage
- Payment Card Industry (PCI) Fines Coverage
- Coverage for data storage services
- Contingent Business Interruption
- Availability of Social Engineering or Fraudulently Induced Transfer Coverage
- Management Liability
- Consequential Reputational Harm

It is critical that municipalities assess what their cyber insurance policy covers. As with other types of insurance, cyber policies often contain a variety of exclusions buried in the policy that can limit coverage. Common exclusions to be aware of include outdated software, unencrypted data and devices, certain types of social engineering scams, and acts of foreign governments. Furthermore, when selecting an insurance policy, municipal governments should carefully consider whether all contractual conditions of the policy are fulfilled, or the insurer will attempt to rescind coverage or deny claims in the event of a cyber incident.

As cyberattacks continue to evolve, municipal governments should periodically assess their specific exposure to threats to determine whether the amount and scope of their cyber insurance policy is sufficient to cover losses resulting from a cyberattack.

Municipalities should note that there is no standard for cyber insurance. Procurement of cyber insurance should consider the underwriting and, where possible, compare policies between competing firms to ensure it meets your needs. Due diligence is also required when analyzing who is providing the work. As mentioned above, if thresholds are not being met, there will be no payout. AMO Digital Government Task Force Members also sought legal clarification on municipal closed-door meeting provisions under the *Municipal Act* s.239(2)(a) for in-camera discussions regarding the purchase of, or consideration of purchasing, cyber insurance. Aird & Berlis LLP, LAS' Closed Meeting

Investigator Program Partner, confirmed in a presentation at the Rural Ontario Municipal Association (ROMA) Conference in early 2020 that council or committee is entitled to convene in a closed meeting to consider matters related to cyber security as well as cyber security insurance. The discretionary exception in s.239(2)(a) allows for closed meetings related to security of municipal property which includes IT infrastructure and data – cyber security expressly relates to the protection of municipal systems, networks and programs (i.e. municipal property) as well as cyber security insurance, as it is inextricably connected to the same subject matter.

After managing a cyberattack, one Task Force member reported that their council enters in-camera meeting to report on IT. The closed-door session provides an opportunity to report quarterly on the status of their IT infrastructure, as well educate and interact under Committee of the Whole provisions.

Education and Training

Protecting municipal government networks from cyberattacks requires more than technological solutions. When it comes to cyberattacks, one of the biggest risks in any municipality is its own council members and staff. Cybercriminals often specifically target municipal council members and staff with phishing emails designed to get them to release sensitive information or click a malicious link. However, when they receive regular training on cyber security best practices and potential scams, municipal council members and staff can also be the first line of defense. Cyber security strategies that focus on preventing external threats without addressing internal threats are liable to fail. The cornerstone of any comprehensive cyber security strategy is training. A key question that any municipal leader should consider is how will you prepare and educate your council and staff to cyber threats and risks?

Ransomware and other cyber security incidents can be avoided through regular cyber security training, security assessments, and strong security policies. It is critical for municipal governments to implement comprehensive security awareness training and testing for all employees (including council members, staff, and contractors) and anyone who interacts with its networks and systems. Effectively training all municipal council members and staff on cyber security issues is an essential component of any comprehensive cyber security program and should, at a minimum, include educating council members and staff on how to recognize risks and potential cyberthreats such as phishing scams, malware, and ransomware.

Municipal governments should also consider creating training manuals for council members and staff. Regularly educating council members and staff on the risks of downloading attachments from unknown sources, using insecure networks, sharing passwords and social engineering can greatly reduce the threat of a cyberattack. Since cyber threats are constantly evolving, creating a culture of awareness requires ongoing education and training and is not something that can be done just once. Continuing cyber security education should be mandatory for all council members and staff throughout the duration of their employment with the municipality.

A constant theme that was heard from delegations to the Task Force was the importance and need of appropriate, robust, and ongoing cyber security training. Municipalities should be considering or implementing cyber security awareness training for their council and staff. The least expensive approach to effective cyber security is emphasizing education and training processes on people.

Post data breach is more expensive than pre data breach and municipalities should be considering hardening not just their technology and systems but their people as well.

Role of the Government of Ontario

Task Force members discussed what role the Government of Ontario could fulfil in assisting municipal governments with cyber security measures. Further to being a good partner by providing access to information about cyber security resources, education and training forums, answer questions about security protocols where provincial IT systems interact with municipal IT systems, and establish protocols for re-establishing connections after a cyberattack in partnership with municipalities. The Province should also strongly consider fragmentation as a viable cyber defense using a variety of security protocols for the broader public sector and municipalities. Fragmentation across the municipal sector would act as a line of defense as one established security protocol could potentially expose all 444 municipal governments to a malignant actor(s).

There could be a role for the Province on building a vendor of record of effective IT security firms that municipal governments could engage. This would help smaller municipalities procure for cyber security support.

Role of Police Services

Task Force members received delegations from the Ontario Provincial Police's Cybercrime Investigations Team and the Royal Mounted Canadian Police's NC3 branch to discuss law enforcement's role in the field of cyber security, particularly on how municipalities can build awareness of cybercrime among council members and staff and how municipalities should be preparing for and reporting cyber crimes.

The following steps are recommended by police services if your municipality is affected by a cyberattack:

- Report to the police service of jurisdiction e.g. OPP or local police
- What information should be reported?: date, time, and detailed account of the incident; the impact to you and/or your operation (level of jeopardy); systems and type of data affected; log files (application, event, security, system, gateway, firewall, suspicious files, threatening emails, ransom note demand, etc.)
- When to report?: as soon as possible, when there is a level of jeopardy (e.g. been threatened, personal or financial information has been compromised, operations impacted)
- Note: items that you recognize and safely deal with (e.g. phishing emails) do not need to be reported.

Both the OPP and RCMP emphasized the importance of education to fighting cybercrime. In our digital age of pervasive technology and interconnectivity, no one is safe from hackers stealing data and taking over systems. The average dwell time, or time it takes a company to detect a cyber breach, is more than 100 days. Police services recommend educating yourself and others on the preventative measures you can take to protect yourself as an individual, business, or government.

Due to the complex nature of cybercrime investigations, measuring success requires a different approach for police services. The Cyber Investigations Team focuses on building cyber awareness through community engagement and information sharing through participation in working groups and the events led by community, industry, and academic partners in Ontario. They assist individuals, businesses, and governments by providing cybercrime awareness and prevention seminars as well as security education resources. They also provide support and mentoring to frontline members at local OPP detachments and municipal police services across Ontario to enhance the ability to respond to cybercrime calls for service.

More information on cybercrime and law enforcement is available in **Appendix A**.

Role of AMO/LAS

What emerged out of discussions on AMO's Digital Government Task Force was the need for strategic partnerships in the field of municipal cyber security. This work cannot be done alone for many municipalities, particularly small, rural, northern or remote, and there could be opportunities for AMO/LAS to identify service providers to assist members in areas such as conducting annual security audits, leveraging the purchase of cyber insurance, and partnering with the Government on Ontario and others on aspects related to municipal cyber security.

The Task Force recognized that there is no single technological solution to protect municipal IT systems. As such, the Task Force recommended against AMO exploring partnerships with vendors of cyber security technology at this time. Internal preparation (e.g. know your IT systems, their vulnerabilities and address those weaknesses collaboratively with your IT staff/support) with appropriate and frequent education and training for council members and staff were viewed as critical components to reduce the likelihood of a potential cyberattack.

As a first step, the AMO Digital Government Task Force recommended that AMO/LAS begin looking at education and training opportunities that would enable council members and municipal staff to recognize potential cyber threats through a training course or other platform. AMO/LAS will work with others, including our partners at MISA-Ontario[2], to design and develop an appropriate education forum for members.

With the impact of the COVID-19 pandemic and the need to continue business and provide services to residents safely, municipalities are digitally transforming at a faster pace, more so than some originally planned. The reliance on computer systems and on the internet to operate and deliver services to residents during the pandemic makes it even more vital that municipalities have proper cyber security tools in place to limit exposure to a potential attack. AMO will work to deliver education and training opportunities to the membership as appropriate.

[2] Municipal Information Systems Association, Ontario (MISA Ontario) is a non-profit organization whose objective is to foster an engaged and active community of municipal professionals, at all levels, to share information, experiences and promote municipal IT practices. MISA Ontario continues to be an advocate for innovation on behalf of all municipalities, small to large, on issues and topics that impact their communities.

Conclusion

Cyber security is a constantly evolving field, mainly because cyber criminals are becoming sophisticated in their methods unleashing severe attacks. A municipality that is not fully prepared or is not taking the threat of a potential cyberattack seriously are perceived as low hanging fruit by cybercriminals.

Cyber security can be complex, overwhelming, and very difficult to implement for those that are underfunded or unprepared. But it is important for municipalities to consider implementing several of the best practices highlighted in this paper, several of which come with low to no cost. Cyber security and cyber risk management is a shared responsibility within organizations, not just something limited to the sphere of IT. IT departments should not be determining the risk management tolerance of an organization but should have guiding role as part of the process and discussion. Politicians and administration have key roles and cyber risks should be prioritized by council and management i.e. having conversations on cyber security and cyber risk management as an item on the budget agenda. Council must play a leadership role in managing risks and championing effective cyber security measures across the entire municipality. Organizations that implement security protocols that involve cooperation with all departments are better prepared to respond to a potential attack – some municipalities simulate a cyberattack involving all departments to gauge response to an incident.

Most importantly, good cyber security involves a combination of internal preparation with your technology as well as education and training of council members and staff. Furthermore, Councils are custodians of municipal data and it is critical to ensure the protection and security of your sensitive and personalized data before a breach in your systems occur. There are reputational consequences in addition to high costs (damage to systems, paying ransom, work hours lost, etc.) that could happen.

AMO understands that there is no one size fits all approach to cyber security. Where it makes sense for AMO to assist the membership is through creating a robust education and training program geared towards council members and staff. AMO will work with our partners at MISA-Ontario to create a potential course offering/education session.

We would like to thank the AMO Digital Government Task Force membership for their participation and critical input into the development of this report. We would also like to thank the delegations that provided us with enhanced understanding of the multi-faceted, layered, and often complicated area of municipal cyber security.

Delegations to the AMO Digital Government Task Force

Ontario Provincial Police (OPP) Cybercrime Investigations Team – Vern Crowley, Detective Sergeant, Cybercrime Investigations Team Outreach Manager

Royal Canadian Mounted Police (RCMP) National Cybercrime Coordination Unit (NC3) – Jeff Morris, Manager for Strategy and Partnerships

City of London – James McCloskey, Manager III, Network and Information Security, ITS

Frank Cowan Company – Jessica Jaremchuk, Director, Risk Management Services, and Stephanie Resendes, Casualty & Cyber Specialist

Canadian Centre for Cyber Security – Alexandra Underhill, Cyber Security Analyst, Sector Lead, Provinces, Territories and Municipalities in Partnerships

Redbrick Communications – Farah Tayabali, Vice President

BDO – Vivek Gupta, National Leader, BDO Consulting – Cybersecurity

TECHNATION – Randy Purse, Vice President, Future Workforce Development

Municipal Property Assessment Corporation (MPAC) – Carmelo Lipsi, Vice President and Chief Operating Officer, and Sujit Jagdev, Vice President and Chief Information Technology Officer

Appendix A – Police Services and Cyber Crime

What is Cybercrime?

Cybercrime has many varying definitions. The OPP's Cybercrime Investigations Team divides cybercrime into two categories:

1. Where a computer system/network or the data that it stores is the target of the crime e.g. viruses, malware, denial of service (DoS) attacks.
2. Where technology is used as a tool to facilitate the crime through the use of the internet e.g. phishing emails, cyberstalking, identity theft.

The RCMP interprets cybercrime to be any crime where cyber – the Internet and information technologies, such as computers, tablets, personal digital assistants, or mobile devices – has a substantial role in the commission of a criminal offence. It includes technically advanced crimes that exploit vulnerabilities found in digital technologies.

Cybercrime Investigations Team and NC3

The OPP's Cybercrime Investigations Team has a mandate to investigate cybercrimes where technology is the target of the crime, that includes instances of hacking, data breaches, and ransomware attacks. The Cybercrime Investigations Team assists in complex criminal investigations where technology was used as a tool to commit the crime i.e. criminal harassment, online fraud. They work collaboratively with law enforcement, government, academia, and the private sector to share cybercrime intelligence. The overall goal of the Cybercrime Investigations Team is to harden Ontario computer systems thereby enhancing security, and reducing victimization caused by cybercrime.

The lack of collaboration and need for a centralized system responding to cybercrime led to the establishment of the RCMP's National Cybercrime Coordination Unit (NC3). NC3 has a mandate to enable and empower Canadian law enforcement to better address cybercrime to reduce the threat, victimization, and impact on Canadians. With a focus on technically sophisticated and high impact cybercrimes, NC3 coordinates and deconflicts cybercrime investigations in Canada and works with international partners; provides investigative advice and guidance to Canadian police services to streamline local efforts[3]; produces actionable cybercrime intelligence for Canadian police services; and, is establishing a national public reporting mechanism for Canadian citizens and businesses to report cybercrimes and frauds to police. In coordination with the Canadian Digital Service (CDS), NC3 is codeveloping a National Cybercrime and Fraud Public Reporting System. NC3 estimates that full operating capacity with the national cybercrime solution will be ready by April 2023. In the interim, NC3 is actively recruiting its team, developing systems and processes towards the national cybercrime solution, and building relationships with local and provincial police services, other government departments and agencies (including the Canadian Centre for Cyber Security), the private sector and NGOs, as well as international law enforcement.

Types of Cyber Crimes

[3] There is no obligation for local police services or the OPP to work directly with NC3 after a cybercrime has been reported. Coordinating investigative efforts with NC3 is voluntary. They will work with the police service in the jurisdiction impacted if requested.

Crimes where technology is the target include:

- Ransomware
- Malware
- Denial of Service (DoS)
- Webpage Defacement
- Unauthorized Access (Hacking)
- Mischief to Data/Theft of Data

Crimes enabled by technology include:

- Fraud (e.g. online scams, fraudulent advertising, phishing, etc.)
- Threatening/Bullying/Harassment/Incitement
- False Information/Hoax/Swatting
- Money Laundering
- Identity Theft

A report[4] authored by Risk Based Security says that 2019 was one of the worst years on record for data breach activity. Although the following highlights are from the United States, several of the data breach trends are typical worldwide, particularly the increase and frequency of breaches:

- There were 7,098 data breaches reported.
- Over 15.1 billion records have been exposed and have compromised consumers personal and financial information.
- The number of records exposed by breaches is up by 284% compared to 2018.
- Web (inadvertent exposure of data online) compromised 13.5 billion records while hacking exposed 1.5 billion records. All other data types combined exposed approximately 120 million records.
- Email addresses and passwords remain high value targets for hackers. Attackers used phishing emails or click bait to lure users into giving up access to their email account. Once in, malicious actors are free to explore the content and contacts of the account holder.

What is Ransomware?

Ransomware attacks have impacted several Ontario municipalities. Ransomware is a form of malware that targets critical data and systems for the purpose of extortion. In most cases, data is encrypted and rendered useless – in latest variants, encryption cannot be broken without a decryption key.

Ransomware is frequently delivered through "spear phishing" emails – the practice of sending emails supposedly from a known or trusted sender in order to induce targeted individuals to reveal confidential information – however many current police investigations have seen Remote Desktop

[4] Risk Based Security, 2019 Year End Report, Data Breach Overview: https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

Protocol (RDP)[5] as the attack vector used to access systems without having to phish for passwords to gain entry to accounts. The system is immediately compromised when hackers access a previously disconnected RDP session.

Once a victim has been locked out of their data or systems, the cyber threat actor demands a ransom payment usually in Bitcoin, a virtually untraceable form of currency. After receiving payment, the cyber threat actor will (supposedly) provide an avenue to the victim to regain access to the system or data. Recent iterations target enterprise end users (staff), making awareness and training a critical preventative measure.

Why are attacks happening in Ontario?

According to the OPP, one of the main challenges to building awareness and cyber security training with organizations and staff is the disbelief that an attack will not happen to them, that they are not the focus of hackers. But as recent attacks in scope have proven, no municipality is immune to attack. Many people find cyber security complicated and sometimes overwhelming to figure out to protect themselves. This lack of awareness underscores the need for appropriate cyber security education and training as the weakest link in the chain is the end user that is managing emails and unsecure documents that could be exposed without proper awareness of potential threats.

Ransoms are also being paid, a key attraction for any hacker. Whether the ransom demand is large or small, the amount paid is a benefit that reinforces the criminal business model of hackers.

Data is easily accessible or not properly backed up making ransomware attacks far easier for hackers to implement and engage.

Attacks often go unreported which may embolden the attacker to continue criminality knowing that law enforcement is unaware of the scope of the problem and therefore not investigating the attack.

The OPP recommends not paying the ransom. However, this decision is ultimately up to the municipality and some have paid ransoms to gain access to critical data or systems immediately. The OPP suggests that organizations consider the following if they pay the ransom:

- Paying a ransom does not guarantee that an organization will regain access to data – there have been several cases where individuals and organizations have paid a ransom and never provided the decryption key to regain access.
- Some victims that have paid the ransom have reported being targeted again by cybercriminals.
- Some victims have been asked to pay even more ransom after their initial payment if they want to receive the decryption keys.
- Paying a ransom reinforces the criminal business model and encourages hackers to continue victimizing others.

[5] RDP attacks exploit legitimate features of the RDP service. Systems administrators manage Windows systems through RDP and can help users troubleshoot an issue from a distance. Hackers may gain access to systems by resuming a previously disconnected RDP session.

Appendix B – Canadian Centre for Cyber Security Programs and Services

The Canadian Centre for Cyber Security (Cyber Centre) is the single unified source of expert advice, guidance, services, and support on cyber security for government, critical infrastructure owners and operations, the private sector, and the Canadian public. The Cyber Centre unites existing operational cyber security expertise from Public Safety Canada, Shared Services Canada, and the Communications Security Establishment in to one high-functioning, responsive organization on cyber security issues. On top of its work to defend federal IT systems, the Cyber Centre also uses its expertise and knowledge to deploy cyber defense tools to critical non-Government of Canada networks designated as being of importance to Canada. That includes municipal government information technology systems.

For small to medium sized municipal governments, the Cyber Centre's Baseline Cyber Security Controls document is a good primer intended for organizations with less than 500 employees that want recommendations to improve resiliency through cyber security investments. The paper provides advice and guidance on accessible cyber security practices and is tailored to balance investment costs and cyber security guidance.

On top of the range of guidance documents, the Cyber Centre also offers several key services that municipalities should consider when building their cyber security toolbox:
The Cyber Centre is there for municipalities to help build awareness and provide best possible tools for on cyber security. The Cyber Centre suggests municipalities to first work direct with local police services if attacked but encourages municipalities to make the Cyber Centre aware of any smaller attacks e.g. phishing, etc.

The Centre is an excellent resource on cyber security covering off issues such as:

1. Awareness Reports and Notifications: access actionable cyber threat intelligence
2. Tools to Assist Cyber Defense Teams: strengthen your organization's defense capabilities
3. Report a Threat to the Cyber Centre: leverage the Cyber Centre's expertise
4. Community Building: further cyber security together

Key questions to consider on cyber security within your municipality and to discuss with Councils

- Internal Governance
  - Is cyber security a maintained priority?
- Investment
  - How much are you focusing resources on cyber security?
- Resilience
  - How prepared are you for a cyberattack?
- Supply Chain
  - Do all components of your supply chain have adequate cyber protection?
- Collaboration
  - Work with commercial cyber experts and leverage Government of Canada advice and guidance

Connect with the Cyber Centre

- Call – 613-949-7048 or 1-833-CYBER-88
- Instagram: @cse_cst
- Email: contact@cyber.gc.ca
- Webpage: www.cyber.gc.ca
- Twitter: @cybercentre_ca