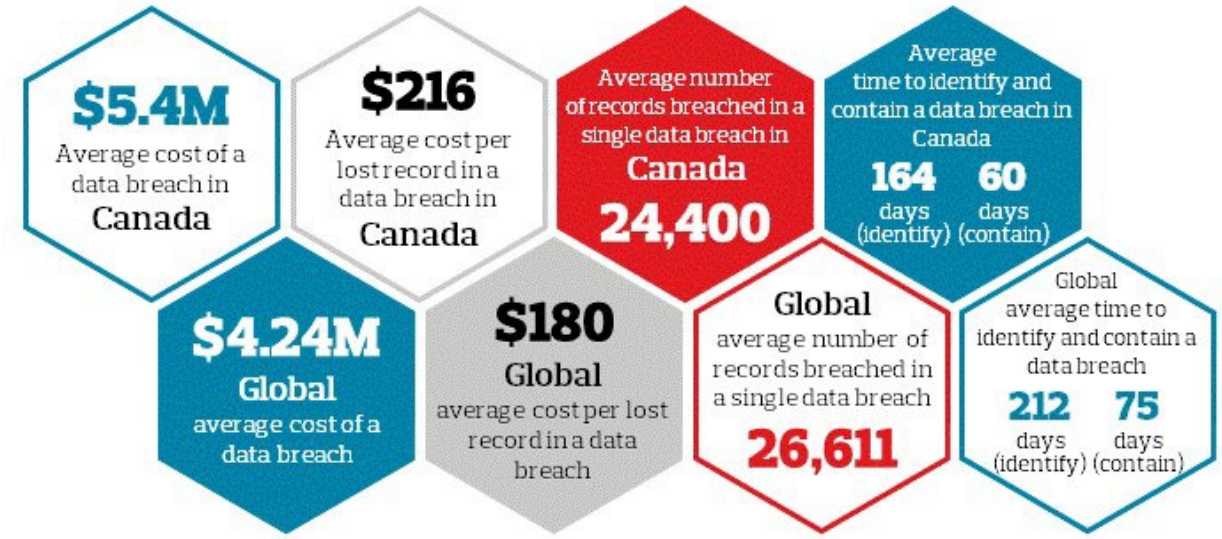
The Ransomware Epidemic
Stay Prepared for Ransomware

Aon Cyber Solutions and Kevin Madden, Principal Attorney – SUMAssure Insurance Reciprocal

According to the 2021 Global Risk Management Survey, cyber attacks were identified as the top risk management concern affecting all organizations. In 2021 cybercrime globally amounted to more than 6 Trillion dollars. By 2025 the cost is expected to rise to 10.5 Trillion.



In recent years, ransomware attacks have been impacting Canadian companies of all sizes and across all industries with little to no discretion and that includes municipalities here in Saskatchewan. Any municipality large or small, that either requires access to critical data or faces loss or hardship in the event of business interruption is a potential ransomware victim.

The Attack Evolution

Malware is software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system or network. Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the systems screen or by locking the users' files until a ransom is paid.

In a ransomware attack, threat actors gain unauthorized access to company networks and files using malicious software or malware. In most cases, a data breach is a precursor to the attack. After access is gained, cyber criminals establish a foothold in the environment (referred to as persistence) and quickly take one of two actions.

In the first, criminals encrypt files, making them inaccessible, and demand a ransom payment in cryptocurrency in exchange for the digital key code(s) to decrypt the files. In the second approach, which has become more common, the attack includes an additional step prior to encryption where the criminals seek specific types of data, including social insurance numbers, health card information, credit card information, payroll information, tax files such as T4 or accounting information, legal documents and other confidential information. Once these documents have been identified, the criminals collect and steal them before executing the malware to encrypt the data on the systems.

Prime Targets Need Rapid Response

Canadian municipalities are considered attractive targets for crime because they are viewed as affluent and protected. Many carry insurance coverage that can assist not only in covering some of the costs associated with cyber attacks, but also in helping connect victims with digital forensics and incident response companies that provide guidance in how to respond. A rapid response means faster time to contain the incident and begin recovery. Rapid response could limit the risk of data theft and the overall impact on an organization.

Committed Criminals Exploit Traditional Systems

Ransomware attacks are intentionally perpetrated by cyber criminals. It is important to distinguish these attacks from a malware infection, which may happen for a number of reasons that do not necessarily involve people. Cyber criminals are sophisticated and motivated. They have spent significant time and resources to ensure they understand both the way in which technology environments are constructed and the possible vulnerabilities within such environments.

Within Canadian organizations, and specifically with municipalities, there is a tendency to build technology environments using a so-called “tried and tested” approach. That means that many municipalities use the same consulting resources to design and implement technology infrastructure. While this is an efficient approach, it also means that in many cases municipalities across verticals may have the same security gaps or vulnerabilities for cyber criminals to exploit.

As organizations have begun to improve their defenses, these cyber criminals have also become more advanced in their approach, including taking pre-emptive measures intended to coerce ransom payment such as targeting and destroying data backups to prevent restoration, and stealing data prior to encryption with the threat of public release. This leaves many victims with the difficult choice of either permanent loss of data and an extended business disruption or paying a ransom to regain access and restore operations.

The Growing Consequences of Ransomware

For many victims, paying the ransom may seem like the only viable option. The possible consequences of business disruption and loss or public exposure of sensitive data are severe, and can include loss of revenue, breached contracts, missed deadlines, failure to meet taxpayer expectations and damage to goodwill. In the most extreme examples damage can even extend to loss of life.

The most recent statistics on ransomware are staggering. Ransomware activity has dramatically outpaced data breach or privacy event activity, with an increase of 323 percent from Q1 2019 to Q4 2021. The average cost of a data breach in Canada is now $5.4 million, higher than the global average of $4.2 million.

8 Risk Mitigation Tips

Ransomware attackers often operate with the same discipline and approach as a traditional business, except they do so in a criminal venture and with criminal intent. Threat actors typically choose the path of least resistance to achieve their business goals, attacking vulnerable organizations and taking advantage of common exploits, or a lack of cyber defense and preparedness. To help mitigate the risk of falling victim to ransomware and to better prepare for a ransomware incident, consider these eight tips:

1. Be proactive.

Being victimized by ransomware tests an organization’s emotional response to crisis, its escalation procedures, technical prowess, business continuity preparedness and communication skills (particularly when the municipality must interact directly with the attackers). Ensure that the incident response (IR) plans, and emergency response plans (ERP) are regularly assessed and updated. Most importantly, test these plans through simulated practice across realistic scenarios to help improve resilience.

2. Educate employees on cyber security and phishing.

Phishing is still a leading cause of unauthorized access to corporate networks, including acting as the entry point for ransomware attacks. Training users to not only spot a phishing email, but to also report the email to their internal cyber security team is a critical step in detecting the early stages of an attack. Municipalities of all sizes must create a culture where all employees feel responsible for enterprise security and are encouraged to participate in the proactive detection of, and defense against, threats, risks and attacks. Phishing awareness is a critical cornerstone to a cyber-secure culture.

3. Employ multi-factor or “two-step” authentication.

Multi-factor authentication means using something employees know (such as a password) with something employees have (such as an authentication key). **Multi-factor authentication should be a requirement for all users across all forms of login and access including email, remote desktops and external-facing or cloud-based systems and networks (e.g., payroll, time-tracing).** In many instances, the presence of multi-factor authentication may prevent the exploitation of stolen login credentials because the attacker does not also possess the necessary second piece of the login process, the authentication key. Multi-factor access controls can be even more effective if coupled with the use of virtual private networks (VPNs).

4. Keep systems patched and up to date.

The rudimentary cyber hygiene activity of system updates and patching often falls by the wayside, especially as operations and security teams are stretched, systems and endpoints age and move toward legacy status, and new systems, hardware and applications are introduced as businesses grow, mature, merge and divest. There are, and will continue to be, major unpatched vulnerabilities that allow attackers to compromise corporate networks. Attackers can often identify a vulnerable system with a simple scan of the internet using free tools. They engage in this exercise broadly and indiscriminately, looking for exploitable systems on which to unleash ransomware and other cyber attacks.

5. Install and properly configure endpoint detection and response tools.

Endpoint detection, also referred to as **Endpoint security** is the process of protecting a network's endpoints – such as desktops, laptops, and mobile devices – from threats. Tools that focus on endpoint detection and response can help decrease the risk of a ransomware attack and are useful as part of incident investigation and response. However, many entities that invest in these tools fail to properly configure them, greatly reducing their ability to detect, alert for and block threat actor behavior.

6. Design networks, systems and backups to reduce ransomware impact.

Ensure your privileged accounts are strictly controlled. Segment your network to reduce the spread of adversaries or malware. Have strong logging and alerting in place for better detection and evidence in the event of incident response. Having a technical security strategy informed by architects who know the latest attacks and adversary trends is important, as is the use of continuous threat intelligence monitoring in open source and on the dark web.

7. Consider risk transfer options.

Because a ransomware attack can threaten an entity’s reputation and goodwill, the complete risk of ransomware can never be fully mitigated or transferred. However, in practicing ransomware preparedness, organizations should consider obtaining appropriate cyber insurance coverage. In doing so, organizations should review how coverage addresses indemnification for financial loss, business interruption, fees and expenses associated with the ransom and incident response, as well as considerations for service providers, such as the ability to work with incident response providers of choice.

8. Pre-arrange your third-party response team.

An effective ransomware response will often include all or some third-party expertise across the disciplines of forensic incident response, legal counsel, crisis communications, and ransom negotiation and payment. Seeking out, vetting and engaging with these professionals during a ransomware incident places additional burden on an already strained enterprise, and is ineffective and inefficient when every second counts and every decision is critical. Because time is of the essence, it is vital to pre-vet and pre-engage team of professionals to prepare to respond to a ransomware attack as soon as it happens.

In conclusion, municipalities are at a high risk for cyber attacks in Saskatchewan. Ransomware attacks are happening in the public sector more and more each year and will continue to become even more sophisticated. To help prevent an attack or lessen the effect of an attack, work with a team of professionals such as IT professionals, lawyers and cyber risk experts to help guide you through the necessary cyber prevention steps that your municipality can take.