SUMAssure
Protection and Ownership
for Urban Municipalities

Risk Management Bulletin

October 2021

It seems a distant memory where every day we would see news articles about cyber attacks happening all over the country to all sizes and types of organizations. While the media may not be reporting much activity on the cyber attacks today, they are still active and are affecting several organizations and having a dramatic effect on operations. These attacks seem to be hitting everyone from small commercial business to large scale attacks on massive software giants and everything in between. Municipalities are no exception. Attacks on municipal organizations have risen dramatically since 2018 with many cases right here in Saskatchewan. COVID-19 and remote working conditions have also had a significant impact causing a substantial increase in ransomware attacks.

- **Ransomware up 486%** from Q3 2018 to Q4 2020
- Global ransomware damage costs are predicted to reach $20 billion this year**, an increase of 57x** from five years ago
- Some insurance carriers have reported an increase of **500%** in ransomware claims from **2018 – 2020**

This ransomware epidemic has had a dramatic effect in the cyber insurance industry causing many insurers to restrict coverages, increase rates, and in some cases no longer offer any kind of coverage. Unfortunately, that still isn't enough and there is now a requirement to have several cyber protocols in place for coverage to be provided. **Whether you are renewing a cyber liability policy or are obtaining one for the first time, you must be able to prove to the insurers that there are some basic elements in place to be successful in obtaining competitive terms.**

> *"Municipalities are no exception. Attacks on municipal organizations have risen dramatically since 2018 with many cases right here in Saskatchewan."*

Specifically, insurers will be looking to confirm the following:

Multi Factor Authentication (MFA) to protect remote network access, administrative access, and access to email with two or more means of identification for access control. For example, for email you must log in with username and a password, and have a verification sent via text or through an application on your cell phone.

Phishing awareness training to educate employees and end users on how to spot phishing emails. As well, know the red flags to drive down clicks on the malicious emails many ransomware attackers use to gain a foothold in a network. Training should be done on a regular basis with all current and new users.

Strong password management to prevent ransomware and other hackers from cracking weak admin usernames and passwords a 16+ character system should be utilized. These strong passwords should be rotated on a regular basis as ransomware attackers use cracked credentials to introduce and implement their ransomware software.

Cyber protection programs and firewalls must be installed and kept up to date to detect and potentially quarantine ransomware and other advanced malware to assist in forensics in the event of an attack. Programs must include malware detections and email protection programs to adequately protect the organization from these types of attacks. Lateral movement detection tools are strongly recommended. After gaining a foothold, ransomware actors typically move across systems using compromised IT credentials. Detection tools enables the attack to be shut down before ransomware is deployed.

Data backup and storage procedures should be reviewed. Having proper protocols around secure backup systems whether cloud-based storage systems or physical backups. Regular testing of backup systems should be performed to ensure data quality and to address any possible issues.

> *“You can help prevent some of these attacks by banning the use of bad passwords, blocking legacy authentication, and training employees on phishing. However, one of the best things you can do is to just turn on MFA. By providing an extra barrier and layer of security that makes it incredibly difficult for attackers to get past,* ***MFA can block over 99.9% of account compromise attacks****. With MFA, knowing or cracking the password won’t be enough to gain access.”*
>
> *– Microsoft 2019*

Once all this is done, the process must be continually monitored and adapted. Education must continue with all users to the programs and regular testing should be done to ensure that the protocols continue to work.

For more information or if you have any questions, please don’t hesitate to contact your account team.

SUMAssure
Protection and Ownership
for Urban Municipalities