ASSOCIATION OF MANITOBA MUNICIPALITIES | INSURANCE PROGRAM

RANSOMWARE

Cyber-attacks on Canadian businesses have been steadily increasing over the past couple of years, with 82% of Canadian businesses reporting an increase in cyber-attacks over the last 12 months. Ransomware, created in 2013, is being increasingly used by cyber criminals to target businesses and even local governments.

32%

Ransomware was responsible for 32% of all cyber claims in 2018.

What is Ransomware?

Ransomware is a form of malware that is designed to block access to a computer system, denying users access to their data until a sum of money is paid. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once downloaded and opened, the attacker can take over the victim's computer and systems.

Once the user's files are encrypted, they can usually only be decrypted with a mathematical key known only by the attacker. The user's computer(s) will often display instructions on how to pay a fee, often in Bitcoin, in order to get the decryption key. For small business owners, it is not necessarily the ransom money that hurts the most – it is the hours and hours of downtime, which results in serious financial threats to their companies.

Ransomware Risk Management Tips

1. **Keep your operating systems and applications up-to-date.** Software updates often include important security patches to reduce vulnerabilities in your systems.
2. **Don't install software or give it administrative privileges unless you know exactly what it is and what it does.**
3. **Install reputable anti-virus and whitelisting software.** Anti-virus software will detect harmful viruses or applications. Whitelisting software helps prevent unauthorized applications from running on your systems.
4. **Create regular off-site back ups of your files.** While back ups won't prevent a ransomware attack, they can significantly reduce the damage. Off-site backups will remain viable even if your central server is compromised, allowing you to recover your data entirely.

What to do if you experience an attack?

1. **Do not immediately pay the ransom.** Often businesses will attempt to deal with the situation on their own by paying the ransom, however there is no guarantee the files will be released and it could ultimately affect your insurance claim settlement.
2. **Notify our claims team immediately.** It is very important we receive immediate notification so that we can ensure your business receives the right advice and guidance. Our claims team is available 24/7 and can be accessed by calling 1-800-665-8990.
3. **We will appoint a specialized IT forensic provider to assist in the recovery of your files.** The provider will provide the appropriate advice on what to do and how to manage the situation.

Ransomware/Extortion coverage is only available with the enhanced cyber liability package (See Cyber Liability Options Insert). If you would like to add this to your policy, please contact your Commercial Insurance Advisor for more information at 1-800-665-8900.