LEAGUE OF WISCONSIN MUNICIPALITIES MUTUAL INSURANCE

State-of-the-Art CYBER PROTECTION

With cyber liability coverage from League of Wisconsin Municipalities Mutual Insurance, you have acess to state-of-the-art cyber coverage to keep you protected against cyber threats.

If your business relies on internet access, email communication, accepts credit card payments, collects customer information, or stores employee data, your business is at risk. Whether your systems become compromised due to malware or personal data is accidentally exposed, you may suffer losses that can be covered by your cyber insurance endorsement.

In 2019

- The Identity Theft Resource Center (ITRC) reported 1,473 data breaches. This is a 17% increase over 2018 records.[1]
- 65% of US organizations experienced a successful phishing attack last year.[2]
- Average ransom demands doubled in 2018, from $42K to $84K.[3]

Cyber Liability protects you against:

- System failure due to ransomware or malware attacks
- Loss and/or exposure of customer or employee data, including social security numbers, phone numbers, email addresses,
- Phishing or email scams targeting your business or employees that result in financial loss

Cyber Risk Support & Training

With access to expert cyber security advisors and online training courses, our cyber support resources help you and your organization mitigate cyber risks and the impact of a cyber security breach. You'll have access to:

- Cyber security advisors to help with scenario planning and policy development
- Online cyber security courses and trainings
- Best practices for cyber incident response planning

Through our partnership with leading cyber insurance provider, Tokio Marine HCC, you have access to a team of cyber experts with the experience and know-how to respond quickly and get your business back on track. Should you suspect a cyber breach, the response our expert claims examiners coordinate the response, including expert legal counsel who will act as your breach coach throughout the claims process. If necessary, specialists may be engaged, including:

- IT security and forensic experts
- Public relations/advertising support
- Breach notification
- Call center and website support
- Credit monitoring and identity theft restoration services

Cyber Threats to Your Business

System Failure Claim Scenario

During a public library's system upgrade, a software malfunction causes data corruption. Unfortunately, an attempt to restore lost data from uninspected backups, was also corrupted during the installation process. The library hired part-time employees to manually recreate the lost data from paper receipts. System Failure Insurance covered the library's data restoration expenses, including the cost of hiring additional staff to recreate the lost data, as well as associated business interruption losses.

1. Identity Theft Resource Center, " ITRC Breach Reports, 2019 End of the Year Data Breach Report", January 28, 2020 https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/

2. Proofpoint, "Threat actors leverage credential dump, phishing, and legacy email protocols to bypass MFA and breach cloud accounts worldwide", March 14, 2019 https://www.proofpoint.com/us/threat-insight/post/threat-actors-leverage-credential-dumps-phishing-and-legacy-email-protocols

3. Coveware, Inc., "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate", January 22, 2020 https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate#:~:text=What%20Is%20the%20Average%20Ransom,that%20are%20actively%20attacking%20companies.

LEAGUE OF WISCONSIN MUNICIPALITIES MUTUAL INSURANCE

State-of-the-Art CYBER PROTECTION

Cyber Crime Claim Scenario

An accountant at a small municipality in the Chicago area received an e-mail from a member of the municipality's finance and budget committee requesting a wire transfer be processed in the amount of $50,000. The wire was sent, but, in a later conversation with a committee member, the accountant discovered that the committee had not actually requested the wire transfer. In fact, the e-mail the accountant received was a "spoof" e-mail, sent by a hacker who had created a fraudulent e-mail account to impersonate a committee member. The bank would not return the municipality's funds because the transfer appeared to be legitimate. Cyber Crime Insurance covered the municipality's financial loss of $50,000.

State-of-the-Art Cyber

League of Wisconsin Municipalities Mutual Insurance's cyber liability insurance provides coverage and support for a broad range of cyber threats and related expenses:

Breach Event Costs - Coverage for mitigation costs and expenses incurred because of a privacy breach, security breach or adverse media report, including legal expenses, public relations expenses, IT expenses.

System Failure - Coverage for income loss, business interruption expenses, and data recovery costs.

Cyber Extortion - Coverage for extortion-related expenses and monies paid as a direct result of a credible cyber extortion threat, including ransomware.

Cyber Crime – Coverage for loss of money or securities incurred due to financial fraud, including wire transfer fraud; charges incurred for unauthorized calls resulting from fraudulent use of an insured telephone system; expenses incurred to notify customers of phishing schemes.

Reward Expenses – Coverage for reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, or phishing attack.

Court Attendance Costs – Coverage for reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, or phishing attack.

BrandGuard® - Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.

Multimedia Liability - Coverage for third party claims including claims alleging copyright/trademark infringement, libel/slander, plagiarism, or personal injury.

Security and Privacy Liability - Coverage for claims alleging failure to safeguard electronic or non-electronic confidential information, or failure to prevent virus attacks.

Privacy Regulatory Defense and Penalties - Coverage for regulatory fines, penalties and regulatory compensatory awards brought by federal, state, or local governmental agencies.

PCI DSS Liability - Coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

TCPA Defense – Coverage for the defense of claims alleging violation of the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the CAN-Spam Act, or any similar federal, state, local or foreign law regulating the use of telephonic or electronic communications for solicitation purposes.

If you are interested in coverage, contact your League of Wisconsin representative or visit us at: www.lwmmi.org

LEAGUE OF WISCONSIN MUNICIPALITIES MUTUAL INSURANCE