TOIRMA Update

By Jim Donelan TOIRMA Executive Director

TOIRMA Enhances Cyber Liability Coverage

On behalf of the Board of Trustees, TOIRMA is pleased to announce the expansion of the Cyber Liability Coverage program for its members. Everywhere we look today, cyber and cybersecurity is the hot button topic of discussion. The bad guys are becoming more sophisticated, and the attacks more complex.

This year, TOIRMA re-designed Cyber Coverage to better protect townships from losses and exposures. While the historical focus of cyber policies has been the theft of data, policies have evolved in the last few years to be significantly broader in scope. Through an expansive search of the insurance marketplace, TOIRMA has partnered with DUAL Cybersecurity to provide enhanced coverage this year.

The following questions and answers relate to the new Cyber Liability Coverage offered by TOIRMA.

Question: *When does the new coverage take effect?*

Answer: The new Cyber Liability Coverage will take effect on June 1, 2020, which is the beginning of the new TOIRMA Program Year.

Question: *What is covered?*

Answer: TOIRMA's new Cyber Coverage is designed to cover claims relating to (1) Network Security Liability, (2) Media Activities Liability, (3) Privacy Liability, (4) Privacy Notification and Penalties Costs, (5) Confidential Information Extortion Costs, (6) Confidential Information Recovery Costs, (7) Business-Network Interruption, and (8) PCI Expenses.

Question: *What was enhanced over prior coverage?*

Answer: There were several coverage enhancements negotiated within the coverage. (1) legal counsel (breach coach) limit increased from $50k to $100k, (2) computer forensics limit increased from $50k to $100k, (3) notification costs limit increased from $50k to $100k, (4) credit monitoring limits increased from $50k to $100k, (5) extortion limits increased from $50k to $100k, (6) business income coverage added with $100k limits, and (7) data restoration coverage added at $100k limits.

Question: *What is "Network Security Liability?"*

Answer: Network Security Liability covers defense and damages a township is legally liable for, resulting from a claim alleging a Network Security Wrongful Act. This covers townships against:

- failure to prevent a third party or an employee from unauthorized access to, use of, or tampering with, Computer Systems, including but not limited to:
    a) Hacker Attacks
    b) Computer Virus attacks
    c) Theft of Electronic Data
- inability of an authorized third party to gain access to the township's services including Denial of Service, unless such inability is caused by a mechanical, telecommunications or electrical interruption or failure that is not under the township's care, custody, and control
- negligent and/or inadvertent transmission of a Computer Virus to a third party
- loss of employee Personally Identifiable Non-Public Information
- negligent and/or inadvertent act, error or omission committed by the township that results in a Network Security Breach

Question: *What is "Media Activities Liability?"*

Answer: Media Activities Liability covers defense and damages for one or more of the following acts committed during the performance of media activities:

- defamation, libel, slander, product disparagement, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related to disparagement or harm to the reputation or character of any person or organization
- invasion of or interference with the right to privacy or publicity
- false arrest, detention or imprisonment, or malicious prosecution
- infringement of any right to private occupancy, including trespass, wrongful entry, eviction, or eavesdropping
- infringement of copyright, domain name, trade dress, title, or slogan, or the dilution or infringement of trademark, service mark, service name, or trade name
- unfair competition, provided it is alleged in conjunction with the types of claims identified in the bullets listed above
- plagiarism, piracy or misappropriation of ideas

Question: *What is "Privacy Liability?"*

Answer: Privacy Liability covers defense and damages a township is legally liable for, resulting from a claim alleging a Privacy Wrongful Act. This covers townships against:

- physical theft of hardware or paper files containing Personally Identifiable Non-Public Information that is in the care, custody or control of the township or an independent contractor, or that is in the care, custody, or control of a third-party vendor, supplier, or contractor that is holding, processing or transferring such information on behalf of the township
- theft of Electronic Data involving Personally Identifiable Non-Public Information
- the township's failure to timely disclose a Security Breach in violation of any Breach Notice Law
- actual or alleged violation of a Privacy Law
- failure by the township to comply with that part of a Privacy Policy that specifically

a) prohibits or restricts the township's disclosure, sharing, or selling of a person's Personally Identifiable Non-Public Information

b) requires the Member Entities to provide access to Personally Identifiable Non-Public Information or to correct incomplete or inaccurate Personally Identifiable Non-Public Information after a request is made by a person

c) mandates procedures and requirements to prevent the loss of Personally Identifiable Non-Public Information

Question: *What are "Privacy Notification Costs & Penalties?"*

Answer: Privacy Notification Costs are first party costs of the township to respond to a cyber incident, including:

- costs to hire a computer security expert to determine the existence of and cause of any Security Breach
- costs to provide notification in compliance with a Breach Notice Law
- Credit Monitoring Expenses
- fees, costs or expenses charged by an attorney to determine the applicability of and actions necessary to comply with a Breach Notice Law

Penalties are civil fines or financial penalties imposed by governmental entities in a Regulatory Proceeding.

Question: *What are "Confidential Information Extortion Costs?"*

Answer: Confidential Information Extortion Costs are first party costs of the township to respond to a threat to harm or damage a Computer System or access or disseminate Personally Identifiable Non-Public Information, including:

- the payment by any township to a third party as extortion for the purpose of ending a Confidential Information Disclosure Threat

- any reasonable and necessary costs or expenses incurred by the township in resolving, investigating or establishing the cause of a Confidential Information Disclosure Threat against the Insured resulting from a Confidential Information Disclosure Threat

Question: *What are "Confidential Information Recovery Costs?"*

Answer: Confidential Information Recovery Costs are first party costs of the township to engage an outside party to restore, recover, recollect or replicate electronic data in the care, custody or control of the township that is damaged or destroyed as a direct result of a Security Breach.

Question: *What is "Business Network Interruption"?*

Answer: Business Interruption Costs means the net income which the insured would have earned had no Security Breach occurred. It also includes Confidential Information Recovery Costs noted above.

Question: *What are "PCI Expenses"?*

Answer: PCI Expenses are amounts incurred by the township pursuant to a Card Processing Agreement because of a township's alleged non-compliance with the Payment Card Industry Data Security Standard and directly resulting from: (1) a Network Security Breach; or (2) the failure to properly destroy, handle, manage, or otherwise maintain Card Information.

Question: *What else should I be aware of?*

Answer: There is a new requirement this year for the coverage to apply. The township must have weekly (or more frequent) backups to either the cloud or onto portable media. While it is new wording, there are a few things to note:

- If you are using a third party provider for your IT services, this should be something they can easily offer to you within the scope of their work (if they are not already). Please check with your provider.
- If you are not using a third party to provide your IT services and everything is handled and stored in house, then this is a basic data security practice that can drastically reduce the pain of a ransomware attack.

Question: *What tools/loss control resources related to cyber security are available?*

Answer: There are several resources available to help make any township a better risk, regardless of where they sit on the information security scale. Services include an ASSUREtrust IT Security Policy Guide with best practices as well as access to eRisk Hub providing:

- Link to report a breach and vendors that can be engaged (law firm, forensics, notification and credit monitoring)
- Link to an external vendor for vulnerability scanning at a preferred price
- Link to an instructional on how to build an effective incident response plan
- A newsroom with links to relevant stories on cyber and information security that is constantly updated
- A training tab with basic video shorts and training resources that can be accessed both free and at a discounted value with external vendors
- A content library for everything you could want to know including best practices, claims studies, incident response planning, trends, stats and more

Question: *How do TOIRMA members access the online resources discussed in the prior question?*

Answer: TOIRMA member contacts have been sent a letter outlining the process for accessing https://www.eriskhub.com/dual. If you need assistance accessing these online resources, please call Danielle Smith at (217) 444-1204 to obtain the activation code. Once registered with the site, TOIRMA members will have access to information such as breach response roadmaps, learning centers, risk management tools noted in the prior question, eRisk resources and a news center with trending cyber and data security information.

Question: *Can TOIRMA members implement policies and procedures to protect data and minimize or prevent cyber liability losses?*

Answer: Yes, TOIRMA members are the first line of defense in the prevention of cyber liability losses. Privacy policies and procedures, breach response and preparedness, risk reduction preparation, and best practices tools shown above are key elements to eliminate losses.

Question: *How do I report a claim or potential incident?*

Answer: Cyber claims and potential cyber incidents will be reported to the TOIRMA Claim Reporting Hotline at (844) 562-2720 (available 24/7) or toirma.org/claims-management. Timely reporting of cyber claims and cyber incidents is crucial so that the proper vendors can be engaged. Using your own vendors can jeopardize or even potentially exclude coverage for an otherwise covered event.

We hope this information is helpful. Please feel free to contact me toll-free at (888) 562-7861 or by email at jdonelan@toirma.org with any additional questions you have.

TOIRMA

toirma.org