TOIRMA Adds Cyber Liability Coverage

By Jim Donelan, TOIRMA Executive Director

On behalf of the Board of Trustees, TOIRMA is pleased to announce the addition of Cyber Liability Coverage for its members. It's difficult to go through your daily routine without reading an article online, in the newspaper, or seeing a TV report regarding cyber problems. It seems like the hackers are out there making our lives more and more miserable each day. During this past year alone, my identity was stolen twice that I'm aware of, and I spent countless hours on the telephone with credit card companies, police officers, financial institutions, stores, the federal government, and the credit rating agencies. I can only hope I'm more secure now than I was before, but who knows. Not only did someone have duplicate credit cards with my name on them, but they also had an identification card. Any of you that have been through this knows just how time consuming a process it can be to correct cyber-related problems. TOIRMA's new Cyber Coverage is designed to better protect townships from losses and exposures not otherwise covered, and becomes effective June 1, 2017.

TOIRMA started in 1986 with only two members. At that time, it was difficult for local governments to obtain insurance coverage at an affordable/stable price. TOIRMA is an intergovernmental risk pool designed specifically for townships, road districts, and multi-township assessment districts. Coverages included in the TOIRMA Program are: General Liability, Auto Liability, Bridge Coverage, Employee Benefits Liability, Equipment Breakdown Coverage (boiler and machinery), Public Officials Liability, Property, Auto Physical Damage, Inland Marine, Workers' Compensation, Treasurer's Bond, and Accidental Death and Dismemberment. TOIRMA also provides members access to the Human Resources Help Line.

Most of the time we think of cyber security problems pertaining to a "hacker" that has broken through our computer firewalls and infected our computers with a virus or taken our information hostage. Although, these are indeed problems that occur, sometimes cyber issues arise from human error. For example, a township official could accidently email out confidential information pertaining to general assistance clients. TOIRMA's Cyber Liability Coverage and resources will help townships by providing tools relating to these issues and situations.

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, 2017, 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) Information Security and Privacy Liability, (2) Privacy Breach Response Services, (3) Regulatory Defense and Penalties, (4) Website Media Content Liability, (5) PCI Fines and Penalties, and (6) Cyber Extortion Loss.

Question: *What is included in "Information Security and Privacy Liability Coverage?"*

Answer: Information Security and Privacy Liability covers damages and expenses a township is legally liable for, resulting from a claim, including violation of a privacy law. This covers townships against:

- theft, loss, or unauthorized disclosure of personally identifiable non-public information or third party corporate information;
- acts or incidents that directly result from a failure of computer security to prevent a security breach;
- failure to timely disclose an incident in violation of any breach notice law;
- failure to comply with that part of a business' privacy policy that specifically:
  - prohibits or restricts the disclosure, sharing or selling of a person's personally identifiable non-public information
  - requires 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
  - mandates procedures and requirements to prevent the loss of personally identifiable non-public information;
- failure to administer (a) an identity theft prevention program or (b) an information disposal program required by regulations and guidelines

Question: *What are "Privacy Breach Response Services?"*

Answer: The new Cyber Coverage provides members with breach services that include the following:

- forensic and legal assistance from a panel of experts to help determine the extent of the breach and the steps needed to comply with applicable laws;
- notification to persons who must be notified under applicable law;

- discretionary notice to individuals potentially affected by the breach in which there is a resulting risk of financial, reputational or other harm;
- credit monitoring and fraud protection services from Beazley partners to affected individuals. Alternatively, members may choose to offer their customers a data monitoring service; and
- public relations expenses, crisis management consultants, notifications to customers where notifications are not required by law, government mandated public notices related to breach events.

Question: *What are Regulatory Defense and Penalties?*

Answer: The new coverage provides defense expenses and penalties resulting from a regulatory proceeding resulting from a violation of privacy law.

Question: *What is "website media content liability?"*

Answer: Website media content liability are damages and expenses for one or more of the following acts committed during the course of media activities:

- defamation, libel or slander;
- violation of the rights of privacy of an individual;
- invasion or interference with an individual's right of publicity;
- plagiarism, piracy, misappropriation of ideas;
- infringement of copyright;
- infringement of domain name, trademark, trade name, trade dress, logo etc.; and
- improper deep-linking or framing within electronic content.

Question: *What are "PCI fines and penalties?"*

Answer: The new cyber liability coverage is designed to indemnify (protect) members from PCI fines and expenses that they may incur following a breach. PCI stands for "payment card industry." Typically, PCI is shown as PCI DDS which means "payment card industry data security standard." For example, if your township accepts credit card payment, and possesses cardholder information, there are exposure and compliance responsibilities.

Question: *What is "cyber extortion loss?"*

Answer: Cyber extortion can include a threat to breach computer security, destroy corrupt data, or interrupt computer systems. For example, a hacker can encrypt your computer files and demand payment for the decryption key. The extortionist typically enters a computer through a malicious email attachment or link.

Question: *Will TOIRMA offer its members any proactive tools/loss control resources related to cyber security?*

Answer: Yes. Members will have access through our cyber partner, the Beazley Group, to online resources designed to help TOIRMA members successfully prepare for, investigate, and respond to privacy or security breaches. These services will assist members in responding to actual or suspected data breach incidents effectively, efficiently, and with the aim of protecting your reputation and continuing day to day business.

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, www.breachsolutions.com. If you need assistance accessing these online resources, please call Debbie Prentice at (217) 444-1204 to obtain your agreement number and activation code. Once registered with the site, TOIRMA members will have access information such as online training and webinars, privacy policies and procedures, breach response and preparedness materials, risk reduction preparation, best practice tools, and summaries of federal and state compliance laws. The website will also provide access to trending cyber, and data security news.

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. In addition, immediate notification to TOIRMA allows the claims department a better chance of minimizing potential losses.

Question: *How much will TOIRMA members be charged for the additional Cyber Liability Coverage?*

Answer: The TOIRMA Board of Trustees decided to include the new coverage into the existing TOIRMA Program. There will be no additional charge.

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.