TOIRMA CYBER LIABILITY | Register for breachsolutions.com

The contact for each TOIRMA member received a mailing dated July 6, 2017 with the Cyber Liability Form, which was to be inserted into the new TOIRMA Program Manual. The letter talked about your access to breachsolutions.com, a proprietary risk management website containing valuable resources, such as sample privacy policies and procedures, breach response and preparedness materials, state and federal regulatory updates, trending cyber topics, and timely data security news and updates. Once you register, you will receive a confirmation email asking you to confirm your registration. If you don't receive the email, please check your spam or junk mail. Once confirmed, you will be able to use the password you created on your first visit to log on to the site.

You will need your Agreement Number and an Activation Code to register. If you need that information, please call Danielle Smith at (217) 444-1204.

Recently one of our TOIRMA members had an experience with ransomware and a Cyber Liability claim was turned in.

There is an informative article posted on the breachsolutions.com website titled *Ransomware: Best Practices for Prevention and Response.* There are some excerpts from the article below. You can find the whole article at breachsolutions.com.

What is ransomware?

Ransomware is a type of malicious software that restricts access to an infected machine, usually by systematically encrypting files on the system's hard drive, and then demands payment of a ransom, usually in a crypto-currency (e.g., Bitcoin), in exchange for the key to decrypt the data.

How can you prevent a ransomware infection?

- Ensure anti-virus software is up-to-date.
- Regularly train employees to avoid phishing attempts.
- Periodically test employees through phishing campaigns, monitor the effect on response rates, and consider a formal sanctions policy (after consultation with HR and your legal counsel) for repeat offenders.
- Block emails with .js, .wsf, and .zip extensions and macros at your email gateway level. If possible, disable the following commonly used attack vectors: Adobe Flash Player, Java, and Silverlight.
- If you use JBoss, review the developer information on configuring and hardening it.
- Evaluate whether application whitelisting makes sense for your systems.
- Enable automated patches for your operating system and web browser. Robust network segmentation can often reduce the impact of ransomware.

- Enable strong identity and access management, with the use of established principles of least privilege ("need to know"), and limit local administrative rights.
- Invest in an intrusion detection system to monitor signs of malicious activity. Implement (and test) a data backup and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location (preferably offline). Backup copies of sensitive data should not be readily accessible from local networks.

How can you respond to a ransomware infection?

- Infected machines should be disconnected from the network (wired and wireless) as soon as possible.
- Evaluate extent of infection, attempt to identify the type of ransomware variant, and determine whether the infected machine was connected to shared or unshared network drives, external hard drives, USBs, or cloud-based storage. You may also want to check for a registry or file listing created by the ransomware.
- Clean the ransomware from impacted systems (a variety of free and paid disinfection tools exist for this purpose) and reinstall the operating system. Do your own due diligence on the tools you use. Beazley does not endorse products in any manner, but reputable tools can be found from, for example, BitDefender, Kaspersky Labs, Norton/ Symantec, and Trend Micro.
- Proceed to restore from a reliable back-up. A well thought out back-up and restoration plan is one of the most important countermeasures against ransomware.

How can you respond when you don't have a backup of the data?

When unable to restore from a recent back-up or when faced with the prospect of operations grinding to a halt, many organizations elect to pay the ransom request, especially where the amount is relatively low. In doing so, organizations often struggle to procure the necessary amount of crypto- currency (e.g., bitcoin), and some thought should be given by organizations on how they would go about doing so.

- There is no guarantee of honor amongst thieves; the attackers might just take the money and run, or their decryption code might fail to work. There is also no guarantee that you're paying the right criminal.
- Some types of ransomware can be decrypted with the right tools. Find out what the variant of ransomware is and see if a legitimate decryption tool is available. Be cautious of companies telling you they can "break the encryption." Many ransomware variants employ commercial-grade encryption against which brute force attacks are difficult or impossible. Additionally, be careful about the source of any "decryption tool" so that you are not causing more harm by downloading another piece of malware.
- Consideration should be given to how and to what extent you should try to communicate with the criminals. Often, ransomware that comes with an

extortion demand has a hotline or even webpages dedicated to guiding affected victims through the payment protocol.

- It is possible to negotiate a lower price with the criminals, as well as to ask them for additional time to pay to buy yourself time.
- Keep in mind that it is likely that the criminals have no idea what type of data is at risk, nor do they usually know that you don't have any backups. Do not share any type of identifying information with them. If they find out your data is very sensitive, the ransom demand could jump significantly.
- Some types of extortion arrangements come with a "proof of life" which can help you verify that the criminal has the ability to unlock your files. Thoughtful consideration and caution should be used if you are accepting any file from these criminals.

If you think you have experienced a Cyber Liability loss, call the TOIRMA Claim Reporting Hotline at **(844) 562-2720 (Available 24/7)** or go to www.toirma.org/claims-management.