CYBER BULLETIN

JUNE 9, 2022

Top Nine Recommended Cyber Standards for 2022

In 2021, there were 4,145 publicly disclosed Cyber breaches in the US that exposed over 22 billion records. Experts estimate the cost of cyber-attacks in 2021 to be over $6 trillion annually. The public utility industry is particularly vulnerable due to the large number of potentially exposed systems.

Cybercrime can have a significant negative impact on your public entity. Vulnerable systems which are hacked can result in reputational risk, extortion, exorbitant fines, lost time due to recovery from an infiltration and more. Historically, cyber criminals have used common but effective tactics against networks with weak security to gain access. This has resulted in an explosion in the rates for Cyber Liability Insurance with increases in rates of more than 400% with higher deductibles and lower coverage. How do you know if you have adequate defense against Cyber-attacks, intrusions, and breaches?

Fortunately, the Fund has resources available for Members to access and reduce the likelihood of a successful attack. By addressing the following nine areas and using the cyber resources on the Fund's website (go to https://www.twcarmf.org/cyber-security/ after logging in to the Fund's website), TWCARMF members can significantly increase their cyber security and decrease the risk of cyber-attacks.

1. Implement Multi-Factor Authentication (MFA) for remote access, laptops, and privileged access.

A critical element of a successful cyber defense is MFA. MFA is when users must provide two or more pieces of evidence to verify their identity to gain access to an application or digital resource. It ensures users are actually who they say they are. MFA verification relies on three different categories of information that's unique such as a password or PIN, a code sent via phone or text, and a security code from an app, a fingerprint, face ID, or voice recognition. It has been said that MFAs are

the easiest cybersecurity measure to put in place, but they have the highest return on investment.

2. Install end-point protection, detection, and response across all devices with 24/7/365 response.

Strong end-point protection helps provide antivirus protection, malware detection, zero-day attacks, email phishing prevention, continuous monitoring, and secure web browsing. An end-point response, unlike antivirus software, runs more comprehensive checks and is a notch above the traditional antivirus tools when it comes to detecting and containing cyberthreats. If there are signs of intrusion, end-point protection will detect the intrusion and immediately and automatically respond. With the cyber-attacks happening today, it is important to have a strong end-point system in place.

3. Update all operating systems and software to current, supported versions and patches consistently.

Computers and servers should be using a supported version. System updates and patches should be applied automatically to fix security flaws. If there are any outdated operating systems like Windows 7 and prior versions or Windows Server 2008 and prior versions, you'll want to segregate those from the Internet and the network until they're upgraded to a supported operating system version or migrated to a new platform.

4. Use strong, complex, passwords, changed at least twice a year, and Active Directory features.

It's a good practice to have a Password Policy, and a good policy includes requiring complex passwords with 14-16 characters and consisting of a combination of upper- and lower-case letters, numbers, and special characters, and are changed at least twice a year. Without a strong password, cyber criminals searching password dictionaries can easily unpack your password, and therefore, unlock your accounts as well. An 8-character complex password could be hacked in just 39 minutes if the attacker were to use the latest graphics processing technology, according to a report by the security firm Hive Systems. *

*CNBC.com
https://www.cnbc.com/2022/03/20/study-if-your-passwords-are-less-than-8-characters-long-change-them.html
March 2022

5. Encrypt and back up data with a disconnected, off-site copy. Test restores twice per year.

Use multiple back-up methods to help ensure data safety, including daily incremental backups to a portable device or cloud storage. Backed-up data should be tested regularly, at least on a semiannual basis to see if it is working properly and can be restored. Make sure your back up is encrypted, and the data is free of any potential malware during the restoration process. Cyber experts refer to and recommend a "3-2-1" back-up strategy, which refers to having three copies of data on two different media and one copy off-site, which could include one that is cloud-based. Robust back up allows members to be back up and running quickly if there is a cyber-attack.

6. Train on cyber security awareness that includes social engineering and fraudulent transactions.

Unfortunately, cyber criminals can be correct once, but employees need to be correct always. Employees can be a member's first and last line of defense. Employees need to be educated, at least annually, to ensure they can identify, avoid, and deal with a cyber threat. Employee cyber security awareness training should specifically focus on anti-fraud, social engineering, phishing, email compromise, and fraudulent transactions. A simple but effective training measure is to remind employees to use sound judgment with email attachments and links.

7. Implement a Business Continuity Plan (BCP), Incident Response Plan (IRP), and test plans once per year.

By documenting policies, procedures, and processes and including them in a BCP or IRP, you will give your organization critical directions for specific attack scenarios which can help avoid further damages, reduce recovery time, and mitigate cybersecurity risk. BCP's and IRP's focus on planning for security breaches and how organizations will recover from those breaches when they occur. Knowing what to do if a cyber event occurs is critical, so everyone in the organization understands what they need to do. Tests on the plans should be performed annually to make sure the plans work and are updated.

8. Implement a Virtual Private Network, MFA network-level authentication, and honeypots for Remote Desktop Protocol.

Virtual Private Networking (VPN) is a useful tool for protecting privacy and data. A VPN will create a secure, encrypted connection between the client user and the office network. Discontinuing the use of Remote Desktop Protocol (RDP), a technical standard for using a desktop computer remotely, is recommended. RDP can easily be manipulated by hackers, and reportedly, 50% of all ransomware attacks start with RDPs. If using RDP, it is recommended that strong passwords, VPN, and MFA should be utilized, and network-level authentication should be enabled. A honeypot (a type of computer security mechanism) could be used as a decoy to lure the attackers to log in to it. Once activity is detected, an alert should be sent to an IT administrator.

9. Request a Cyber Risk Assessment and Consultation included with your Fund membership.

The Fund has consultant services available to all members to provide a comprehensive appraisal of your current cyber risk and preparedness level. Lee Cain, TCRMF Cyber IT Risk Consultant will meet with designated staff you choose which may include IT, Compliance, Risk, Operations and/or the General Manager.

Outcomes of the Cyber Risk Assessment include:

- An extensive review of your current IT environment and threat assessment
- A list of the top areas to help prioritize cyber security needs
- The ability for your staff to consult with an experienced IT/Cyber expert regarding Center needs
- A comprehensive report to use for departmental goal setting and strategy
- An Executive Summary of the report findings

- Access to templates used to develop strong internal plans, policies, and procedures, related to IT and cyber security and compliance
- Being prepared to provide the information required to secure Cyber Risk Insurance
- The peace of mind that comes with having a supportive “second look” at potential vulnerabilities

The aforementioned nine areas can provide a first line of defense to help protect your public entity from cyber threats. These mitigation efforts will improve functional resilience by reducing the risk of compromise, ransomware attacks, and severe business interruption. Cyber resources are available exclusively to members on the cyber website found on the Pool’s website (https://www.twcarmf.org/cyber-security/).

Please reach out to your TWCARMF Cyber Risk Consultant, Lee Cain, for an onsite IT Risk Assessment. Mr. Cain can assist with the development of procedures to minimize a data breach. You can easily contact Lee at (Lee.Cain@sedgwick.com) or call (512-619-1437).