CYBERSECURITY IMPORTANCE

When Robert Tappan Morris developed a worm in 1988, all he wanted to do was figure out how many computers were on the internet. What started as a curiosity instead turned into the world's first cyber-attack. The program was simple. He designed it to jump from computer to computer without needing help from anyone. As it wove its way through the internet, it kept track of all the devices it encountered and reported the final amount back to Morris. The program worked too well, infecting nearly 10 percent of all devices on the internet at its peak, jamming traffic, and preventing people from talking to each other.

Since Morris' innocent cyber-attack, attacks have drastically grown and are specifically targeting government entities now. In 2019, 23 towns in Texas were hit by a "coordinated" ransomware attack that prompted Governor Greg Abbott to order a "Level 2 Escalated Response" which is one step below the highest level of alert, Level 1, or "emergency." This came after state and local ransomware attacks in New York, Louisiana, Maryland, and Florida. The majority of cyber-related claims are due to phishing, ransomware, third-party breaches, and employees accidentally sending out personally identifiable information (PII). Cybercrime is expected to reach nearly $6 trillion in damage by the end of the year 2021. That's the bad news. The good news is an estimated 79 percent of all cyber-attacks could be prevented by having a good cybersecurity plan.

Here's a general plan to serve as a starting point that public entities can follow to help reduce your risk on the top ways hackers exploit vulnerabilities. While no plan can provide complete protection, this one will help entities prevent some of the more common ways your network can be attacked.

Action Plan

What you don't know can hurt you. This is why the first part of protecting your network starts with knowing what's on it. First, you should document all of your hardware, software, and applications.

- Create a list of all the computers (PCs, laptops, etc.), connected devices (printers, fax machines, etc.), and mobile devices (smartphones, tablets, etc.) that you have on your network. All of these are entry points into your network.
- Document all of the programs that are installed directly on computers and used by everyone.
- Keep a list of all the applications that people use on their tablets, phones, and web applications (Dropbox, Google Drive, etc.).

Once you have all of your hardware, software, and applications documented, you'll want to analyze and examine them for vulnerabilities.

- Locate all unused equipment and completely wipe or delete all data from them. If you plan to use them in the future, store them in a secure location. If not, properly dispose of them. Some attackers scout landfills looking for old hard drives on desktops, laptops, phones, and more. It is common to identify unused equipment that's not secured or wiped.
- Go through the list of all of your applications and software. If any of them are no longer being used, they should be thoroughly uninstalled from devices, cloud storage, on premise storage, servers, etc. If you are still using the applications, update them. A lot of "forgotten" applications and software remain installed on devices.
- Ensure the passwords used for accounts are secure. When feasible, each unique account should require a separate and secure password. It is common to see passwords written down unencrypted and not secure, posted on equipment, and never changed.
- Check for applications and programs that serve multiple storage purposes. When you have multiple applications or programs performing the same task, dedicate just one as your main option and the other as your backup option.
- Since we're talking about storage, create a records management plan for your electronic and paper records that includes documented retention schedules. Review them on an annual basis and securely destroy any outdated records utilizing shredders or a third-party shredding company. Secure all paper records remaining.

Once you've documented all the hardware, software, and applications on your network, and you've removed any old equipment or redundant tools, you'll want to make a plan to lower your cyber security risk by putting these practices in place.

- Update and change your passwords often. If a hacker somehow acquires your password, they'll only have a limited time to use it for criminal purposes before it's changed to a new one. Keep your passwords complex. Use new and different passwords for each account. Don't store them on sticky notes or digital documents. Implement two-factor authentication, where possible.
- Update operating systems, software, and firmware (network equipment, cameras, scanners, printers, etc.). Set schedules and reminders for you and the staff. Make them required, if possible.
- Update hardware, when possible (newer chipsets are usually less vulnerable). Older hardware often has more information about its vulnerabilities available to hackers. Older hardware isn't always capable of running most up-to-date software, which increases your security vulnerability.
- Install and maintain a full version of endpoint security for all devices with automated virus signature file updates. Do not use free versions of anti-virus software.

You'll also want to manage what's happening behind the scenes. This includes keeping track of new installs, the number of users, preparing a safety net, and educating your end users.

- Implement a mandated process for overseeing the installations of new programs and applications. You can do this through software or provide a document that helps guide people. Part of that process should also include documenting on what device and where each program is installed, especially if you have multiple buildings. This will make it easier to maintain a list of all the hardware, software, and applications on your network and make them easier to update later.
- Limit your users. The fewer accounts you have, the fewer opportunities there are for vulnerabilities and attacks. As part of this process, grant administrator access and other rights only to the people who absolutely need it.
- Back everything up. I'll repeat this again. Back. Everything. Up. Ideally, all of your data should be backed up to a secondary source that's separate from your primary source. In the event that your main source is compromised, hacked, breached, or even malfunctions, you'll have a safety net to help get everything back up and running as quickly as possible.
- Employ a cyber-security awareness training program. There are multiple platforms out there. An example is KnowBe4, a platform the TWCARMF Board recently approved purchasing for use by the membership. It's designed to help you integrate baseline testing using mock attacks, interactive web-based training, and continuous assessment through simulated phishing, vishing, and smishing attacks to build more resilient and secure "human firewalls."

This is a general guide to help you improve your entity's security plan. We know that a lot of entities will need help implementing risk control. Texas now has a cyber risk control program to help implement risk control services ranging from small to large. If you're looking to improve your cyber risk, contact us and we'll help connect you to our new cyber services.