Chapter 9: Your Cyber Security Checklist

I've talked about cyber security and the popular risks from ransomware, hacking, *phishing*, and *social engineering*. So what can you do about it? I don't have a one-size-fits-all solution that stops everything. In fact, any product that guarantees 100% protection from hacking is pure snake oil (you may wish to google snake oil salesmen if you are too young to get this reference!). When I started my company back in 2001, it was to help companies fix their IT problems, run backups and make sure antivirus was on every computer. Hackers were around, but mostly in the movies or a focused attack on a big corporation or government. I switched by business model from this break-fix mentality to managed services when I saw that hackers were really getting sophisticated with their viruses and *worms*. Antivirus needed to be monitored 24/7 so attacks or compromises could be dealt with swiftly to prevent the computer from becoming unusable (which resulted in a rebuild). Like an onion, the layers of protection I put over my clients is the best way to prevent cyber-attacks. Not one layer is sufficient; all must work together to protect the client. Regardless of all the technology we have, all it takes is for one employee to give out their password and the network is compromised.

So how do I do it? What are all the layers? Here's a checklist to get you started. Don't forget there's a glossary in the back for the words you see italicized. For each item you don't choose to do, that would go on your risk assessment as an accepted risk.

- ☐ **Backups:** Do you backup all critical information? Are the backups stored offline? Do you get a backup report EVERY day? Even on holidays? Are they successful?
- ☐ **Test Restore:** Have you tested your backups? Every day is ideal but can you do it weekly? Monthly?
- ☐ **Two-factor Authentication (*2FA*)**: Have you implemented 2FA on your email, cloud systems and remote access?
- ☐ **Password Management**. Do you utilize a password management system so that employees can easily keep all passwords unique and complex? This is a big one. I have seen passwords found on the *dark web* utilized to gain access to other systems. Absolutely do NOT store passwords in browsers!!!
- ☐ **Guard Your Email**: Email is the number one entry point for hackers by far. Work with your IT Pro to ensure that spam filters and security gateways are setup on your email to block threats before they hit the inbox. Sandboxing is a method where attachments and website links are tested before they get to the employee's mailbox. This is above and beyond what a spam filter does and will cost more.
- ☐ **Staff Training**: Another big one here because employees are the "weakest link". Have you trained staff on cyber security best practices? Do you have an ongoing program to keep cyber security top-of-mind? Phishing simulations put staff to the test. Can they pass? Do them regularly. The hackers are always coming up with new and clever ways to fool your staff and get around basic spam filters. You must keep your guard up year around.
- ☐ **Vulnerability Patching:** Have you implemented appropriate patching of known system *vulnerabilities*? Do you do this on a regular basis? Patch Windows, Mac, servers, switches, firewalls, phones at the very least. Don't forget other devices or appliances on the network (see #14).

- ☐ **Business Continuity**: Are you able to sustain business operations without access to certain systems? For how long? Have you tested this?
- ☐ **Antivirus with EDR:** *Endpoint Detection and Response* (*EDR*) allows your antivirus to do more. It can provide additional protection against ransomware and offer forensic information if a breach does occur. Unless you just love learning IT, I would leave the installation, configuration, and management to your IT Pro.
- ☐ **Encrypt Hard Drives:** There was a time when an encrypted hard drive was very slow. That is no longer the case. Every laptop we sell goes out the door with *encryption* on. Laptops are too easy to steal or lose. Windows Pro comes with a license of BitLocker and makes it easy to lock down. Highly recommended.
- ☐ **Encrypt Emails:** Email *encryption* is a must in any regulated industry. But it can also be necessary for any business. I can't tell you how often I've had a CPA ask me to email my previous year's tax forms over. Don't do that. Ever. In fact, if you receive such a request its time to find a new tax preparer. However, if you must email a tax form or your employee list to the health insurance company, then encrypt that email. Please. Your staff will thank you.
- ☐ **Implement DLP:** Data loss prevention (DLP) is a method of blocking the transfer of personal identifiable information. Most often its done on emails. So if an employee forgets to encrypt an email with a social security number or credit card number, the DLP policy will find it and block the transfer. DLP is fairly easy to implement in Microsoft 365. Please refer to your IT Pro for implementation. This is usually not expensive to implement and is very effective.
- ☐ **Risk Assessment:** Find out what your risks are, what you can tolerate. It can be a real eye-opener.
- ☐ **Vulnerability Scan:** What is out there that needs to be updated? It could very well be that smart refrigerators or security system on your network that needs to be patched or flat-out removed. In 2021 a casino was hacked through their fish tank thermometer. Just because a device or appliance has wi-fi doesn't mean you have to put it on the network.
- ☐ **Dark Web Scan:** The dark web is part of the internet that is not accessible by your typical browsers and search engines. It requires a special browser for access. While true its used a lot for illegal activities it is also used by third-world countries that are under oppressive regimes. The dark web is a popular marketplace for buying and selling user credentials. A dark web scan looks for your company emails and passwords on the marketplace. If it doesn't come up on the scan, it doesn't necessarily mean its not out there. However, if it does come up on the scan, change the password immediately and never use it again. The "for sale" list changes daily as hackers gain access to new systems and steal credentials, so a regular check of the dark web is necessary. However, using a password manager (see #4) can greatly reduce the risk by allowing unique passwords for every application and website.
- ☐ **Firewall Technology:** Better quality *firewalls* come with intrusion detection system (IDS) and intrusion prevention system (IPS). In simple terms, one detects intrusions and the other stops it. Since threats are constantly changing, a firewall with security like IDS/IPS will come with a paid subscription. Your business-class firewalls will offer a multitude of protections built around IDS/IPS so defer to your IT Pro for the benefits offered by your firewall. And keep your firewall security subscriptions up-to-date. A firewall should be able to do SSL inspections. This allows the firewall to see inside encrypted transmissions. Refer to your IT Pro for the pros and cons of this service.
- ☐ **Policies and Procedures:** All companies with computers should have a set of policies and procedures around IT. They should dictate how the computers are to be used.