**The Cost of Cyber Crime**

Target, Equifax, Adobe, eBay, LinkedIn, Yahoo, Twitter, Marriott, MGM Resorts, Garmin. What do all of these businesses have in common? They have all been victims of cyber-attacks.

In 2019, The FBI's Internet Crime Complaint Center (IC3) received a total of 467,361 complaints with reported losses exceeding $3.5 billion.

In 2019, the IC3 observed an increase in the number of BEC complaints related to the diversion of payroll funds. In this type of scheme, a company's human resources, or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally routes to a pre-paid card account.

**Losses reported for 2019 per crime type**:

- Business Email Compromise (BEC) - $1,776,549,688
- Spoofing - $300,478,433
- Phishing/Vishing/Smishing/Pharming - $57,836,379
- Ransomware - **$8,965,847
- Denial of Service/DDoS - $7,598,198
- Malware/Scareware/ Virus - $2,009,119

** Regarding ransomware losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate.

In 2019, the state of Missouri ranked 22nd out of the 57 states, American territories, and the District of Columbia for reported victims of cybercrime totaling 5,083 victims.

In 2019, the state of Missouri ranked 26th for reported losses due to cybercrime totaling $27,290,803.

Other research shows that non-profit organizations are becoming bigger targets because of the personal donor information that they keep. There is a growing concern that most non-profits do not have the proper security measures in place to protect themselves from cyber-attacks. (see resource links below)

**What should you do to protect your business from the devastating losses reported above?** There are multiple security point tools that can help you, such as solutions for vulnerability management, patch management, on-wire monitoring, logging, and asset management.

**Vulnerability Management Solution –** New vulnerabilities are created every day. How do you know what your risks are if you are not actively and consistently scanning your network for vulnerabilities?

If you have a patching program, how do you know if your patches were successfully pushed to all of your devices? Vulnerability scanning will identify any devices that are not up to date with patching. What about 3rd party patching? Same answer. Vulnerability scanning will sniff out the 3rd party software that needs patched.

How do you know if your network gear like firewalls, routers and switches are up to date on their firmware versions? Vulnerability scanning will tell you.

How can you possibly know what to remediate if you do not have a vulnerability management solution?

**Patching Solution –** If you have workstations, servers, and network devices, you should have a patching solution. Would you purposely leave your car unlocked at the mall if the back seat and trunk were full of Christmas presents for your family? Working from devices that are not properly patched is like leaving your car unlocked at the mall. All it takes is one bad actor snooping around the parking lot, testing doors to see if they are open and POOF, anything valuable you left behind is gone. The same applies for patching. All it takes is one bad actor snooping around your network to find the open door and your sensitive information is gone.

**On-Wire Monitoring Solution –** This solution is important for a healthy security program as it is patrolling your network and inspecting the traffic coming in and going out. It is like travelling at an airport. Before you can get into the terminal, you have to go through security. Your bags are searched, and your body is scanned to find anything that could cause harm to others. A good on-wire monitoring solution with 3rd wave artificial intelligence is doing the same thing; scanning 'bags' and 'bodies' to make sure nothing dangerous is coming in or going out of your network.

**Logging Solution –** Logging helps with tracking changes to your network. If you do not have a logging solution, then you do not have a record of who did what and when. Servers, firewalls, and other IT equipment keep log files that record important events and transactions. This information can provide important clues about hostile activity affecting your network from within and without. Log data can also provide information for identifying and troubleshooting equipment problems including configuration problems and hardware failure.

**Asset Management Solution** – It was discovered that the Equifax attack was because the bad actor found an unidentified asset in their network that was able to be breached. Do you have a complete list of all of your hardware and software assets? If you do not, how do you know what to patch, maintain, and monitor?

https://www.councilofnonprofits.org/tools-resources/cybersecurity-nonprofits

https://www.nonprofitpro.com/article/why-cybersecurity-should-be-on-your-nonprofits-radar/