JANUARY 2020

Newsletter

A New Year Means Evaluating Your CyberSecurity Protocols

OWEN IT

Did you know?

- 230,000 malware samples are created every day by hackers
- 60% of small businesses ultimately fail as a result of cyberattacks
- Over 3 million cryptojacking attempts were discovered between January and May 18 2018
- 4000 Ransomware attacks have occurred every day since 2016

Do these statistics scare you? They should.

10 Most Important CyberAttacks of the Decade

The only way to keep history from repeating itself is to learn from the mistakes of the past. The following is a list of the most significant cyberattacks from the last decade, as compiled by TechTarget:

1. Yahoo - 2013 - With the unfortunate legacy of being the largest breach in the history of the internet, all three billion Yahoo accounts were compromised. The organization took 3 years to notify the public of the breach and that every account's name, email address, password, birthdate, phone numbers, and security answers had been sold on the dark web.

2. Equifax - 2017 - Probably the most damaging attack occurred just 3 years ago with the hack of Equifax. The hackers were successful in gaining access to 143 million Equifax customers and information vital to the lives of all. The data stolen from Equifax included customer's names, birthdates, social security numbers, driver's license numbers, and addresses, and the hackers released over 200,000 credit card numbers and more than 182,000 documents containing personal identifying information.

3. Sony Pictures - 2014 - Hackers were successful in wreaking havoc on Sony Pictures by releasing damaging emails sent between Sony employees and discussing what they really felt about some of the world's top film stars. The hack was in retaliation for Sony's production of a Seth Rogen film, The Interview, and featured an attempt to assassinate the North Korean leader, and propelled North Korea into international prominence.

4. Marriott Hotels - 2018 - This attack has gained notoriety because the malicious actors behind the scenes had an unprecedented four years with which to move around the Starwood system. The hackers gained access to the names, credit cards, passport numbers, and addresses of millions of people who stayed at the hotel between 2014 and 2018 and no Starwood hotel was left untouched. Starwood Hotels operate under the brand names of Sheraton, Westin, W Hotels, St. Regis, Four Points, Aloft, Le Méridien, Tribute, Design Hotels, Element, and the Luxury Collection.

5. Ashley Madison - 2015 - While this attack was not financially significant, the damage it caused was devastating. When hackers breached Ashley Madison, the "discreet extramarital dating website" in 2015, more than 30 million email addresses and hundreds of credit cards were leaked. The company was sued in 2017 for $11 Million as a result of the breach, but the ramifications for some were life-altering.

6. Target - 2013 - Affecting more than 40 Million Target customers, cybercriminals were successful in obtaining payment card details. In the years following, Target ultimately admitted the number was even larger, and estimated that the impact reached 110 Million of their consumers, resulting in the ousting of Target's then CIO.

7. Capital One - 2019 - One of the most recent breaches occurred in July when Capital One bank acknowledged that for almost 14 years (2005 to 2019), hackers gained access to the financial information of 100 million Americans and six million Canadians.

8. The United States Office of Personnel Management - 2015 - Perpetuated by the Chinese government, the attack on the US Office of Personnel Management is considered one of the most significant to ever hit the government in the history of the country. The hackers gained access to 21 Million records of current and former government workers, even including information from background checks of individuals who were not even hired by the government.

9. First American Financial - 2019 - for over 15 years, real estate title insurance company First American Financial was the victim of a breach that exposed over 800 million financial, real estate deeds, loans and other real estate specific files.

10. Stuxnet - 2010 - Formed in collaboration with the United States and Israel, the Stuxnet worm was the first example of government-led cyberattacks causing infrastructure damage to an opposing force. The worm destroyed over 900 of Iran's uranium enrichment centrifuges and ruined most of the nuclear program through targeting of their Siemens SCADA system.

The biggest challenge for businesses like yours with cybersecurity is the simple fact that users are unaware of the risks. Keep in mind that 90% of cyberattacks are as a result of human error. Employees are the weakest link in the chain when it comes to your cybersecurity. Have you taken the time to evaluate your internal policies and security? Here are a few things you can do

3 Key Strategies To Secure Your Network

1. Educate, educate, educate: As employees are your weakest link when it comes to your network security, one of the best ways you can strengthen your cybersecurity is through educating your employees on the ways malicious sources gain access. Email phishing, text phishing, and more can put your business at significant risk. We are happy to help you develop an employee cybersecurity training module! Contact us to start.

2. Multi-factor authentication: As your managed services provider, we utilize safety measures just like these in our own office. Multi-factor authentication sends a unique code to the user's cell phone before allowing them access to any sensitive data.

3. When in doubt - don't click: Phishing is one of the most successful ways malicious sources have to gain access to your sensitive data. Antivirus provider, Norton, suggests that you never fill in personal or company information into any pop-up or link you did not specifically request.

Your corporate data is the lifeblood of your business. Whether the information you hold falls under compliance or are just sensitive information vital to the survival of your business, a cyberattack or breach can have significant effects on your business. We want to help you ensure the security of your business, so we are offering a New Year's special for a free 30-min Security Audit of your current systems and processes and get you off to a spectacular 2020. Give us a call today at 01174 220485 to schedule your free audit today.

Letter from the MD

Looking back over the last decade - and years of significant changes in technology and data security - it is remarkable to me how far the industry has come. Cybercriminals may get savvier, but so do we, keeping one step ahead and thwarting any attempt of malicious sources from gaining access to you.

2019 was a very enlightening year for us, and I wanted to take a moment to thank you for choosing us as your trusted advisor for your business technology needs. We plan to continue to strive for excellence and focus our energy on keeping your business working for years to come.

Here's to a happy, successful, and high growth 2020.

Jason Owen

Holiday hours

Office hours:
M-F 8:30 AM to 5:00 PM

Helpful links:

3 Security Threats Your Business Should Be Preparing for Now

ConnectWise Control Used As Entry Point In Texas Ransomware Attack