



Q-News

September 2021

A Word from Jack



Meeting Compliance Requirements: Our newsletters, blogs, and videos tend to be heavily focused on privacy and network security. Privacy and network security are the basic components of an IT security program. Quanexus has always focused on assisting clients manage their

IT infrastructure. About 15 years ago we expanded our services to assist clients with meeting different regulatory requirements. Some of the industries we focus on are banking and finance, medical facilities, local governments and government contractors. While clients in different industries must meet different regulatory requirements, the basics are the same.

We have developed a methodology that lets us transform regulatory requirements into a comprehensive IT security program that includes policies, procedures, and controls. Creating policies is typically the easy part. Implementing the tools and procedures to comply with policies is a bit more challenging. The other critical component of an overall IT security program is the feedback loop. This is the documentation that proves to management and if

necessary, an outside auditing team, that your policies are being followed and regulatory requirements are being met.

In the last 24 months, we have seen a huge increase in the number of clients that are now required to meet different regulatory requirements. Some of our clients were surprised when they found out that they needed to implement a formal IT security program. The requirement for a formal IT security program often comes from one of their clients that operates in a regulated industry. If you find yourself in a situation where your client is asking about IT controls or your security program, we can help. If you have any concerns about your current IT security program or implementing a new program, please give me a call for a free consultation.

What is DNS? Back to Basics

DNS was in the news with an outage that took down large corporate websites, and prevented airline passengers from checking in. Today we will explore what DNS is, and how it allows users to navigate the Internet.

Computers communicate with one another using strings of numbers called IP addresses. Instead of asking users to try to remember which string of numbers connects to Google or Delta Airlines, the domain name service (DNS) links an IP address to a website or web service. This system makes our lives easier and was built to be an efficient way for an operating system and browser to find the IP address for a given website. The problem is when one of these DNS services goes

down, it can take down large swaths of the Internet.

A DNS service provided by Akamai suffered a problem after an update cycle. The outage took down many sites including Southwest Airlines, Delta Air Lines, Fidelity Bank, US Bank, FedEx, UPS, the PlayStation Network and more. Akamai noticed the problem and reverted the update, but some sites took up to 24 hours to resolve to the correct IP address again. The website Downtetector tracks outages across the Internet and reported 48 services were down during the outage. The company emphasized the incident was not the result of a cyber-attack, but a bug triggered by a software update.

DNS services are a part of the Internet most users are unaware of until something goes wrong. Companies like Akamai control DNS resolution for large parts of the Internet, so when one service provider has a problem, many websites can be affected. Individual sites can also be affected by an attack on their DNS servers. Hackers can flood a domain's DNS servers in an attempt to disrupt the IP address resolution for a given site.

Quanexus™

571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com



CYBERSECURITY



CLOUD



COMPUTER



VOICE

Cyber Attacks Increase Again

Metrics in phishing and ransomware are skyrocketing; users continue to be the deciding factor in cybersecurity.

“Attackers don’t hack in, they log in, and people continue to be the most critical factor in today’s cyberattacks.” said Ryan Kalember, EVP of cybersecurity strategy, Proofpoint.

A new report out this month shows phishing attacks were up 440% in May, a new record for a single month spike. Energy industries like oil, gas, and mining saw a phishing increase of 47% over the first half of the year, while manufacturing saw a 32% increase over the same amount of time. Credential phishing was the most common target, accounting for two thirds of attacks.

Hackers continue to find new and more sophisticated methods of attack. COVID-19 is still a popular phishing vector, but hackers are now turning to

AI learning to target their victims. This new approach has been deemed smart phishing. Criminals are using intelligent malware to mine user behavior on mobile or desktop platforms. The data is used to spear phish a user on a service they regularly access.

Phishers are also using file sharing platforms instead of email attachments. Most users understand an email attachment from an unknown sender is dangerous. Criminals are exploiting the credibility of Dropbox and other file sharing services to embed malicious links hosted on these platforms.

An increase in phishing, results in an increase in ransomware. In the first half of 2021, ransomware demands increased by 518% and payments went up

82%. To match the record set in phishing attacks, a new payment record in ransomware was recorded at \$570,000 up from \$312,000 last year. The study also noted average payment amounts were up 171%.

Experts cite the global move to remote work as a large factor in the increase, as well as a lack of employee education on cybersecurity. “People aren’t learning from their cyber mistakes and more concerning, they aren’t equipped with knowledge on how to prevent repeat mistakes,” says Grayson Milbourne, security intelligence director at Webroot. Educating employees and then testing that education with IT controlled internal attacks continues to be an overwhelming factor in fending off hackers.

Why Hackers Don't Take a Holiday

The FBI released a warning before Labor Day citing a hacking pattern over long or holiday weekends. This year the meat processing company JBS was attacked on Friday heading into Memorial Day weekend. The Kaseya attack occurred on the Friday before the long Fourth of July weekend. The Colonial Pipeline attack took place over Mother’s Day weekend, a time many employees would have been more likely offline. We are still waiting to hear if any attacks occurred over this past weekend, but it’s clear hackers find holidays useful.

In general, ransomware attackers like weekends; they want the most amount of time inside a network to look around as possible. Attackers are also interest-

ed in the least amount of oversight, and if they are discovered, the least number of staff to deal with the issue. A long weekend, when many employees might also take off on Friday, is prime time to move around the network and encrypt files. Ransomware reports tend to spike on Monday when victims return to work to find their data encrypted.

Unfortunately, staying secure from hacking is not a matter of somehow locking down systems on Friday, and starting them back up Monday, holiday or not. Attackers typically have already gained access to the system, but they wait for the weekend to move around or encrypt files. The FBI used this past weekend to draw attention to the in-

crease in attacks and to give business owners another opportunity to think about their cybersecurity standing. The recommendations in the report were not quick solutions, but the practices and procedures we talk about on this blog continually:

“Don’t click on suspicious links. Make an offline backup of your data. Use strong passwords. Make sure your software is up to date. Use two-factor authentication.”

Understanding the way hackers work, and the patterns emerging from this year of increased attacks is another step in keeping your business and customer data safe.

T-Mobile Data Breach

The third largest wireless carrier in the country admitted to a data breach affecting 40 million customers and prospective customers. That number grew to 54 million after the FCC said it would investigate the incident. Images from the dark web show the data is for sale and includes user's name, address, phone numbers, drivers' license, Social Security number, and date of birth. The breach not only impacts current users, but also former customers, and prospective customers who gave T-Mobile their information to run a credit check but are not current customers of the wireless provider.

The company is facing criticism because this is their fifth data breach in four years. Even though this is by far the largest breach, it follows two attacks in 2020, one in 2019, and one in 2018. Security professionals are also criticizing T-Mobile's communication

to their customers. Some users received a text message about the breach, while others did not. The company released a statement that in part said, "We have no indication that the data contained in the stolen files included any customer financial information, credit card information, debit or other payment information..." This is an oversight because the data in the breach is everything a criminal would need to open new lines of credit in the victim's name.

The other major concern is the breach could open victims up to SIM swapping. Criminals can use the data in the breach to convince the wireless carrier that they need a replacement SIM card for their number. Once the criminal has taken over a user's phone number, they can use it to access two-factor authentication codes, and log into more secure accounts like banking and credit card accounts.

What to do if you're a T-Mobile customer?

First, change login passwords and PIN numbers. T-Mobile allows users to log in using their phone number, so if a criminal can find your password in another data dump and connect it with the PII from this breach they may be able to log in.

Experts are suggesting customers should freeze their credit reports until T-Mobile has more information on whose data was lost. All three credit bureaus allow users to put a lock on their report so if someone attempts to open credit in their name, it will be blocked, and the user will be notified.

T-Mobile is offering a free service to prevent someone from transferring a phone number to another carrier called "Account Takeover Protection."

Largest DDoS Attack on Record

Yandex, the Russian version of Google, was hit with the largest DDoS attack in the history of the Internet. This attack followed a different attack in August that at the time was three times larger than the largest on record. A distributed denial-of-service (DDoS) attack occurs when a criminal uses compromised computers or other IoT devices to bombard a server, service, or network with requests. It's a purposeful traffic jam to take down a targeted website. The network of compromised devices being weaponized is called a botnet.

In August, Cloudflare said they stopped a DDoS attack against a financial institution. That attack peaked at 17.2 million requests-per-second and was the largest until this recent attack on Yandex. The more recent Yandex attack peaked at 21.8 million requests-per-second,

so the strength of the botnet is growing. Both attacks are attributed to a hacker group called Meris.

The botnet is made up of unsecured routers manufactured by a single company. The hacker group found a way into routers and are using them to overload the website of their choosing. Criminals are able to create these botnets because companies sell cheap, unsecure devices that consumers buy and put on the internet. These devices are usually much cheaper than their secure competitor.

The company who makes the routers say they have fixed the firmware, but the majority of routers online are using an earlier version of the firmware that's still vulnerable.

"The biggest contributor to the IoT bot-

net problem — a plethora of companies white-labeling IoT devices that were never designed with security in mind and are often shipped to the customer in default-insecure states — hasn't changed much, mainly because these devices tend to be far cheaper than more secure alternatives." Krebs on Security

The devices you have connected to your home and business network matter. Devices should be patched and updated often because when issues are found, they are repaired. If your device is working on a three-year-old version of the firmware, you're opening up your network to vulnerabilities. Additionally, quality devices make a difference. These IoT devices are security cameras or baby monitors, but they can also be industrial sensors or manufacturing devices. Any device connected to the Internet is susceptible.



Five Cybersecurity Statistics

77% of organizations saw more or the same number of cyber-attacks over the past year.

Business owners recognize the new cybersecurity threat landscape. Criminals are targeting businesses in countries with more developed economies at a greater rate. The US and Canada are at the top of the list at 53%, with enterprise and midsize businesses being the most likely targeted at 50%.

15% of organizations closed their business because of a cyberattack.

Businesses are feeling the impact of the large increase in attacks over the past couple years. Organizations cited employee downtime as the largest financial repercussions after an attack. Reputation damage, and theft of intellectual property were also on the list, but one in seven businesses reported they had to close their doors completely after an attack.

62% of organizations anticipate an attack in the next 12 months.

Ransomware is at the top of every list because criminals follow the money. Many businesses have no choice but to pay ransoms, which keeps the cycle of attacks high. Identity theft anticipation is a close second at 60%.

70% of organizations plan to increase their cybersecurity budget this year.

Businesses in all sectors are seeing the need to increase cybersecurity. Companies in financial services, transportation, and technology are at the top of the list for increased security. CEOs are realizing the minimum is no longer acceptable to protect the assets their business runs on.

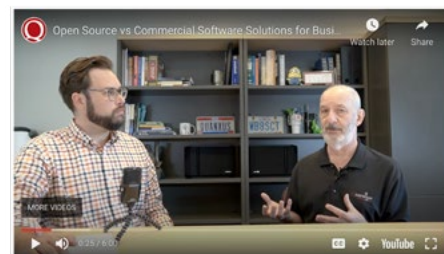
58% of organizations believe they will face an insider security threat over the next year.

Increases in cybercrime will give employees the opportunity to initiate a breach both through misconduct and intentional theft. The move of many businesses to work remotely only increases this risk. Businesses have less control over their data than they did 18 months ago. The increase of cybercrime combined with remote data opens the door for abuse.

Business owners are being forced to take cybersecurity seriously. The solutions to the cybersecurity threat landscape change daily. If you are looking for a security approach that fits a need as well as a budget, reach out and see if we would be a good candidate.

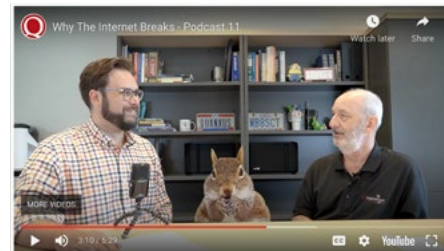
Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss Open Source vs. Commercial Software and Why the Internet Breaks!



Open Source vs. Commercial Software

[Click Here for Podcast- Open Source vs. Commercial Software](#)



Why The Internet Breaks

[Click Here for Podcast- Why The Internet Breaks](#)



Quanexus

571 Congress Park Dr.
Dayton, OH 45459
937.885.7272

quanexus.com

Follow Quanexus on Social Media!

Find Quanexus on Facebook, Youtube, LinkedIn, and Instagram! Click on the buttons below to access our social media pages. Like, comment and subscribe!

Also, subscribe to our email list to regularly receive tech news, cybersecurity alerts, and information on upcoming events.

Visit Quanexus.com to sign up!



[@Quanexus571](#)



[@Quanexus](#)



[@Quanexus](#)



[@Quanexus571](#)



[@Quanexus571](#)