Q-News

February 2022

A Word from Jack

Clients and prospects are always asking, how much does good cyber protection cost. The harsh reality is there is no budget big enough to guarantee your data and your network is safe. If governments and major organizations are successfully attacked with their big budgets, how can a small company with a small budget ever have enough protection? This leads to the question: how much is enough? My simple answer is you must do what is reasonable for your industry and size of organization. While this answer is somewhat ambiguous, this is the legal test that will have to be satisfied to determine if you acted responsibly or if you were liable.

At a minimum, there are basics that every organization must perform to meet the legal test. If you are looking for a starting point, I highly recommend you review two documents. The first document is the Center for Internet Security 18 (CIS-18). This lists 18 security controls that are divided into three implementation levels. Level 1 includes 56 safeguards and is considered a foundational set of cyber defenses. Level 2 adds an additional 74 safeguards, and Level 3 adds an additional 23 safeguards. For most clients Level 1 or Level 2 will be adequate.

The other document is the Cybersecurity Framework. This is a framework and does not include specific controls. These two documents can be used separately or together. I will be covering more on the CIS-18 in future articles.

Norton 360 Cryptominer

The popular antivirus company quietly added a cryptomining tool to their software in July of 2021, but the addition recently captured the attention and outrage of the cybersecurity community.

Cryptomining uses idle computers to verify cryptocurrency transactions. In return, the verification computer is rewarded financially, usually in cryptocurrency.
Norton's new add-on mines Ethereum to a pool of other users and charges a hefty fee in the process. The mining tool is not on by default, but users reported having issues not being able to turn it back off once it was enabled.

Critics point out the massive 15% fee Norton is charging as opposed to 1-2% other Ethereum pools charge. There are additional fees associated with getting the Ethereum out of the pool and exchanging it for another currency. Then, there is the increase in electricity usage since the mining software uses otherwise idle computers to do the work.

Norton's FAQ section explains the fees a user should expect. "The coin mining fee is currently 15% of the crypto allocated to the miner. Transfers of cryptocurrencies may result in transaction fees (also known as "gas" fees) paid to the users of the cryptocurrency blockchain network who process the transaction. In addition, if you choose to exchange crypto for another currency, you may be required to pay fees to an exchange facilitating the transaction. Transaction fees fluctuate due to cryptocurrency market conditions and other factors. These fees are not set by Norton."

Norton is the clear winner here with their 15% fee, but it's unclear if individual users will see any benefit.

There is also a security risk. The optics of an antivirus company opening users up to greater risk is not a good look. Cryptomining requires a greater understanding of password and security practices that may be beyond the reach of Norton's target demographic. The move appears to disregard their typical user in favor of skimming some crypto without assuming any risk.

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

Cybersecurity Year in Review

2021 will go down as the year that the public and many business owners started taking cybersecurity seriously. The primary story of the year was ransomware- how it's evolving, and the attacks on large and critical businesses.

Colonial Pipeline was a marker for cybersecurity in national news headlines. The general public followed the attack and subsequent shutdown of the fuel pipeline in the southeastern US. The news sparked panic buying at the gas pump and the first successful cyber-attack on critical infrastructure in America.

2021 was also a year that business owners took cybersecurity more seriously. Cybersecurity spending was up 12.4% from 2020 after the pandemic and remote work had already increased attacks last year. Business owners saw a peak in cybercrime in October of 2020 that continued through the first half of 2021.

Ransomware organizations evolved from a group of hackers to something that resembles a business. Some ransomware groups offer customer service to help victims pay a ransom and use a decryption key. We also saw criminals begin to use the data they stole to attack customers of the business, or their employees. In the past, it was possible to recover from an attack with a quality backup system, but these new threats are forcing more victims to pay.

However, the news was not all bad. The most aggressive ransomware group of the first half of the year, REvil, mysteriously went offline in July. The group was responsible for extorting $11 million from the meat processing company JBS Foods. The criminal website came back online in September, and just last month we learned the FBI was successful in hacking into the criminal servers when they came back online. They arrested two of the criminals and retrieved $6 million in cryptocurrency.

Another positive sign for cybersecurity is the increased use of multi-factor authentication. Important accounts like social media and banking are all moving to a second form of authentication as the default instead of an option that can be turned on. Many universities are also planning to move to MFA in the new year.

Cybersecurity in 2022

In our Year in Review article above, we covered the events and trends in cybersecurity over the past year. Which attack vectors will evolve and who will be the primary targets this year? Today we dive into three cybersecurity predictions for 2022.

Phishing will continue to evolve in 2022. We saw a large move to text message phishing, or smishing, this year. These will continue along with high-quality spear-phishing campaigns. The most common cause of a breach last year, at 20%, was stolen user credentials. We look for criminals to use publicly available information of employees to create more convincing and sophisticated phishing campaigns to continue to exploit user credentials this year.

Successful phishing attacks accounted for 36% of breaches this year, which is up 11% from 2020. Both, the continued evolution of phishing strategies along with employees working from home, contributed to the increase in successful breaches. Employees are more susceptible to phishing attacks from home. Consumer-grade networks are not as successful at stopping the phishing request at the door, and distractions at home make employees more likely to click on the malicious link.

Ransomware will continue to be the primary attack vector in 2022. The average cost of a ransomware attack rose from $3.86 million in 2020 to $4.24 million in 2021. We talked about the triple threat of ransomware in a recent podcast, and we look for criminals to continue to use or manipulate data in order to make money.

Small and medium-sized businesses will become the primary targets of phishing and ransomware in 2022. Large businesses increased their cybersecurity budget during the pandemic, and spending is expected to jump 3.6% in 2022. All of this defense spending by large businesses and governments means criminals will have to target more small and medium-sized businesses to continue to be successful.

IoT Security

How many devices did you add to your home Wi-Fi network this holiday season? By the end of 2021, there will be an estimated 12 billion IoT devices connected to the Internet. IoT (Internet of Things) devices are often referred to as 'smart' devices and are becoming more common in household appliances. Smart refrigerators, locks, and thermostats are all gaining market share each year, but the influx of network-connected devices add an entry point for criminals. IoT devices often add a security threat to a network because they are not as secure as a laptop or smartphone.

Criminals can use large quantities of IoT devices as a botnet to overload and offline targeted websites. The primary devices targeted in these attacks are inexpensive IoT devices with default passwords. Criminals learn the password for one device and can take control of thousands of the same device across the internet.

On a smaller scale, hackers may compromise a single device to learn personal information about the user. If the device stores name, address, email, or phone number, this information may be available to a criminal. This information can be used with other information from the thermostat or security cameras to learn when homeowners are away normally.

Criminals can also use poorly secured IoT devices as a jumping-off point to move laterally through the network. This can be a threat to home and business owners alike. If employees connect unsecured IoT devices to the business Wi-Fi, they can pose a threat to the business network.

Generally, off-brand or inexpensive devices are less secure. They more often than not will have a default password and are not kept up to date with security patches and updates. Consumers should take time to research the security credentials of devices they are adding to their network. This is more important now that many employees are working from home and are adding devices to the same consumer-grade network they are also using for work.

Ransomware Attack on Payroll Company

The HR and payroll software Kronos was hit by a ransomware attack. The parent company UKG said it may take several weeks for the HR tools to return to normal. Kronos Workforce Central is a suite of software tools used to manage employees including scheduling, clock in/ out, attendance, and payroll. Some businesses are already raising the concern that they may not be able to pay employees until the tools come back online.

Kronos is used by tens of thousands of organizations including half the Fortune 1000. The high-profile HR management tool is used by many city governments including the City of Cleveland. Other customers of the software suite are universities, hospitals, Tesla, and the MTA in New York City.

"UKG recently noticed a ransomware incident that disrupted the Kronos private cloud, which houses a solution used by a limited number of customers. We take immediate action to investigate and mitigate the problem. Wake up, warn affected customers, notify authorities and work with leading cyber security experts. We are aware of the seriousness of the problem and support our customers. We are mobilizing all available resources and working hard to restore the affected services." the company said.

Beyond the headache of finding an alternative scheduling solution, and the possibility of not being able to pay employees around the holidays is the concern of compromised employee data. The City of Cleveland released information from the parent company that employee PII may have been compromised. UKG informed the city that the attack may have compromised employees' first and last names, addresses, last four social security digits, and employee ID.

For more information about how criminals are using ransomed data including employee PII, watch our podcast on The Triple Threat of Ransomware.

New CISA Warning

The United States' Cybersecurity and Infrastructure Security Agency (CISA) issued a new warning to US organizations following the cyberattacks in Ukraine. Click here to read the Insights PDF in its entirety. The publication is intended to get the attention of senior leadership of US organizations and encourages them to "take urgent, near-term steps to reduce the likelihood and impact of a potentially damaging compromise."

The alert highlights steps companies should take to reduce the likelihood of malicious intrusion. Included in these steps are multi-factor authentication for remote access, disabling all ports and protocols not essential for business, and ensuring software is up to date. The report goes on to outline steps for detection, incident response, and preparedness.

The Insights warning also links an alert titled Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. It's clear the FBI, NSA, and CISA are concerned tensions between Russia and the US over Ukraine will spill over into cyberattacks on critical US infrastructure.

The advisory reads, "CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation."

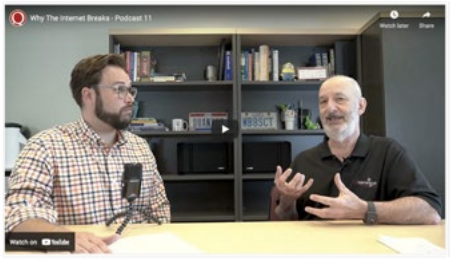
This report also follows the huge increase of malware attacks on the Ukrainian government and private businesses. The attackers have defaced websites and corrupted Windows and Linux-based server data. In Microsoft's investigation of the attacks they wrote, " [The malware] is designed to look like ransomware but lacking a ransom recovery mechanism, is intended to be destructive and designed to render targeted devices inoperable rather than to obtain a ransom."

Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss MFA or Multi-Factor Authentication, and The Triple Threat of Ransomware!

New Ransomware Response Scam

Click Here for Podcast- New Ransomware Response Scam



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