Q-News

A Word from Jack

July 2020

It is challenging to fully cover some topics in a single article. My goal for starting the newsletter was, and still is, to share key topics that I find interesting as I read through my industry's technical journals. With advances in media, Quanexus is now creating a lot of web content. A new feature in this edition of our newsletter is, the inclusion of interactive hyperlinks.

Cyber Insurance: One of our primary goals at Quanexus is to create reasonably secure IT environments. Every organization, whether formally or informally, has some form of risk management program. At minimum, a risk management program includes insurance. There are many types of coverages available, but a very confusing coverage is cyber-insurance. In this month's newsletter I address some of the issues with cyber-insurance. The best advice I can give anyone is work with a trusted professional who has specific experience with cyber-insurance. I've seen many happy and some sad stories as a result of not understanding what coverages were included in a policy.

CyberEdge Cyber Defense Report 2020

CyberEdge recently released its 2020 Cyberthreat Defense Report. Below are their top five takeaways from the report. They are interesting points to view the Knoxville attack through. Statistically attacks are up, they are up because they are working, and employee education is still one of the largest contributors to the criminal's success rate.

1. The bad guys are more active than ever. The percentage of organizations affected by a successful cybersecurity attack had leveled off during the previous three years, but this year it jumped from 78% to 80.7%. Not only that, for the first time ever, 35.7% of organizations experienced six or more successful attacks. The number of respondents saying that a successful attack on their organization is very likely in the coming 12 months also reached a record level.

2. Ransomware attacks and payments continue to rise. Ransomware is trending in the wrong direction: 62% of organizations were victimized by ransomware last year, up from 56% in 2018 and 55% in 2017. This rise is arguably fueled by the dramatic increase in ransomware payments. 58% of ransomware victims paid a ransom last year, up from 45% in 2019 and 38% in 2017.

3. People are the biggest problem. The greatest barriers to establishing effective defenses are: (a) lack of skilled IT security personnel and (b) low security awareness among employees. According to respondents, these are more serious than issues like too much data to analyze, lack of management support and budget.

4. But IT security is having some successes. Respondents say the adequacy of their organization's IT security capabilities has increased in all eight of the functional areas. They rated these improvements as greatest in application development and testing, identity and access management (IAM), and attack surface reduction through patch management and penetration testing.

5. Advanced security analytics and machine learning are becoming "must-haves." Implementations of advanced security analytics took off over the past year and are expected to keep rising. Organizations are showing a strong preference for IT security products that feature machine learning and other forms of AI. ~ Source: CyberEdge Group

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

Back to Basics: Multi-Factor Authentication

Multi-Factor Authentication (MFA), or Two-Factor Authentication (2FA) are systems to identify a login with more than just a username and password. You have probably experienced Multi-Factor Authentication when logging into a banking app. They may have asked for a fingerprint or a one-time password they sent you. Often these apps will only ask for a second form of authentication if you are logging in from a new location.

MFA is a way to secure your login credentials beyond just using a password. Many users choose passwords that are easy to crack, or use the same password on multiple services. If one password is compromised, they are all compromised. MFA is an extra step to secure a given login.

Multi-Factor Authentication types are broken into three categories:

Something you know: Password, Mother's Maiden Name, DOB, PIN.

Something you have: Cell Phone, USB token, RFID chip.

Something you are: Fingerprint, Retina Scan, Facial Recognition.

The most common form of MFA is an SMS text message to your phone. This extra step stops criminals from accessing an account where they have figured out the password. Also, the app or service could see this login attempt with the correct password, but not the second factor of the text message. This could prompt a notification from the service to re-set your password. Additionally, if you receive a text message and are not trying to log into your bank account, you know someone is trying to access your account. While SMS 2FA has its own set of vulnerabilities, it is still much more secure than only using a password.

We read an article last week that reinforces this theory. An Xbox user was not using MFA, and when his account got hacked, the hackers turned on MFA so that he couldn't recover his password and get back in. Click here to read the article.

This article illustrates a great point. If a service you are using has an option for MFA, but you're not using it, this opens up a huge vulnerability for the account. If the account gets hacked, the hacker can turn on MFA and make it nearly impossible to access the account again. In the case of the Xbox account, it was also tied to a bank account, so the hacker turned on MFA, locking out the original user permanently, then started buying games on the linked bank account.

Most companies will not let you back into the account if you don't have the extra point of authentication. If 2FA or MFA is an option and you're not using it, the hacker who breaks into the account will.

Back to Basics: Patching and Updating

Microsoft released two patches this week outside of their normal monthly update. These two vulnerabilities opened Microsoft users to hackers and were serious enough that the company pushed the updates out of schedule. This is the kind of story that emphasizes one of the steps in our Q-Stack. You can read the whole story on the Microsoft patches Here. Today we're going **Back to Basics with Patching and Updating.**

When we talk about patch management in the IT world, what we are really talking about are updates. Operating system and application developers both release patches to correct errors or bugs found in software, or security updates when vulnerabilities are found. Hackers and software companies are in a continuous battle for the next vulnerability.

There are many aspects of patching to think about. Servers, operating systems, and software all have patches. Any of these three components could present a vulnerability a criminal could exploit. Many systems offer automatic updates, but these do not always cover all updates. It's best to have a professional manage you company's updates for times like these when a patch comes out of schedule. Hackers are reading the IT news just like we are, so they know there's a Microsoft vulnerability that could be open for a couple weeks.

Another factor to consider is end of life software. As machines and operating systems age, there is a point where developers stop supporting software. We covered this issue last year when Microsoft decided to continue to support Windows 7, but with limitations. Users had to pay for the support and it only lasted a year as a stopgap. At some point the software does not pass the 'worth it' factor for the company, and they discontinue support. In a business setting, this is a problem you should see coming, and have a solution to well before the abandonment date.

Now that many companies have employees working from home, it's an even more important time to focus on patches and updates. If employees are using a personal computer, these devices are an unknown on the business network. Even if employees are only accessing email, and remote services, patching and updating is still a critical step to keeping that personal machine working. Educating users about the basics of IT security is always important, but now it's even more critical as many employees are using person equipment to do their job.

Business Email Compromise (BEC) Scams

A Business Email Compromise, or (BEC) for short, is a type of attack that targets company email. A hacker gains control of a business email and uses that access to request money or data.

The most recent data we have available from April to May shows a 200% rise in BEC scams, and the trend continues to go up. These types of hacking events are on the rise because they result in much higher amounts of money than a normal phishing attack. On average a BEC attack results in 100x greater profit to the criminal than a normal malware attack.

The FBI outlines five BEC attacks.
Invoice Scams: An invoice scam could originate with your company, or a vendor you work with. The criminal gains access to a professional email account and uses that access to send an invoice. Jack talks about an invoice scam we saw in the Miami Valley where the criminal simply changed the routing number, and let the business send the wire transfer as usual. Watch Jack's video here.

Account Compromise: Criminals gain access to an executive's email account and use the address book to request money from business contacts. Once criminals have access to executive email, they will watch traffic as well as read email history. Criminals can hang around in a compromised email for weeks looking for the best way to steal money.

CEO Fraud: Attackers pose as company CEO or other upper level executive, and email employees in the finance department instructing them to transfer funds to an outside account. Many employees would be hesitant to question a request from the CEO.

Legal Impersonation: Criminals pose as a law firm representing the company with confidential information. This scam is done over the phone, or email, and will typically fall at the end of the workday or week. The criminals in this scam rely on urgency, and confidentiality.

Data Theft: This tactic normally targets Human Resources departments for confidential data instead of money. Criminals will pose as other members of the company and ask for employee information or database access.

All of these methods rely heavily on quality research, and targeted social engineering. The criminals know exactly who they are impersonating. They gain access to a business email account through any number of tactics like password reuse, a separate phishing attack, malware, or missing security patches. Criminals can spend weeks inside the compromised email developing a method of best attack.

Employee education is the key to prevention, especially in Finance and HR departments. Open communication as well as quality IT Security is the best way to prevent these kinds of attacks. Employees should be encouraged to confirm requests for money, especially if they are out of the ordinary. The criminals first have to gain access to the business email in order to develop this kind of attack. A high quality layered security approach is the best defense against a criminal gaining access to a business email in the first place.

Cyber Insurance Introduction

While cyber insurance policies have been around since 1997, only recently have they become popular. Many companies have started offering cyber policies. Because of the explosive growth of this industry and the diversity in policy coverages, it can be difficult to understand what you are buying. While there are professional agents that have taken the time to understand cyber policies, there many more out there offering policies without understanding what the polices cover. I will be doing a webinar on this topic later this month, but here is a brief summary of some key areas.

Policies typically contain 4 to 5 sections. They are the declarations, insurance agreement, conditions, exclusions and definitions. Knowing what is covered is just as important as knowing what is not covered. I can share many sad stories of companies that had cyber insurance, thought they were covered, but were unable to collect.

To help understand coverage, or lack of coverage, here is a brief summary of one of those sad stories that happened here in the Miami Valley.

The owner of a small business had his email password compromised. The criminals continued to monitor his email account for a while. The criminals were able intercept an invoice that included wire instructions. The criminals modified the invoice and changed the account number for the wire transfer. The business typically pays their vendors via wire and everything looked like business as usual. The business paid (wired funds to the criminals account) the invoice as instructed. The company didn't learn of the issue until their vendor asked for payment because they had not received it. By this time, it was too late, the money was gone.

The company notified the police, and their insurance company. They were not covered for this incident because it was not considered a theft. The owner of the company authorized the payment to the criminal. The language of the policy was specific on what would be covered and not covered. Because this was an authorized payment, they were denied coverage.

I can't stress this enough, when shopping for cyber insurance, ask lots of questions and make sure you understand your coverage. It is always best to work with a professional!

Cyber Insurance Checklist

Cyber Insurance is a quickly changing market. Because this a dynamic market, not all agents stay current in the product offerings. It is important to work with an agent who has training in cyber insurance! Below is a checklist of some key factors to consider when purchasing a Cyber Insurance Policy.

Examples
To help understand possible coverage issues, consider these examples:

Wire Fraud: Will you have coverage if an email is intercepted and you wire funds to a criminal, vs. your vendor? This does not represent theft, the fact that you authorized the wire to a criminal is an authorized act. In the last blog I mentioned definitions, it is important to understand terms such as theft, phishing, etc.

Work from Home: Many companies have rushed into work from home modes. A few concerns are, do you have coverage for employees using personal devices to connect to the company network? The conditions section of a policy typically requires all systems to run currently supported operating systems, be properly patched, and current malware solutions installed. If your employees are working from home, and have been for a few months now, are you sure the systems still meet the required conditions of the insurance policy you signed?

Your Company
Does your policy cover damage done by employee owned equipment connected to your network or systems used in your work from home program?

What are the requirements to be eligible for coverage? What organizational measures must you have in place to qualify for the policy? Examples: Security Awareness Training, Incident Response Plan, or an Information Security Policy.

What requirements must be followed for a claim to be covered? Examples: Time frame to report an incident, customers must be notified of an incident, or insurer must be involved in ransomware negotiations.

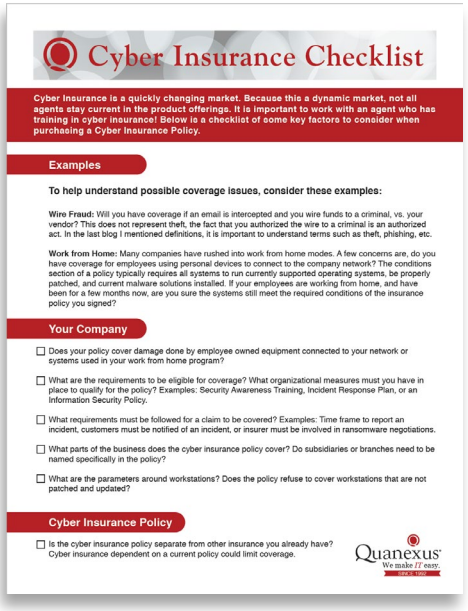
What parts of the business does the cyber insurance policy cover? Do subsidiaries or branches need to be named specifically in the policy?

What are the parameters around workstations? Does the policy refuse to cover workstations that are not patched and updated?

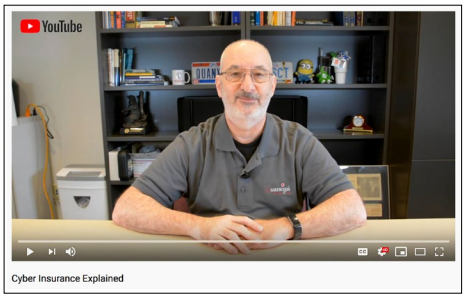
Cyber Insurance Policy
Is the cyber insurance policy separate from other insurance you already have? Cyber insurance dependent on a current policy could limit coverage.

Is there a waiting period for policy to take effect after contract is signed?
What types of data breaches are covered under the policy? Are there parameters around how the data was stolen for the policy to cover loss?

What is covered in a Phishing attack? Some policies have specific language around social engineering attacks, what is covered, and financial limits to these types of attacks.



Click Here for Complete Cyber Insurance Checklist



Click Here for Jack's Video on Cyber Insurance

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