Q-News

July 2021

A Word from Jack

The cyber world just continues to get more challenging. I've recently had a few astonishing conversations about how a company can protect themselves against the impact of a cyberattack. There is a big misconception that cyber insurance is an adequate protection. In this edition, we address cyber insurance, and what you can expect to see at your next insurance renewal (more stringent underwriting, and higher premiums).

The best way to avoid an attack is to do the right things. By doing the right things you make it hard for the criminal to turn you into a victim. There are two key incidents a company may experience. The first is a loss of a critical function and the second is theft or loss of client or company data. When you think about how to protect your organization, consider the following: What are the critical functions the organization performs, how are the critical functions protected, and have plans to recover and resume critical functions. For data protection, it is important to know where your data is (internal and client), how it is protected, and what notification processes are required, based on the states and industries you operate. Quanexus is an IT services organization with a strong background in risk management.

SolarWinds Under Attack Again

SolarWinds products are the focus of a new attack discovered by Microsoft.

The software provider, who suffered a supply chain attack that compromised federal agencies and Fortune 500 companies last year, issued a new emergency patch Friday. SolarWinds published an advisory along with a hotfix for the Serv-U product line. Microsoft spotted the vulnerability being exploited in the wild.

"Microsoft has provided evidence of limited, targeted customer impact, though SolarWinds does not currently have an estimate of how many customers may be directly affected by the vulnerability," company officials wrote. "SolarWinds is unaware of the identity of the potentially affected customers."

"The vulnerability exists in the latest Serv-U version 15.2.3 HF1 released May 5, 2021, and all prior versions," said SolarWinds. "A threat actor who successfully exploited this vulnerability could run arbitrary code with privileges. An attacker could then install programs; view, change, or delete data; or run programs on the affected system."

The vulnerability affects Serv-U Managed File Transfer, Serv-U Secure FTP, and the Serv-U Gateway. In their advisory SolarWinds says they believe only the Serv-U tools are affected, and that the attacks were focused on "a limited, targeted set of customers."

SolarWinds has been the target of three attacks over the past year that we know about. The large Orion attack in December, that targeted nine US agencies, gained large attention and was designated as a nation state attack. A second attack occurred in March when hackers used SolarWinds web-facing servers to spread malware to users. In their statement, the software company said the current attack is not related to the others. Customers should continue to check the advisory page for updates and permanent patches.

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

Cyber Insurance – More Expensive and Harder to Get

Getting cyber insurance used to be very easy for small and medium size companies. A few years ago, there was virtually very little or no serious underwriting activity and applications were just being accepted. With all the big breaches in the world and small companies constantly being hit (typically by ransomware), insurance companies are tightening up their underwriting requirements and appropriately pricing risk.

We often get requests from clients to assist with completing their cyber insurance applications. I always caution clients to be forthcoming with information. Insurance applications are legal documents, and it is fraud to provide false information. Additionally, if you provide false information on your application, there may be grounds for an insurance company to deny your claim. In the last few years, regardless of how the applications were answered, the client was always granted the insurance. I never saw any company denied coverage.

We are now starting to see applications asking for specific IT security and privacy controls. They are asking for details on products that are being used, and what third parties have access to the network, including outside support vendors. On a few applications we have seen specific required controls that must be implemented to be eligible for cyber insurance. The most common required control we see is the requirement for multi-factor authentication (MFA). Specifically, MFA is being required for the following:

- **Web access to email.**
- **User remote access to network.**
- **Admin access to servers and workstations (no local admin permitted).**
- **Third parties including service providers.**
- **Network backup environment.**

We suggest, as time and budget permits, every organization should be implementing MFA on as many systems as possible.

State and Local Cybersecurity

We have seen the perfect storm of cybercrime over the last year. The pandemic forced many employees to work remotely and in less secure environments. Staffing shortages and long hours meant healthcare workers were more vulnerable to phishing attacks. Lately, we've seen large corporations victimized as well as the IT infrastructure used by fortune 500 companies and the Federal Government.

State and local governments sometimes struggle the most to keep up-to-date with a cybersecurity framework. Often, city governments do not have the staffing or budget to maintain current supported hardware, not to mention proper employee education on IT best practices.

States are recognizing the threat and responding. So far in 2021, at least 44 states and Puerto Rico have introduced more than 250 bills or resolutions that deal with cybersecurity. The legislation is focused primarily on the following areas:

- **Requiring government agencies to implement cybersecurity training, to set up and follow formal security policies, standards and practices, and to plan for and test how to respond to a security incident.**
- **Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance.**
- **Creating task forces, councils or commissions to study or advise on cybersecurity issues.**
- **Supporting programs or incentives for cybersecurity training and education.**

Coverage in the news of attacks like the local water treatment plant in Florida, demonstrate how utilities can be impacted. Additionally, the attack and subsequent shut down of Colonial Pipeline showed how a wrinkle in a private supply chain can become a national concern. The Federal Government reacted to the pipeline shutdown with new regulations on pipeline owners and operators, but they also introduced new cybersecurity regulations on businesses who operate the power grid at the same time.

We are seeing renewed concern for IT security at every level of government. The pandemic may have worsened the threat of attack, but it also emphasized a long standing problem.

Pipeline Attack Follow-Up

The ransomware attack and subsequent shutdown of Colonial Pipeline captured the interest of the government and the general public a few weeks ago. Previously the government took a hands-off approach to pipeline security, leaving the risk assessment in the hands of the corporation. That changed Thursday when the TSA released new cybersecurity regulations for the pipeline sector.

The new regulations require critical pipeline owners and operators to report confirmed and potential attacks, as well as keep a 24-hour cyber security coordinator on staff.

"The cybersecurity landscape is constantly evolving, and we must adapt to address new and emerging threats," Secretary of Homeland Security, Alejandro Mayorkas said Thursday in a statement. "The recent ransomware attack on a major petroleum pipeline demonstrates that the cybersecurity of pipeline systems is critical to our homeland security."

The security directive will also require pipeline companies to review current security practices and identify any gaps. Companies have to report the results to the US Cybersecurity and Infrastructure Security Agency (CISA) within 30 days.

The Colonial Pipeline shutdown highlighted the vulnerability of critical infrastructure, and their reliance on IT services. Colonial Pipeline points out the hackers were not able to get into the technology that actually operates the pipeline, but the intended result of a shutdown and public panic occurred, nonetheless. We have seen cyberattacks on hospitals, police departments, city governments, and schools, but this was the first event that crossed over to the general consciousness. The SolarWinds breach a couple months ago piqued the attention of business owners, and made some start thinking differently about the scope of a cyber event. This ransomware attack had a similar effect on the public. Images of lines at gas stations and citizens filling up any container available with fuel changed the narrative on cyber security.

The attack also emphasized the discussion of cyber insurers response to ransomware. Following the peak of ransomware payouts in Q3 of 2020, some insurers dropped ransomware coverage from their policies A report from the Government Accountability Office said, in part, "insurer appetite and capacity for underwriting cyber risk has contracted more recently, especially in certain high-risk industry sectors."

Ohio Personal Privacy Act

With the increase in cybercrime, and level of sophistication hackers are using, states are looking to new legislation to protect consumers and businesses. Last week, state representatives introduced a bill that would give Ohioans more control over their personal data and protect Ohio businesses from litigation. The Ohio Personal Privacy Act would be the first in the country to provide a safe harbor for businesses who can prove they have nationally recognized data protection in place.

The bill is focused on businesses with a gross revenue over $25 million and businesses who control or process the personal data of over 100,000 Ohio residents in a calendar year. The bill would also apply to smaller businesses if 50% of their revenue comes from the sale of personal data, or they control more than 25,000 residents' data.

The bill does not cover data already covered by HIPAA, data subject to Children's Online Privacy Protection, financial data, higher educational institutions, business-to-business transactions, or employee data.

The bill would require businesses to inform consumers of the personal data being collected, and how it would be used. It would give consumers the ability to view the data collected on them, opt out of their data being sold, or delete the personal data altogether.

"In the absence of a comprehensive federal policy on the collection and use of personal information, Ohio has an opportunity to position itself as a technology leader on multiple fronts," commented Rep. Carfagna. "House Bill 376 will balance reasonable privacy standards to protect Ohioans with less bureaucracy and regulation on businesses. I'm thrilled to work with my joint-sponsor State Rep. Thomas Hall, Lt. Governor Husted and Attorney General Yost to create what we believe will serve as a national model for data privacy."

The bill also provides a defense for businesses. If a company follows the privacy framework outlined by National Institute of Standards and Technology (NIST), they are protected against legal action through the proposed bill. This is the first bill of its kind that takes the liability off the business if they can prove they were following best practices when they suffer a breach.

How Backups Combat Ransomware

Ransomware attacks are not slowing down. A critical step in the Q-Stack IT infrastructure is the backup. We protect data with many layers of defenses, but we also back up the data to recover from a ransomware attack or hardware failure.

The first step is to have a backup plan. There are different backup solutions for different kinds of data. Not all data is the same, and not all data should be backed up the same. When exploring backup solutions, consider how sensitive the data is, how quickly it will need to be recovered, and how much data will need to be recovered.

In the Colonial Pipeline attack, Colonial paid the ransom very quickly, only to find out the decryption key worked so slowly they were able to restore from backups faster. A complete backup solution that includes cloud, local, and air gap provides redundancy as well as recoverability.

Cloud backups store the data off site and can work very well for some types of data. The compromise with cloud solutions is they can be slow for large amounts of data. Cloud backups also have a built-in risk in the event the provider suffers a breach. Because of this inherent risk, many industries choose to keep their most sensitive data off of cloud solutions, and on backups not even connected to the internet. Watch our Podcast on Air Gap Backups Here.

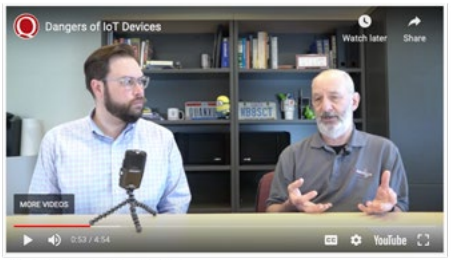
Local backups are inexpensive and can recover large amounts of data quickly. However, local backups are subject to fire or water damage if the building suffers an emergency. Additionally, local backups can be hacked, erased, or the data stolen if they are connected to the internet or the business network.

A final step is to make sure the data is recoverable before an incident. In many cases the first time a business attempts to recover data is after an attack. An IT provider can simulate backup recovery to confirm the backups are properly working and validate the backup process.

Backup solutions and combating criminals is becoming more difficult for small and medium sized businesses. It's important to have a plan, and understand the data being guarded. If your business needs help developing a backup solution, please reach out and see if our solutions might be a good fit for your organization.

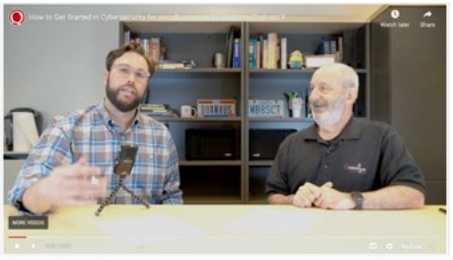
Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss IoT Devices, and Getting Started in Cybersecurity!



Dangers of IoT Devices

Click Here for Podcast- Dangers of IoT Devices


How to Get Started in Cybersecurity - Quick Wins

Click Here for Podcast- Getting Started in Cybersecurity

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