IT Strategy Brief

ISSUE 12 | VOL 5 | December 2019

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:

NJ County and City Hit by Ryuk Ransomware Attacks

On November 9 and November 12, the computer systems of Union County and the city of Dover, respectively, were both targeted by a ransomware infection. Details in either case are still limited at this time, however, the attacks affected the internal networks of both governments to some degree before service was restored. The public agencies were able to regulate the damage with external help from IT service firms.

Union County and Dover, Morris County, NJ Cyberattacks

The first attack occurred on a Saturday, so the Dover municipal government was not aware of the infection until the following Tuesday – the same day Union County's network was hit, though they were able to respond to the incident much more quickly as it happened on a weekday. Both experienced a slowdown in their internal email servers, while the latter also saw some website assets affected. Statements from both governments claim that no data was lost and most services have been restored as of this writing.

Hundreds of Cities Infected with Ransomware

These cyber incidents follow a rapidly growing trend of public institutions being targeted by ransomware attacks. Hospitals, police departments and now municipal and state agencies are increasingly victimized by malware infections that encrypt databases and demand a payment to unlock those files. Baltimore, Philadelphia, and several cities throughout New Jersey are only a few of the many that have been assailed by malware infections.

These developments have not gone unnoticed and have been addressed at multiple levels of government. However, despite the efforts by local and federal agencies, ransomware continues to affect cities, states and private businesses across the country. This is because hackers know what techniques to use against overextended networks like those of public institutions and SMBs, including social engineering and exploiting popular applications like the Office 365 suite.

Continued on page 2...

What our clients are saying: Pee Jay's Fresh Fruit

"SWK's response time has been great. There have been many times we've submitted an email with an issue and received a call back within 5 minutes. Very impressive!

Shay always goes above and beyond. Earlier this year we had an email issue with an outside vendor, and he got involved - even contacted the outside vendor himself - and made sure to stay on top of the situation. When I put it on the back burner, he still was working on it and even though it was not a quick fix, he helped resolve it!

Our biggest benefit by working with SWK is that we have confidence that if any IT issues arise, they will be dealt with quickly. If it's not a quick fix, it will be thoroughly examined and diligently worked on until it's completed."

Anthony D'Agostino
Pee Jay's Fresh Fruit

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner!

Last Month's Contest Winner:

Cindy Daley
Friendly Planet Travel

Please complete our brief survey in order to be placed in the running to win this month's gift card prize!

1. What do you like most about our services?

2. Tell us about a specific experience with us that you were happy with.

3. What are the biggest benefits you've received or experienced since hiring us?

4. What can we improve?

Email Jon Stiles (jonathan.stiles@swktech.com) with your responses
OR
Fill out our online form: http://bit.ly/nwsnews-survey before **Dec 31st** to get your name in the hat.

You could win a $25 Gift Card!

NJ County and City Hit by Ryuk Ransomware Attacks

Continued from page 1…

What is Ryuk and Why You Should Be Worried About It
Another worrying trend among many recent ransomware attacks – including the majority of reported incidents in NJ – is that the same type of malware was used in most cases: Ryuk. The profile of Ryuk makes it a huge concern, as researchers note that it is deployed almost exclusively for targeted attacks with critical files encrypted and larger ransoms demanded. Additionally (or perhaps, appropriately), this type of ransomware can be employed through several different methods and channels, and can delete all evidence of its presence.

This last factor reinforces the theory that many of the latest malware samples have something in common. It could mean that cybercriminals are copying each other, though it could also mean that they are actively sharing data and methodologies or that it could even be the same group carrying out all of these attacks. The nature of the Dark Web makes it difficult, though not impossible, to consistently track down culprits.

NJ is a Prime Cybercrime Target
Of the now eight reported ransomware attacks in NJ, Ryuk was used in three – along with the Dover and Union County attacks, the Cherry Hill School District was also a victim of a breach by the same malware type. Besides these examples, all but the attack against Newark – which was hit by the similar SamSam virus - were attributed to unknown actors. The reality is that many (if not most) departments and businesses in New Jersey and nearby metropolitan areas do not disclose when they are hacked.

Ryuk has largely replaced SamSam as the ransomware of choice, but given the similar tactics between the two, the former's rise was likely enabled by the lack of actionable information on the latter. This leads to victims falling for the same scams as those before them, as the data, knowledge and experience needed to spot infection vectors and respond to locked files is lacking.

Learn How to Defend Against Ransomware
SWK Technologies has firsthand experience with helping clients deal with ransomware (see how we helped Continental Food and Beverage, distributors of Inca Kola, save their files). We can provide you with tools and expertise to help you combat this growing threat and prepare your business to defend your network against malware infections.

Download our free Business Guide to Ransomware ebook to learn more about what to expect and you can begin protecting yourself against what's out there.

Creating a Sense of Shared Cybersecurity

In cybersecurity, people are your weakest link and your best defense – you have probably heard us say this more than once. Just as your business cannot run without people, neither can you network security. Any cybersecurity plan is twofold, in that you must prevent employees from exposing you to cyber risks while empowering them to detect and respond to potential threats.

Creating and enforcing a security culture takes work, but is increasingly necessary. A majority of SMBs have been targeted by hackers, and as the world becomes more connected, so too will your business. Anyone who uses a computer, smartphone or tablet accessible to your network will have a cybersecurity role, and thus bear responsibility for your network security.

Here are a few steps that will help you establish a shared sense of cybersecurity in your business:

Data Integrity and Compliance
Your first cybersecurity concern should always be data protection. Network breaches, credential leaks and the theft of critical and personal information can and will have serious consequences for your business. The most impactful will be the monetary losses that can result from the breach of consumer trust and data security regulations, as well as expenses for resolving your security vulnerabilities.

Data protection best practices range from basic solutions like password security education, to implementing multi-factor authentication and other services that add an extra layer of security for your network users. These procedures reinforce for users both the importance of their individual practices, AND the sensitive nature of the data their credentials unlock.

Cloud Networks and Real-time Access
Most devices and applications are moving towards some level of cloud capability – if you are using Office 365 on your desktop or a Verizon smartphone, then your data is already exposed to the cloud. User security only becomes that much more important when using digital platforms, and is inherently an exercise in shared cybersecurity. However, just as with every Internet advancement since the 90's, cloud security just requires extra vigilance until the added steps become second nature for system users.

This, of course, requires that you actually educate your employees on what NOT to do – and what might happen if they do it anyway. This includes all levels of your company, as managers and executives are often the biggest targets to exploit for human error. Remind your users that they are not just accessing hardware whenever they press a key or touch a screen, but a communications node connected to dozens, hundreds or thousands of other endpoints.

Continued on page 4...

Shiny gadget of the month: Sonos Move Portable Speaker

Sonos, who has been regarded as one of the top speaker producers announced this year a first for them… a portable speaker. While obviously the concept of a portable speaker is nothing new Sonos had never created one.

They call it, Sonos Move, and it packs many of the features that other high end portable speakers have like being weather resistant, high quality sound, and shock resistant, but they've also added some new features. The most notable is the tweak they did to their Trueplay calibration system that allows the speaker to automatically calibrate for the best possible sound. It was demoed at a preview event by placing it on a bookshelf (one of the worst spots for it due to the reverberations of the space) and after a few seconds it adjusted to compensate for the echoes.

The battery is supposed to last 10 hours on a charge and can easily be kept charged by placing on its wireless ring base. Setup is simple and consists of just plugging in the device, downloading the app, and linking it up with the speaker. It also comes with Google Assistant and Amazon Alexa built right in so you have your voice assistants ready to go without an extra connection to a device being required.

These features seem like they could be great for anyone who enjoys their music (and who doesn't), especially if they already have Sonos speakers in their home because it will connect right in with the rest of their Sonos sound system. Even if they don't, having a top of the line speaker that is portable brings it own advantages. Now you can bring your tunes outside, follow you around to any room in your home, out to a tailgate, or even to the beach.

The only real drawback for some might be the price which comes in at $399. Though for anyone who is familiar with high end speakers this is not extreme. It certainly seems like a really cool gadget for the holidays and the AI audio calibration is intriguing. You can find out more on their site www.sonos.com/en-us/shop/move.html. What do you think of Sonos' latest speaker?

States Impose Greater Data Privacy Standards

New York and California recently passed expanded data privacy regulations that some observers say move the US closer to the breach reporting standards the GDPR brought to the European Union. Though it remains to be seen whether this approach actually spreads to other states, it does reflect the increasingly popular opinion of both experts and the general public that more data custody laws are required.

A recent article in the Harvard Business Review goes a step further and calls for a globally accepted standard of breach reporting. As the authors point out, countries besides the USA have already adopted more comprehensive, collaborative and universal disclosure obligations which enable organizations to share relevant data on cyber attacks. With these precedents having been established, it seems inevitable that some type of universal reporting standard will be passed in the near future.

Here are the most important to know about the new regulations and how they may affect your business:

California Consumers Privacy Act (CCPA) - American GDPR?
The CCPA was passed in 2018, but compliance and enforcement does not go into effect until January 2020. With stricter boundaries for personal data usage and steeper fines for violating consumer privacy under these terms, it has been compared to the EU's General Data Protection Regulation in purpose and scope. In the latter case, given the size of California and its economy, its impact is expected to extend well past state lines with remote sellers and residents increasing dependent on interstate commerce.

New York SHIELD Act
Earlier this year the Stop Hacks and Improve Electronic Data Security Handling Act (**SHIELD Act**) was passed to improve data security for consumers due to the increased number of cyberattacks going on in the country. For companies that maintain or process New York residents' personal information (PI) they will need to comply with the new changes. Three new categories of data security and breach notification requirements were introduced:

- Financial account and payment card numbers that "could be used to access an individual's financial account without additional identifying information, security code, access code, or password"
- Biometric information, "meaning data generated by electronic measurements of an individual's unique physical characteristics"
- A "user name or email address in combination with a password or security question and answer that would permit access to an online account."

The goal is to broaden what is considered Private Information within New York's general business law and state technology law. These increased data breach reporting requirements will go into effect on March 21, 2020. In order to meet these requirements companies will have to evaluate their data security programs to determine if they will need to increase the level of security going forward.

Most Americans Want More Data Protection Regulations
75 percent of American respondents told a Pew research group that they want to see the federal government do more to protect their data - specifically from businesses. Almost 80 percent said they have no confidence "… companies will take responsibility when they misuse consumer data." The report makes clear three things: US citizens do not trust commercial interests with personal information, they feel no control over their personal information, and they believe that laws should be passed that puts that control back in their hands.

While some of the most flagrant abuses of customer data have been penalized, many have criticized the government – including voices *within* the government – saying that it has not been enough. This is exactly why states like California and New York have begun passing their own data privacy laws, and given the influence both these examples have on the national and international economies, the standards they apply are likely to spread.

Get Ahead of Compliance with Data Security Best Practice
Growing popular favor means that a comprehensive federal data privacy regulation is bound to appear sooner rather than later. As new laws and regulations for compliance are introduced to protect user data the task can become more and more daunting for SMBs. Don't let compliance needs become an added stress to your business. For starters you can read our Cybersecurity Tips eBook and for more in-depth answers you can contact us to learn about the options you have to be protected and make sure you have your compliance needs fulfilled.

Gift Card Trivia!

This month's question is:

According to the survey in the article revealed that nearly ____% of Americans have either fallen victim or know someone who has fallen victim to robocalling in 2019. (Hint: The answer is in this newsletter.)

a. 48%
b. 24%
c. 74%
d. 35%

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **December 31st**, in order to be placed in the running for this month's gift card prize!

We can help you with:

- Complete network management and support
- Troubleshooting and problem solving on all PCs and Macs
- Cloud services and virtualization
- Hardware installation and support
- Virus / spyware removal and protection
- Security solutions
- Employee awareness training
- VPN (Virtual Private Networks)
- Remote access / Mobile computing
- Server installations and upgrades
- Spam filtering
- Hosted email
- Web content filtering
- System backups, on-site and off-site
- Help desk

Contact us

Give us a call for more information about our services and products.

SWK Technologies, Inc.
South Jersey
650 Grove Road, Suite 106
West Deptford, NJ 08066

North Jersey
120 Eagle Rock Ave., Suite 330
East Hanover, NJ 07936

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at
www.swknetworkservices.com

SWK NETWORK SERVICES

Creating a Sense of Shared Cybersecurity

Continued from page 2…

Cyber Risk Assessment and Employee Cybersecurity Training
As everything above shows, training is the first on most lists of cybersecurity strategies, but you cannot force everyone in your business to become an IT expert. Besides the sheer amount of instruction needed to turn every amateur into a security specialist, cyber stress can cause as much damage as a data breach (because it can lead to one anyway). Any user security improvement plan should be conceptualized and deployed according to a risk-based approach.

Assessing cyber risk includes reviewing where you may be vulnerable (ERP software, industrial systems, business application suites, etc.), and calculating the number of endpoints and users that may be exposed in those areas. From here, you can design and schedule training programs by business unit, with content based on role and credential access to critical systems. Most importantly, you can help your employees understand how their security approach affects their personal lives as well – and how improving practices at work secures their devices at home as well.

Get Your Employees the Tools to Protect Your Business
There is no avoiding the fact that SMBs these days require a culture of cybersecurity, but ensuring that your employees understand their part means providing the tools that allow them to do so. SWK has the resources available to help you teach your people how to protect themselves and your business from all threats.

Download the Cybersecurity Toolkit for SMBs e-book to learn how to create a culture of shared network security for your business. software and the other for entertainment.

Tips for staying safe this holiday season

In November, McAfee a cybersecurity company, released their findings from a recent survey focused on holiday scams. The survey revealed that nearly half (48%) of Americans have either fallen victim or know someone who has fallen victim to robocalling in 2019. The use of robocalling has grown in recent years and this statistic makes it one to watch out for this holiday season. This is not the only scam to look out for though. Email phishing and text phishing (41% and 35% respectively) are still popular methods being used by hackers.

While these scams may not be multi-million dollar breaches you read about in the news 74% said that they lost more than $100 and 30% lost more than $500. With a growing number of stolen credentials being made available for cybercriminals to purchase on the dark web it only increases the likelihood that these numbers will increase this year. The troubling fact is that while many people may be aware of the threat over the holidays, they won't actually do anything about it to protect themselves.

The Cybersecurity and Infrastructure Security Agency (CISA) issued a statement and encourages users to be aware of potential holiday scams and malicious cyber campaigns, particularly when browsing or shopping online. Cyber actors may send emails and ecards containing malicious links or attachments infected with malware or may send spoofed emails requesting support for fraudulent charities or causes.

CISA encourages users to remain vigilant and take the following precautions:

- Avoid clicking on links in unsolicited emails and be wary of email attachments (see Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams).
- Use caution when shopping online (see Shopping Safely Online).
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.

In addition to these precautions we recommend:

- Never reusing passwords and always using a strong password (capital letters, numbers, symbols all mixed in).
- If you get an email from someone you know that appears suspicious always check with them before acting on anything the email requests.
- Using two-factor authentication when possible

The holiday season is meant to be spent together with loved ones, not dealing with the stress of recovering from a hacker. Keep these tips in mind this holiday season for a safe and happy end of the year. Remember, if you are ever suspicious of anything you can always reach out to the SWK team for help, or if you are looking for more ways to protect you and your employees, contact us to learn about the solutions we have that will help.