IT Strategy Brief

ISSUE 1 | VOL 6 | January 2020

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

9 Cybersecurity Trends to Watch in 2020

A new year means it is time to deal with old and new cyber threats. 2020 will bring many technological developments, but expert opinions vary on which of these will be leveraged by hackers, if any. Cybercriminal practice has been to rely on different versions of the same technique until enough victims become wise to the vulnerabilities that allow it.

Yet the new decade may very well be a time of escalating cyber attack brought on the proliferation of new technology. Additionally (or maybe consequently), public demand for greater data security controls is creating a greater incentive for business to put more effort into their cyber defense strategy.

Here are nine cybersecurity trends to keep an eye on in 2020:

1. Personal Information and Data Privacy
California's CCPA and New York's SHIELD Act have made waves in the data privacy discussion, as each of these laws emulates the comprehensive protections of the EU's GDPR. Their passage comes as momentum is building among politicians and the public to pressure businesses to put more effort into securing personal data. This conservation is likely to heat up further in 2020.

2. AI Bias, Deepfakes, and Machine Learning in Cybersecurity
There are many predictions on how AI will be used for either cyber attack or defense, but the real-world applications are still technically theoretical, with only a few shocking but rare (proven) examples. Ironically, human influence keeps artificial intelligence's ability to execute imperfect by leading to AI bias, and both hackers and security professionals will spend the next year learning how to overcome this.

3. Automated Systems and Robotics Security
Manufacturing and industrial control systems have always represented a supply chain vulnerability, but the introduction of robotics automation may bring new security gaps to address. Hackers may exploit diminishing human oversight to silently breach these automated networks and attack central command points in the production space.

4. Open Connections – 5G, IoT and Cloud Networks
The implementation of the fifth generation of wireless networks (AKA 5G) has raised alarm bells in cybersecurity circles. Many of these warnings reinforce the concerns already present about the faster and more open connectivity of Internet of Things (IoT) and "As-a-service" cloud-capable devices. However, 5G networks will potentially expand the scale of the threat with an attack surface that includes every connected device in your vicinity.

5. Mobile Device Security Threats
5G also presents new dangers for smartphones and tablets, as the speed at which this technology is being deployed may outpace the ability to secure mobile endpoints. A growing concern is that hackers will uncover one or more critical native mobile device vulnerabilities and break into otherwise protected networks at a greater rate in 2020.

Continued on page...2

What our clients are saying: Parts Life, Inc.

"Help is always available at SWK Technologies when you need it. Their staff is friendly and courteous. They get back to you promptly and stay on top of your issue. It's a pleasure working with a company that cares."

Meredee Parsons
Parts Life, Inc.

PARTS LIFE, INC.

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Nishita Desai
Torrent Pharma, Inc.

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?

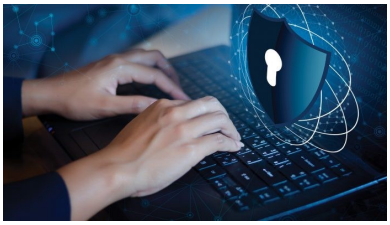
4. What can we improve?

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

You could win a $25 Gift Card!

9 Cybersecurity Trends to Watch in 2020

Continued from page 1…



6. Targeted Ransomware
Ransomware is certainly not new, but trends indicate veteran hacker groups are refining their tactics as well as their technology when it comes to fil encryption. Ryuk, SamSam and other newer file-locking malware types reflect the evolution of ransom schemes to a targeted model that requires deep research, profiling and creativity in execution.

7. Cyber Cold War
Against a backdrop of rising global tensions, some cybersecurity professionals worry that these emerging technologies will help escalate a new Cold War, but one that revolves around a cyber attack. Cyber warfare provides many political and tangible advantages, and can cause significant harm to an enemy while still being cost-effective for the aggressor.

8. Cybersecurity Collaboration and Shared Responsibility
By now, everyone has heard that cybersecurity is a shared responsibility, and this approach will only become more integral to future security strategies. CCPA, SHIELD, and whatever comes after will also reinforce a building momentum towards organizational and vendor security across several industries.

9. Hackers Will Rely on the Same Tricks for Now
Despite all of the above, the biggest trend being observed right now is that hackers are still refining existing techniques instead of immediately adopting new ones. Ransomware, phishing and more common attack methods remain the preferred choice of most cybercriminals, for now.

Protect Your Business with SMB Security Best Practices
Emerging technologies will still be more complex, harder to obtain and easier to track than the proven tools hackers already had in their arsenal in 2019. Until the resources available provide more reward than risk, cybercrime will continue to focus on exploiting human error for at least the beginning of 2020.

Download our Essential Cybersecurity Toolkit for SMBs e-book to discover the best practices that will keep your business protected in the new year.

Wawa Breach Leads to Malware, Wire Fraud and Lawsuits

On December 19, 2019, Wawa CEO Chris Gheysens released an open letter informing customers of the convenience store chain that their data may have been exposed. Gheysens revealed that Wawa had discovered a malware infection on their servers on December 10 and managed to contain it by December 12. The infection occurred sometime before March 4 when their network had been breached by a yet to be revealed attacker.

Wawa Data Breach and Server Malware Infection
The malware affected payment processing servers for approximately 850 store locations for the eight months after the initial breach, though Wawa's investigators found most fraudulent activity occurred after April 22, 2019. According to Gheysens, the infection may have exposed payment card information (credit and debit numbers, cardholder names and expiration dates) at in-store and gas terminals throughout every location affected. No other personal information seems to have been leaked, and no ATMs at the locations were found to be affected.

The letter also informed potentially affected customers that Wawa had set up a deal with Experian to provide identity protection services at no extra cost. Customers can use activation code "**4H2H3T9H6**" to register for identity theft protection and credit monitoring by visiting **www.experianidworks.com/credit** or by contacting Experian at **1-844-386-9559**.

Lawsuit Filed Against Wawa for Negligence and Noncompliance
Though Gheysens' letter claims that no evidence had yet been found (at the time of writing) of any unauthorized use of the leaked data, a class action lawsuit was filed shortly after against Wawa by a group of affected customers. The lead plaintiff, Tabitha Hans-Arroyo of Woodbury Heights, NJ, says that she frequently used her credit card at Wawa locations and became the victim of a fraudulent charge using her information.

Not long after the breached was announced, Hans-Arroyo received a notification that her card had been used in a $2500 online purchase from Walmart – she claims this was not her's and that her credit information was compromised. Now, Hans-Arroyo and the other plaintiffs are suing Wawa for damages "caused by Wawa's negligence, breach of contract and violations of state consumer protection statutes," as outlined in the suit documents.

Hackers Are Always Out There – Protect Yourself from Malware
What happened to Wawa can happen to anyone. Hackers are always searching for ways around static network defenses to silently infect your system while you are not looking. With 82,000 malware threats released every day, you must stay on top of your cybersecurity – especially when breaches like Wawa's can expose data that can later be used to hack YOU.

Download our report to learn the Top 10 Ways Hackers Get Around Your Firewall and discover how you can prepare for inevitable cyber threats.

Shiny gadget of the month: Dabby

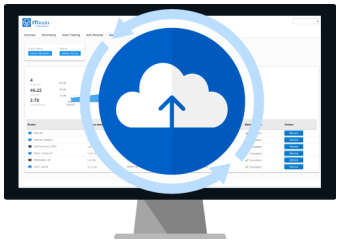
It is now the year 2020, technology is reaching new levels and most of us have a variety of devices we use for streaming TV and movies in our homes. That means you probably have a couple boxes, dongles, etc. you use to stream content on your TV's. On top of that there are now so many streaming services and subscriptions that it can be hard to find where your favorite show or movie is to watch and you have to flip between all these apps to try and find it. This is where Dabby comes in…

Dabby, which debuted at the CES show this month, is a little home entertainment hub that wants to simplify your life. It looks a little like a tablet, (or Echo Show) but combines the features with that of a Roku or Apple TV. The real draw of this gadget is that it will use the power of AI to take all your subscription streaming services along with all the free content out there on the web and combine them into a superpowered AI search for what you want to watch. That's right, you just say "Hey Dabby, watch The Witcher" and boom you have it right there, or "Hey Dabby, watch the scene where Thanos snaps his fingers'" and it will find it. If you don't have access to something it can even give options to rent it right there.

Beyond the search capabilities Dabby has some other cool features. For instance, you can take the device and carry it from room to room and through the use of the sensors you can continue watching in the next room seamlessly. You can even use it as a standalone device to watch with if you wanted. If you have a friend with a Dabby you can set it up to stream simultaneously with that friend and have a live video feed between you and your friend on the Dabby screen while the content plays on the TV, which could be cool if you wanted to watch a show or sporting event with a friend who can't otherwise be there. If you're not using it, it can even function as a digital picture frame too.

All these new tech features sound really cool, but it comes at a bit of a steep price of $400. The idea behind it is intriguing, and hopefully the features work well, especially the AI search, but since this has yet to be released only time will tell. You can pre-order now and there is an expected ship date of April 2020. You can check it out for yourself on their website www.heydabby.com and they have some little videos to show more of it off. What do you think? Would you be willing to give it a try?

Business Continuity with Cloud-Hosted Data Backups



Disasters can strike at any time, bringing your business to a grinding halt and cutting into your revenue. Implementing a business continuity plan will help you secure your valuable data by backing it up in case of network outage. However, data backup can become too complicated for internal IT departments to manage. Should you get hit by a disaster or a breach, a lack of proper file backup could mean the end of your business — all the more reason to integrate cloud hosting in your data backup strategies.

Here are four reasons why hosting your data backups in the cloud is better than internal storage:

Cloud Networks Allow Better Uptime
Backing up to an internal drive or an external hard drive won't completely secure data. If someone steals your device, you instantly lose the backup it contains. Natural disasters, cybercrime, or man-made errors will also likely destroy your backups. As a result, your company could face expensive downtime.

With cloud-hosted backup, however, things are different. The entire purpose of a cloud backup is to make sure your data is available when you need it. Top cloud service providers will offer redundancy, which means they will make a backup of your backups. This increases uptime and ensures optimum levels of data availability.

Fast Resource Provisioning Through IaaS
When backups are being implemented, spikes in user activity or cloud environment accessibility can slow down a website or other running systems. This is where a cloud hosting provider comes in handy. By closely monitoring user activities, providers can see spikes either before or as they are happening. The provider will provision more resources and virtual machines to manage the influx of users. This type of flexibility is particularly useful when data backups are in process.

Back Up Data More Frequently
Most companies work on files and update information throughout the day, so it's important to have a real-time backup plan ready in case an unexpected disaster occurs. When you back up data in the cloud, you will no longer have to worry about managing the frequency of your backups.

Most cloud-hosted providers offer round-the-clock or other fixed backup frequencies, while others let you set your own backup schedule. Some of the services offered by these providers will back up files as you make changes, so you'll know that the very latest version of files and data are always backed up.

Distributed Cloud Infrastructure with Real-time Server Access
Cloud-hosted backup means the delivery of data backup to users all over the world. Selecting the right type of cloud hosting partner is equally as important as having a cloud backup plan in the first place. If international users are trying to access database or download applications through your business website, latency will become a factor — the closer the user is to the data, the faster they'll be able to access information.

Let Secure Cloud Hosting by SWK Back Up Your Data
Businesses everywhere are utilizing cloud backup solutions, so don't be the one left behind. Gain real-time data security, faster deployment times and unlimited scalability when you migrate to the cloud with SWK Technologies.

Learn more about SWK's Secure Cloud Hosting solution and give us a call today to discover how to start your cloud migration.

Gift Card Trivia!

This month's question is:

What other NJ public institution was hit by a ransomware attack a week before the Meridian Health attack? (Hint: The answer is in this newsletter.)

a. NJ Transit
b. Hanover Police
c. Livingston School District
d. None

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **January 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

Biggest NJ Healthcare Network Hit by Ransomware

Yet another New Jersey healthcare provider has confirmed that their network was compromised by ransomware this past December. Hackensack Meridian Health, the largest association of hospitals in the state, confirmed that the attack which disrupted their systems around December 6 was in fact a malware infection that locked down their files. They were only able to regain control after paying off the hackers an undisclosed amount provided by their insurance policy.

Hackensack Meridian Health Ransomware Infection Extent
The malware which infected Hackensack Meridian affected "anything with computer software — scheduling and billing systems and labs and radiology," an IT professional in the Meridian network told NJ Advance Media. For five days, many electronic systems went down, forcing non-emergency procedures to be rescheduled and for medical professionals to return to manual processes.

A spokesperson for Health Professionals and Allied Employees, a union that represents nursing staff, told the press that they had reports that members had to return to recording everything with pen and paper. However, documents had to be frequently rechecked for accuracy and some operations became stalled as hospital staff ensured that no incorrect information would cause any harm. In at least one case, a patient had to provide her medical history to her doctor herself as the records were not available.

As of this writing, Meridian IT staff have been able to restore most of their network, and the NJ Health Department says it is "working closely with the leadership team" at Hackensack Meridian according to Government Technology magazine.

Healthcare, Public Sector and SMBs Biggest Ransom Targets
Hospitals have frequently been victims of ransomware, though the consolidation of healthcare networks like Hackensack Meridian Health and RWJ Barnabas Health make them even more attractive targets. Each of these chains are valued at over $5 billion, and the inevitable centralization of data between member hospitals means that hackers can hold a greater (and more lucrative) amount of information hostage with less touchpoints to worry about.

Many other non-profits and public institutions throughout NJ have been victimized by ransomware attacks, including the Livingston school district just a week before Meridian. However, many small businesses have been threatened with malware and ransom demands as well. The common factor between these parties is the value of the data – figuratively, or literally, a matter of life or death for many – and the resources they have on hand to restore their infected system.

Back Up Your Data to Defend Against File Locking Malware
Ransomware hackers are continuously trying to infect your system and lock down your data – only backing up your data in a secure environment provides a guarantee that you will be able to retain your critical files. SWK's backup solution is the best way to protect your information from being lost forever to cybercriminals or other disasters, and resuming operations.

Download our free e-book on Data Protection and Backups for SMBs to learn how to prevent downtime by keeping your electronic information secured in the cloud.