IT Strategy Brief

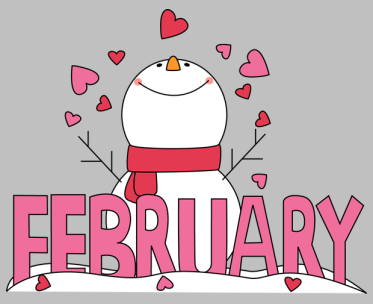
ISSUE 2 | VOL 6 | February 2020

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:



NJ a Target of Hackers with Many Cybercrimes Unreported

New Jersey is a big target for hackers, as we have covered previously. In 2018 alone, there were over 8400 victims of cybercrime in the state accounting for $80 million in losses, according to the FBI. One reason network breaches are so prevalent is that only a fraction of victims ever say anything. Only about 15 percent report that they have been hacked, with the majority remaining silent.

City and Public Sector Ransomware

The public and non-profit sectors face an ongoing ransomware epidemic that shows no signs of slowing - government agencies, hospitals and even schools are falling victim to infection. NJ has been home to several high-profile incidents within the past few years, including the Union County and Dover attacks, the recent Hackensack Meridian Health episode, and the time the city of Newark was ransomed by Iran hackers using SamSam. The latter culprits also targeted a whole string of healthcare and government institutions, reflecting the wide reach of these types of attack profiles.

Not Just Malware - Wire Fraud, Data Breaches, and More

Many NJ-based government employees and organizations are exposed to other cyber threats besides ransomware, along with many businesses who have also fallen victim to similar tactics. These include data breaches large and small (with at least one case of doxing), multiple incidents of wire fraud phishing scams, and many other types of cyber attacks. The most common factors in all of these incidents, of course, are credential abuses and backdoor access obtained by socially engineered attacks or another method leveraging human complacency.

Unsecure Network Access Fuels Hacking

Nearly all of these examples came from a hacker exploiting a critical but overlooked gap that allowed them to get past security. It is easy to attribute these to weak cybersecurity controls in the public sector, yet that is not solely the case. Many private businesses have fallen for the same tricks, but are not obligated - or compelled - to report incidents, leaving the rest of the world in the dark about these cyber threats.

Continued on page...2

What our clients are saying: Cooper Wilbert Vault Co.

"When we first switched to SWK they recommended that we setup our network on Microsoft Exchange/Microsoft 360. This was one of the best things we ever did. It helped streamline everything. However, this is one of the great things about SWK, is that if they see something that would really benefit you as a company and save time and money they will introduce it to you, not as a SALE, but as something that will help you in your business. Hands down having SWK as an extension of our company. We now feel like we have a dependable IT Department. "

Beth Cooper
Cooper Wilbert Vault Co.

Wilbert

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Lori Lynch
Foundation Title LLC-Marlton

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 **Feb 28th** to get your name in the hat.

You could win a $25 Gift Card!

DHS Warns Businesses to Watch for Iran Cyber Attack

On January 4, 2020, the Department of Homeland released a bulletin warning Americans to prepare for potential cyber attacks sponsored by Iran. This alert came in light of promises of retaliation made by Iran and allies against the US for the killing of Islamic Revolutionary Guard Corps (IRGC) Quds Force commander, Qassem Soleimani, on January 2. The primary concern is Iran's ability - and willingness to conduct open cyberwarfare and the long-term effects it could have.

Fallout from Iraq Drone Strike and Historical Tensions
Already there have been several recorded attacks against web properties and critical databases, some blatantly pointing to Iranian culprits and some still suspected of it. Iran has a history of going after US and allied targets during periods of tension through either intermediaries or their own internal cyberwarfare forces.

Iran's Hacking Capabilities
Ever since falling victim to their own cyber virus, Iran has worked hard to pursue a cyberwarfare strategy. Through a network of IRGC units, state-sponsored "hacktivists" and outsourced contractors, Iran has augmented its espionage activities with a cyber component responsible for hundreds to thousands of attacks over the past decade.

Though not thought to be as advanced as their Russian or Chinese counterparts, Iranian hackers have managed to carry out significant strikes against various targets and have been accused of many more. Even recently, multiple other cyber attacks attributed to Iran or their surrogates have occurred all over the world, with confirmed breaches in Bahrain, Europe, and the US.

Continued on page...3

NJ a Target of Hackers with Many Cybercrimes Unreported

Continued from page 1…

Some of the most nefarious cybercrimes in New Jersey were executed against commercial organizations, many who have gone unnamed. No business wants to reveal their vulnerabilities, but this adds to the level of obliviousness throughout the state. From websites to payroll system to voting machines, many networks in NJ are not built to deal with the combination of human error and doggedly persistent hackers.

This is evidenced by many of the examples of successful or attempted hacks that have affected New Jersey in recent years:

- Montville man charged after walking into two NJ businesses and installing keylogger software onsite, stealing employee and company data
- Two Russian nationals were charged in NJ for hacking Heartland Payment Systems in Princeton along with several other large corporations
- Insurance provider Premera Blue Cross forced to pay $10 million in restitution to NJ and 29 other states after a hacker gets into their poorly defended network
- Local Asbury Park business has their website and social media compromised by a disgruntled contractor, who uses the properties to harass and defame the owners
- SEC servers in Middlesex county are breached, exposing the unpublished earnings of several companies

Cybercrime Replacing More Typical Crime
A list of top cybercrimes in New Jersey reflects the growing reality in this state, and many others - digital crime is either replacing or augmenting traditional crime. As some of the examples above reveal, a profitable hack can be completed with little to no physical access and no geographic limitations.

Take for instance the food and beverage industry, one of the biggest victims of theft by organized crime. Hacking weak supply chain networks allows criminals to optimize smuggling by altering inventory and accounting data themselves without having to rely on someone internally. Web access allows thieves more flexibility in coordination as well, such as when a group of Chinese hackers contracted a NJ-based couple to help facilitate a real estate wire fraud scheme.

Petty crime is also increasingly moving towards cyberspace, such with the growing number of would-be Ferris Buellers attempting to alter electronic records in the Jersey City, Elizabeth, Secaucus and other school districts. The possibilities of cybercrime can embolden first-time and consistent criminals alike, and several factors make New Jersey a place burgeoning with potential targets.

Don't Let Hackers Catch You Off Guard - Call SWK Today
Cybercrime is just a reality of our digital world, but typical business thinking has not caught up to modern hacking methodologies. Both expert and amateur cybercriminals are looking for ways to compromise your system, which is why you need a service like SWK's to watch your network around-the-clock.

Contact SWK Technologies to learn how our managed Network Services will ensure that your data will be protected against hackers of all types.

Shiny gadget of the month: Albicchiere: Smart Wine Preservation & Dispenser

Have you ever had to pour out a bottle of wine because you had a glass and then didn't get back around to finishing the bottle before it went bad? You are not alone, according to Albicchiere the US pours $1.27 Billion of wine down the drain a year! However, Albicchiere a countertop wine gadget is here to help solve this problem.

Nicknamed "Albi" the device is a small gadget that will not only chill the wine to the proper temperature but also dispense and maintain the quality of the wine for **up to 6 months** thanks to their technology. You can choose between loading in your own bottled wine into their special smart bags that are empty or pre-filled bags you get through Albi directly.

The device itself has a built-in screen that provides details about the wine, like characteristics and location as well as tracking if it is going bad or running low. It can also be connected to your smart home devices like Google Home or Amazon Alexa if you really wanted to be fancy and have it pour you a glass on command. You can even set parental control features to lock the wine dispenser from its companion app on your phone so that children can't use it when you're not around. The app also lets you browse a selection of wines and make purchases for new wine, see recommendations, as well as set the temperature of the wine. Albi is even portable, so you can take it with you if you wanted to move it to another room, maybe by the couch for some wine and a movie, perhaps outdoors for that picnic, or trip to a winery where you're sitting outside but don't want the wine to get hot.

Beyond all the cool features and technology behind it Albi also aims to help with sustainability. The smart bags make it easier to ship wine and reduce transport costs (carbon footprints). They've already signed up 200 wineries to sell in Smart Bags. The bags themselves can be reused and are created with BPA free packaging. So now you can have a glass of wine and feel better about helping the environment too.

Albi debuted ad the Consumer Electronics Show this year and already has sold out of their initial offering on kickstarter at $249. It may seem a little pricey but for similar gadgets it is actually not bad and this one boasts better abilities. They still have some early bird specials and has an estimated ship date of October of this year (at the time of writing). This is a really cool concept and hopefully it lives up to the hype. What do you think? Would you benefit from one of these?

DHS Warns Businesses to Watch for Iran Cyber Attack

Continued from page 2…

The Cyber Cold War Landscape in 2020
A state of Cyber Cold War has existed between the US and Iran for at least a decade, with the former widely suspected of taking part in the Stuxnet infection and the latter attempting to retaliate ever since. However, the new age of cyberwarfare is complicated by the 'Wild West' nature of the Web. There is a much greater level of plausible deniability with cyber attacks than traditional kinetic warfare or physical espionage.

This allows any country – or group – to avoid open conflict while still pursuing their objectives, perhaps even disguising themselves as another potential bad actor as Iran experienced with their own ostensible ally, Russia. Another example would be the cascade of cyber attacks Israel claimed were attempted against its airport system during the World Holocaust Forum. Israeli cybersecurity professionals were able to trace the attacks back to Iran, as well as Russia, China, North Korea and Poland.

Given the list of countries involved, including some whose leaders would have been affected if the attacks were successful, it is hard to pin down the exact culprits or even their true purpose. It could just as easily have been cyber spies as anti-Semitic terrorists, and there is no telling whether this was coordinated or just a random assortment of hackers.

What to Expect From Iranian or Other Nation-State Hackers
Planning an effective cyber attack takes time, skill and patience. For all of Iran's successful hacks, most were successful due to a mix of lack of victim cybersecurity controls and the Iranians' luck. Even some of those successes were done by mistake, and the only clear objective has been to humiliate rivals and enemies, and this has limited damage in most cases.

However, this could prove to be a double-edged sword as if Iran ever decided there was nothing to lose, they could target as many poorly-defended endpoints as possible. Though their cyberwarfare arsenal includes various tools, Iranian hackers have shown proficiency with malware, especially with "data wipers" and ransomware. This means that they could potentially decide to begin overwhelming weaker cybersecurity targets by destroying or locking down data to cause financial damage or even generate revenue for themselves.

Prepare Your Data Against Incoming Cyber Threats
The reality of the digital age is that data has become a valuable commodity, and governments and cybercriminals alike are discovering ways to capture it for their own interests. If your business is ever caught in the crossfire of international tensions, your data will be the first thing exposed – unless you ensure you have cybersecurity controls in place.

Download SWK's free e-book to learn how to better protect your critical data with secure cloud backups.

Gift Card Trivia!

This month's question is:

Even with many businesses not reporting cyber attacks in NJ how many victims were there in 2018? (Hint: The answer is in this newsletter.)

a. 7200
b. 3300
c. 890
d. 8400

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **Feb 28th**, 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

44 Million Microsoft Users Reuse Compromised Passwords

A study by Microsoft discovered that over 44 million user accounts were reusing passwords that had been compromised in past breaches. The research was prompted by a previous data breach that leaked at least 3 billion Windows login credentials, which included those affected passwords.

Microsoft Security Intelligence Report 2019
Microsoft's identity research team traced, cross-referenced and compiled the user login credentials obtained from various breaches between January and March 2019. This was done to help determine the amount of Windows accounts that could be exposed and required security updates from Microsoft. Previous research had determined that password played a significant role in facilitating data breaches.

Microsoft Azure Cloud Security
The previous data breaches affected both Microsoft Office suite and Azure customers, and the report highlighted the cloud security dangers that weak password practices exacerbate. Specifically, the study expounded the threat posed by virtual machine (VM) hijacking that could result from a lack of cybersecurity in IaaS resource provisioning.

Office 365, Phishing and Malware
Much of the rest of Microsoft Security Intelligence report focused on the other typical security concerns that have historically plagued Windows computers. Namely, the research team covered the phishing attacks and malware infections (including ransomware) that Microsoft Office applications have proven vulnerable to.

As the report itself distinguishes, no matter the rate at which the technology is upgraded, Microsoft product users are consistently susceptible to exploits which leverage human error. Phishing, ransomware and remote code executions have often been at the top of this list, exacerbated by unsecured cloud connections and complacent security practices.

When Password Security Not Enough, Use MFA
Multi-factor authentication (MFA) adds a second layer of defense to traditional network security infrastructures, one that even the Microsoft Security Intelligence report claims has a 99 percent effectiveness rate. Using MFA on top of a basic password requirements ensures that your user accounts will have an extra step before access, protecting your system against credential data leaks.

Download our guide to securing remote access to learn more about MFA with DUO and how it protects your system users against breaches, no matter where they are.