IT Strategy Brief

ISSUE 2 | VOL 5 | February 2019

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:

7 Cybersecurity Questions for the C-Suite .....Page 1

What our clients are saying .....Page 1

772 Million Emails Leaked in Biggest Data Breach Yet .....Page 2

Sophisticated Phishing Scam Imitates Apple Support .....Page 2

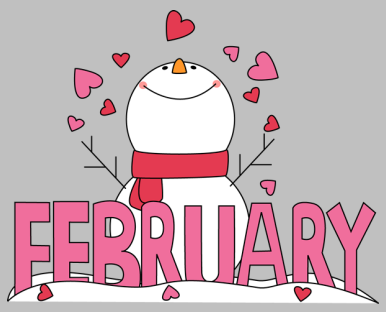
Survey chance to win a gift card! .....Page 2

Shiny gadget of the month: FlexPai .....Page 3

TRIVIA .....Page 3

Services we offer.....Page 4

Government Shutdown May Have Threatened National Cybersecurity .....Page 4



7 Cybersecurity Questions for the C-Suite

The advances in technology seen in the past few decades have led to the widescale adoption of networked devices in both private and public spaces. However, the gap between IT and business leadership have led to a breakdown in communication and lack of understanding of the full scope of defending these assets. This top-level ignorance in turn affects the IT decision-making organization-wide and the common practice in the case of a successful breach is to assign blame, discuss implementing new procedures, and continue as before until the next attack.

The scope of a cyber defense program is what often catches decision-makers off-guard. Increasingly, every machine in the workplace is connected in some shape or form and each is an attack space. Business leadership should remain informed of the steps taken to protect against a breach from each of these devices. To do so, they must ask themselves several questions on the status of their cybersecurity practice, as outlined in this opinion piece by the Forbes Technology Council.

Here are seven cybersecurity questions to ask the C-suite to determine the state of their network defense:

1. Do You Have a Real-Time Inventory of Your Networked Assets?
Since every device expands your attack surface, whether they are for private or company use, each piece represents a digital touchpoint that must be protected. A network security review will include being able to locate and identify each and every potential gateway into your enterprise's network. This must encompass not only desktop hardware, but mobile devices used for business purposes, and which tools your traveling and remote employees may be exposing your network to.

2. Can You Monitor All of Your Networked Assets Consistently?
Once all possible touchpoints are identified, they then have to be tracked – week-to-week, day-to-day and even hour-to-hour. Many cybercriminals rely on breaches going unnoticed to avoid repercussions, either from silent infiltrations or from their victims preventing news of the attack becoming public knowledge. The most optimal time to achieve the former is when your organization least expects an attempt.

3. What Would be the Chances and Impact of a Breach of One or More of These Assets?
A potentially hard but necessary question to answer is just how well can you measure the vulnerability of each of your networked assets? Some machines are easier to exploit than others, while some provide more direct access to critical systems or data and there will be at least a few that could qualify for both categories.

Continued on page 3...

What our clients are saying: Tangibl Consulting, LLC

"I am very pleased with the prompt service SWK provides Tangibl Consulting. Your staff are very personable and knowledgeable."

John M. Evanich
Electrical Designer / IT Services
Tangibl Consulting, LLC

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Michael Postles
Garland Technology

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 **March 1st** to get your name in the hat.

You could win a $25 Gift Card!

772 Million Emails Leaked in Biggest Data Breach Yet

A record-breaking collection of almost 800 million unique email addresses were found being leaked online by Australian cybersecurity and data breach expert, Troy Hunt. Hunt reported on the data dump - which he termed "Collection #1 – mid-January through his personal website and broke down the combination of files from the initial list of over 2.6 billion rows. The 772 million email addresses were accompanied by over 21 million unique passwords after Hunt cleaned up the data fields.

The "Megabreach"
The files were found by Hunt on the cloud storage service, MEGA, after several sources called his attention to its existence. A serious concern highlighted by Hunt in his reporting is that the existence of the combinations within this data indicate that it was collected for the purpose of leveraging "credential stuffing" attacks. Credential stuffing is a form of brute force attack that utilizes automated injections of leaked login information to attempt to gain access to a matching account.

Collection #1-5
Not long after Hunt published his findings, cybercrime reporter Brian Krebs followed up on the story and found that Collection #1 was actually part of a much bigger trove of hacked information that could be several years old. The entire set of email and password combination data has been advertised for sale since at least October 2018 by a Telegram user named "Sanixer." Collection #1 was one many such folders being sold online by Sanixer, who indicated directly to Krebs that it was lower value option given that the data had already been advertised previously in different places.

The Real Danger of Collection #1
Many of the credentials featured in Collection #1 had already been shopped around by Russian hackers on the Dark Web, according to Krebs' sources. As the data is older, it does not present an immediate danger to most users – unless any versions of the passwords collected are still being used. Being the largest recorded collection of email and password combinations available for sale, it does provide an opportunity for less sophisticated hackers to take advantage of.

Learn Network Security Best Practices to Avoid a Data Breach
Your organization's employees are your first and last line of defense – every individual is a walking digital touchpoint that provides as many entryways as devices they use to access your network. Leaked passwords and email addresses are one of many ways they can be hacked and exploited as a channel into your business's valuable data. It is good practice to change your passwords periodically, if this data breach is not warning enough, you should probably take the time update your password if you have not done so recently.

Read our guide on gaining employee buy-in on cybersecurity practices to learn how to ensure you're your organization stays protected from the bottom up.

Sophisticated Phishing Scam Imitates Apple Support

A new iPhone phishing scam has come to the attention of several tech and cybercrime publications, in which the perpetrators have managed to almost flawlessly emulate Apple Support's official profile. The scam consists of an automated call to an iPhone that warns the user of a data breach experienced by Apple that compromised several use IDs. The message then instructs the user to contact Apple Support at a separate 1-800 number.

The nature of the scam itself is not necessarily new, but reviews of the number from which the calls originate from have consistently portrayed it as belonging to Apple Support with no indications otherwise. iPhones display the caller's profile containing all the details of the genuine Support number, including Apple's home webpage and the physical address of their headquarters. Would-be victims who contacted the real Support hotline confirmed that side-by-side comparisons of the calls looked exactly the same.

Apple has been a frequent target of these types of phishing scams, along with several other popular media companies. This is technically not even the first to leverage Apple's official channels to lure in unsuspecting victims, though it is one of the most sophisticated examples seen thus far. In any form, phishing is designed to catch someone off-guard and this means that scammers are always introducing new methods to do so.

Protect Yourself from Phishing
Many often underestimate how easy it is to fall for a phishing scam, but without recognizing the signs, you – or one of your employees – may end up at the mercy of a cybercriminal masquerading as a customer support representative. Ensuring that everyone in your business is trained to spot the red flags will enable you to keep your organization protected from unexpected scams.

Sign up to learn more about our Phishing Defender solution and find out how you can gain access to training, analysis and other resources that will prepare your business for the worst.

Shiny gadget of the month: FlexPai

Every year the Consumer Electronics Show takes place in January to show off all the latest and greatest tech that is right around the corner. The concept of folding displays has been talked about for a while now, but no one has commercialized it yet. This year the FlexPai became the world's first commercial foldable smartphone with flexible display. The FlexPai takes a smartphone and tablet and combines them into one unique product. It has a fully flexible display that claims to be virtually unbreakable and extremely durable during testing. It comes with two cameras and can be bent to capture objects at odd angles.

Since the screen flexes around from one side to the other you have an entirely new interface to work with. You can use it as a phone where it splits the screen and you can watch video or work in an app on one side and get incoming messages or calls on the other without interruption. You can also open the device flat into tablet form to multitask with multiple things open on screen, or simply use it like a normal tablet.

Since they are first to market with a device like this one thing to note is that it uses their own Water OS, which the company stands behind to continue to update. The FlexPai currently has two options for 128 GB and 256 GB priced at $1318 and $1469 respectively. You can see how the gadget works in some of their demo videos on their website http://www.royole.com/flexpai.

It will be interesting to see how this technology unfolds going forward with big companies like Samsung who have been rumored to be developing this technology as well. The concept of a phone and tablet in one is certainly an intriguing idea. Many people already have both and if you can consolidate that it could be a home run for the companies who can get it right. Would you use something like this? If the technology worked well I know I would.

7 Cybersecurity Questions for the C-Suite

Continued from page 1...

4. How Long Would It Take for a Breach to be Detected?
As previously stated, often the greatest advantage hackers have is stealth and some attacks can be deterred by vigilance. Regardless of the stage of the breach, any attempt to control the extent of the damage must begin with recognizing where and when it took place.

5. Can You Quantify Your Ability to Limit the Attack?
Cyber resilience, or the extent of an organization's ability to respond to and sustain the effects of a breach, represents the true measurement of your business's IT investment. This reflects not just surface level protections against hacking, but the full scope and ultimately the viability of your digital assets when faced with a disruption as significant as a dedicated cyber assault.

6. What Has Been Done for Cyber Resilience?
This is another question that must be answered honestly to truly gauge the state of your cybersecurity practices. In purely practical terms, all other defensive measures are secondary to ensuring your business actually survives a cyber attack in the first place.

7. Can You Estimate ROI on Your IT Security Initiatives?
Taking cyber resilience into account, the final step is to calculate your informational security expenses against the sustainability of your organization in the face of a breach. This will give you a clearer picture on the value of your investment and the return you are receiving on your cybersecurity initiatives.

Knowledge is Key to Protecting Against Cyber Attack
Experience and training are the best tools for identifying cyber threats and defending your network against them. Arming your organization – from decision-makers to individual employees – with the right information allows you to recognize the signs of a breach and respond appropriately.

Download our e-book, "The Essential Cybersecurity Toolkit for SMBs," to learn how to better protect your business.

Gift Card Trivia!

This month's question is:

Where do the Apple phishing scam calls appear to originate from? (Hint: The answer is in this newsletter.)

a. Unknown Number
b. One of your contacts
c. Apple Support
d. The Apple Store

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **March 1st**, 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

Government Shutdown May Have Threatened National Cybersecurity

(As of January 2019) The shutdown of multiple government agencies had left many with having to furlough employees for an extended period of time, including several within the Department of Homeland Security, the National Security Agency and other departments which employ cybersecurity professionals. Many of these personnel are tasked with helping to monitor networks connected to critical US infrastructure, commerce, and military installations, or to support those that do.

Agencies Stretched Thin
While the shutdown technically only affected those employees deemed nonessential to these operations, there is a worry among observers about the effects on the system as a whole for both the short and long terms. Essential personnel found themselves stretched to handle expanded duties, and research on cybersecurity trends like came to a complete standstill as a vast majority of the staff at those institutions were furloughed.

These conditions created the potential to stall the federal government's ability to respond to an external attack at a critical juncture. It also might have exacerbated an ongoing labor pool issue within the public sector when it comes to qualified network security professionals, which was already aggravated by a greater dilemma that has not been fully addressed since the last shutdown in 2013. National security agencies have already had a difficult time attracting the number of candidates required and were short-staffed before being forced to furloughed those they already have.

Cybersecurity Labor Shortage
The high demand for these types of personnel has led to many finding better opportunities in the private sector. Agencies such as the NSA instead focused on promoting patriotism and the importance of the mission to attract candidates, but suffered from low morale and high turnover due to the difficulty of the work and the lopsided balance of prospective benefits. When the 2013 shutdown occurred, many employees simply left.

The length of the most recent shutdown is expected to create an even bigger impact in the availability of qualified experts for the US's cybersecurity initiatives. Even worse, the situation may be exploited by nation-state hackers that have already sought to undermine American networks for wealth or ideological reasons.

Do Not Take Your Network Security for Granted
The lack of a federal security net for US networks will put greater pressure on individual organizations to mind their own digital assets. Even if the shutdown remains resolved, the nation's cybersecurity institutions will take time to heal and it will pay to be proactive about protecting yourself against cyber threats.

Sign up for a Network Vulnerability Test from SWK to evaluate the state of your security practices and determine if you need to refine your approach.