IT Strategy Brief

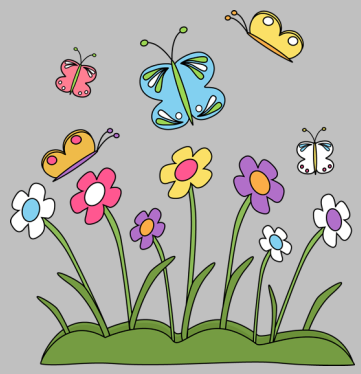
ISSUE 4 | VOL 5 | April 2019

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:



Is Your SMB Ignoring Information Security?

Cybersecurity, information security, network security, IT security – the number of terms used to describe your IT asset and data protection reflect just how much work it is to define the full scope of it. Maintaining computerized systems and databases is as complex as it is necessary, accompanied by the growing reality that machines will be increasingly networked. The advantages of technologies like cloud computing, the Internet of Things (IoT) and AI will only continue to make them popular and – more importantly – cheaper to adopt in the future, until they become industry standards down to the small business level.

However, securing the IT infrastructure for these assets will still cost time, effort, and money – and not as much as a breach of the new accompanying endpoints would. Cybercrime is predicted to cost businesses over $8 trillion by 2022, along with up to 33 billion personal data records being stolen by 2023. Basic information security measures employed by small-and-medium-businesses are being fast outpaced by the speed of which their attack surfaces are expanding.

Rate of Cyber Attack

A survey carried out by UK-based Sophos and Vanson Bourne revealed a concerning trend among respondents, which were divided between larger and mid-market businesses. Though organizations under the enterprise size had less recorded cyber attacks on average (about 63 percent versus 73 percent), they were also more likely not to be able to trace a breach to its source. The results indicate that the smaller a business is, the less effective they are at detecting an attack.

This is because SMBs have less resources for around-the-clock IT asset monitoring or even investigating signs of a breach. With every hacking story focusing on extensive attacks against larger victims, it is easy to think that those are the most common cases. The reality, however, is that experienced and amateur cybercriminals alike historically have cast a wide net and go after the easiest targets at the time - it is only a matter of acquiring their attention at the right moment.

Continued on page 3...

What our clients are saying: C. Abbonizio Contractors, Inc.

"SWK Technologies services have been very prompt and they always have a solution. A few months back a tornado came through the area and our server went down because we had lost electricity. Within an hour of calling SWK someone was at our office with a smile and cupcakes to get us back up and running."

Maureen Cleary
C. Abbonizio Contractors, 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:

Anthony D'Agostino
Pee Jay's Fresh Fruit

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 **May 3rd** to get your name in the hat.

You could win a $25 Gift Card!

Congressional Bill Will Set Security Standards for IoT

A bipartisan group of congressional members recently introduced a bill in the House of Representatives aimed at establishing minimum information security standards for IoT devices used by government agencies. The Internet of Things (IoT) Cybersecurity Improvement Act of 2019 (H.R. 1668) was sponsored by Rep. Robin Kelly (D-IL) and co-sponsored by an equal number of Democrat and Republican representative. The official purpose of the bill is "[t]o leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices, and for other purposes."

H.R. 1668 is actually a revised version of an earlier bill introduced into the Senate in 2017 by another bipartisan collected headed by Senator Mark Warner (D-VA). The Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (S. 1691) was being reviewed by the Committee on Homeland Security and Governmental Affairs before it became stalled, and the same happened to another version also put forward by Rep. Kelly. The newest iteration aims to overcome the earlier hurdles by allocating the responsibility to the National Institute of Standards and Technology (NIST) for establishing the final guidelines.

Future Baseline for IIoT
The idea behind each version of the bill has been to induce manufacturers who rely on government contracts to enforce information security best practices for their IoT products. This self-regulation is expected to stabilize cybersecurity standards across the industrial IoT (IIoT) manufacturing sector. The current form of the IoT Cybersecurity Act specifically is attempting to take advantage of a concentrated effort by NIST to build the foundations for this baseline, which ostensibly will minimize the amount of bureaucratic deliberation.

27 Billion IoT Devices
There are expected to be nearly 27 billion IoT-capable devices by the end of 2019, which is expected to grow to over 75 billion by 2025. Part of the reason for this exponential proliferation is that so many popular products now can feature IoT capability. Chances are that sitting in your hand, pocket, or desk is a tool that can access most smart devices on the market right now, and that your next upgrade will connect to even more in the future. As data-capturing sensors become more of a commonplace reality, the IoT ecosystem will take over an even greater percentage of our digital real estate.

A New Design
The IoT Cybersecurity Improvement Act takes the above expectation into account along with the historically poor approach of IoT device manufacturers to ensuring long-term network security. The bill would essentially force the hand of existing and future producers into implementing their own information security standards within their products. Similar to how life science industries self-regulate to prevent FDA penalization, the bill would create incentive for IoT device makers to begin policing themselves and establish best practices for their sector.

Do Not Rely on Current Security Standards for IoT
This bill will hopefully generate a greater impetus for smart device manufacturers to enforce security standards for their products. However, it will still be a long time before the industry aligns itself around these guidelines and several of the billions of IoT machines out there now are incompatible with future upgrades.

Read our post on the network security challenges of IoT to learn more about the threat that comes with smart devices and how you can protect yourself against it.

Don't get fooled by the 12 most used subject lines in phishing emails

Firewalls, anti-virus, VPN, encryption are all cybersecurity terms you may have heard over the past few years, but what good are they if a hacker gains access to your network through an employee? Phishing has become one of the most dangerous methods used to gain entry into a network. Cyber criminals are aware of how often people are using email and have devised clever ways to try and fool someone into doing their work for them.

Barracuda Networks analyzed 360,000 phishing emails over a three month period and identified the 12 most common subject lines that were used. According to Barracuda's spear phishing report, here are the top subject lines being used:

1. **Request**
2. **Follow up**
3. **Urgent/Important**
4. **Are you available?/Are you at your desk?**
5. **Payment Status**
6. **Hello**
7. **Purchase**
8. **Invoice Due**
9. **Re:**
10. **Direct Deposit**
11. **Expenses**
12. **Payroll**

Continued on page 3...

Shiny gadget of the month: Pick-up Pools

Spring is here and with it comes warmer weather. After a long winter everyone wants to get outside and get some fresh air. Before you know it people will be swimming and trying to cool off in pools, but maybe you don't have a pool. Do you have a truck? If you do then this gadget will turn your truck into a pool!

Pick-up Pools, like most inventions, was inspired by Tommy Prestella's (the inventor of pick-up pools) toddler daughter asking him to go swimming, but they didn't have a pool. So he made a makeshift one with a tarp in the back of his truck. From there he came up with an idea that would create liners to make the bed of a truck water-tight.

Tommy has been selling the product on his website for a few years, but due to having to change manufacturers and being deployed to Africa he has had a slower start to kick things off. However, they were recently featured on the TV show Shark Tank and had Mark Cuban invest in his idea.

You can get one right now on their website https://pickuppools.com/with an option to fit any size pick-up truck. This would certainly be a fun thing to have this summer. If you don't have access to a pool you can casually hang out in the back of your truck wherever you wanted. It would certainly turn heads at any tailgate. Or who wouldn't want to back their truck up to their kid's baseball game and chill in the pool in style.

While it may not be for everyone the pick-up pool certainly seems like it would be a fun gadget to play around with this summer. What do you think?

Is Your SMB Ignoring Information Security?

Continued from page 1…

Lack of Attack Visibility
Hackers have become creatures of opportunity and most prioritize the path of least resistance. Unless they ask for a ransom, you will likely never know anyone has been in your system until it is too late. This obscurity is the greatest strength any attacker will have since you can only fight a threat once you see it. The report referenced previously showed that most threats were discovered within servers – an area once considered safer than normal by the respondents – and that in the US, it took at least 12 hours to even uncover a breach.

Even we at SWK have to deal with attackers attempting to slip past our defenses unnoticed, despite email filters and other measures catching dozens to hundreds of similar efforts per week. This image demonstrates how easy it is to create a fraudulent address that can fool protections for a short while and exploit the factor that is never foolproof - the human element. It is only because of firsthand knowledge of such attempts and clear instruction on internal practices that these scams are found quickly.

Lack of Endpoint Awareness
An endpoint is defined as the last stop in a communication node and in terms of information security, it refers to every machine that a can access network. This ranges from desktop computers to smartphones to anything in between that delivers messages through an Internet connection. The modern workplace can become a chaotic mess for IT teams to handle because of the proliferation of networked devices, including those of remote and traveling employees being used outside of an internal security net.

Expertise Shortage
The lack of resources that can be devoted to information security practices among SMBs is exacerbated by the small candidate pool for experienced cybersecurity personnel. Such hires are sought after throughout the private and public sectors, and smaller businesses will not be able to compete with the rates offered by giant enterprises to fully assemble a dedicated IT surveillance unit. Without a team committed to monitoring your network infrastructure, the chances of a breach going undetected increases.

Strengthen SMB Information Security from the Ground Up
As a SMB, it is impossible to ignore just how useful the Internet is for your business, yet you must face the reality that it leaves you open through endpoints that you will never have the resources to cover every day. That is why you must also leverage your greatest cybersecurity weakness into your greatest strength.

Download the Essential Cybersecurity Toolkit for SMBs to learn how to reinforce your business against cyber attack.

Don't get fooled by the 12 most used subject lines in phishing emails

Continued from page 2…

I'm sure just by skimming over the list you may have seen one or two of these or even get legitimate emails from people within your organization using one of them. Their goal is to seem simple enough and familiar enough that you will take action. It can be especially convincing when receiving an email that would appear to be from a superior requesting action. No one wants to be the reason an invoice wasn't paid or worse yet not be able to collect their own paycheck because there was something that needed to be done. However, it may not always be that person. Hackers have found ways to pose as people within your organization and if you are not careful it could fool you.

Should you ever encounter an email with one of these subject lines or a suspicious email it is always better to check directly with the sender especially if there are financial transactions requested to ensure they really did ask. Always keep an eye out for suspicious links and hover over any linked text to see what the link really leads to before clicking.

People are always going to be targets for these phishing attacks. Preparing your team with knowledge is the best defense you have against stopping phishing emails in their tracks. SWK has an employee awareness training solution that helps to train your employees for what to look out for and identify a bad email. There is even an offer to try a complimentary phishing test to see if anyone does fall for a fake email. See for yourself here: swknetworkservices.com/services/phishing-defender/

Gift Card Trivia!

This month's question is:

According to the research by Barracuda Networks what is the most common email subject line used in phishing attempts? (Hint: The answer is in this newsletter.)

a. Free
b. Urgent
c. Payroll
d. Request

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **May 3rd**, 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

Avoid Getting Phished Out of Your Tax Return

Tax season is a favorite time of scammers of all types looking to grab money and personal information from potential victims. The beginning of this period is filled with hackers and other cybercriminals attempting to intercept your credentials. However, the time of expected tax returns are when you really begin seeing creative attempts to extort victims through phishing campaigns.

IRS Phishing Scams

The IRS has in recent years begun to make clear to taxpayers that the agency never initiates contact via digital media channels. This is due to repeated spoof emails appearing every year claiming to represent federal tax collectors. These fake messages may look like legitimate government communications at first glance and often contain a threat of a lost tax return if action is not taken.

Hackers Leverage Your Vulnerabilities

Tax phishing emails rely on the fear of bureaucracy and monetary loss to compel victims to act without reading too deep into the message. Those affected may be more worried of the consequences of not following through on their tax return than they about their immediate data security. Hackers that have picked up any of your personal information can also capitalize on the opportunity with a socially engineered cyber attack.

Tax Preparers Also Get Phished

Besides federal agencies, cyber scammers also have a habit of imitating tax preparers and tax preparation software companies. This includes big names like Intuit TurboTax as well as a slew of links advertising free downloads for off-brand tax applications. Tax preparation professionals themselves are often targeted so that hackers can gain access to client data or file for returns in their name.

Find Out How Vulnerable You Are to Phishing

Phishing is a pervasive form of cyber scamming because even the strongest network defense can let a spoofed email slip through. Identifying a potential fake message requires human input and judgment. If you receive a message from someone seeking your information concerning your or your client's tax return, look for all the signs that they may not be who they say they are.
Sign up for our Phishing Defender solution for hands-on training that includes testing your employee's response to simulated phishing attacks.