IT Strategy Brief

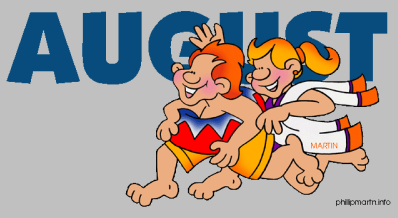
ISSUE 8 | VOL 5 | August 2019

INTEGRATE SEAMLESSLY

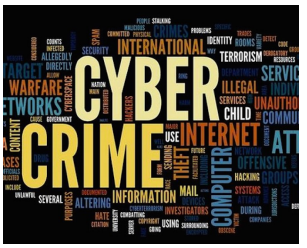
SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:



Discreet Cybercrime the Biggest Cybersecurity Threat to SMBs



The biggest cybersecurity threat to your business is not the one you can see – it is the silent breach that compromises your network without being noticed and executes on its objective only when you cannot fight back. Data security is divided between preventive and reactive controls; bypassing the former requires the patience to uncover inevitable flaws, while the obstacle of the latter relies on human action.

If your preventive controls can be compromised without being noticed, then hackers will be able to completely circumvent your reactive controls. That is the strategy that ransomware and other, more persistent forms of malware have relied on to get past defenses, yet individual and organizational perception of cybersecurity consistently remains passive. This is what puts smaller businesses lacking resources at risk, as all cybercriminals have to do is fool the system you rely on to breach your network.

Network Breach Dwell Time – Undiscovered Threats
A study of smaller and midmarket businesses by Infocyte found that SMBs consistently experienced cyber attack "dwell times" of up to 798 days of persistent malware infections. Dwell time is the period between when an infection first occurs and when it is finally detected, and can vary between attack types (Ex: ransomware exhibited an average dwell time of only 43 days according to the study). However, dwell time does not include how long it takes to actually remove the malicious files, so the lengths quoted by Infocyte should be considered the minimum expected amount of data breach response time.

Fileless Malware, Riskware & Hidden Ransomware
A significant contributing factor to the success of these attacks is the rise of different types of infection vehicles. Hackers are simultaneously leveraging existing network security gaps while deploying modified forms of malware to trick preventive antivirus controls.

An example of the former is riskware, which as illustrated by the previously cited study can go unnoticed by businesses for even longer than persistent malware. Any program that can be exploited by cybercriminals falls into this category, and can include many otherwise benign applications. Because riskware encompasses many common and non-malicious programs, it can be much harder to pick up legitimate threats, especially when relying on automated tools like antivirus software.

This is also true for the more advanced forms of malware, including the much more destructive examples of ransomware popping up lately. LockerGoga, MegaCortex, and the various targeted infections of Baltimore, Philadelphia and other cities were often proliferated by bypassing the systematized security protocols of programs like Microsoft Office, and remaining silent until they can access domain controls and begin encrypting files or even shutting out users entirely. Alternative attack methods like fileless malware rely on the same concept to get past preventive cybersecurity, which typically only seeks out traditional infection footprints to conserve time and resources.

Continued on page 2...

What our clients are saying: Cooper Wilbert Vault Co.

When asked about what she liked about our services:

"The quick response. Having SWK is like having your own IT Department that you can count on. Our computer system is a big part of our business and having SWK gives us a piece of mind that if something goes down we have a team of individuals that are going to help us get back up in running in minimal time. Time is money and if the computers/server goes down the clock is ticking. Each "computer guy" we have encountered is extremely knowledgeable and pleasant to deal with."

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:

Amy Jo Morris
SobelCo

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 **August 30th** to get your name in the hat.

You could win a $25 Gift Card!

Construction SMBs Face Increased Phishing Risk

Certain industries are more susceptible to being phished – that is what the results of KnowBe4's annual survey repeatedly reveals. In 2018, insurance, manufacturing and technology companies overtook the nine other sectors surveyed by KnowBe4. Additionally, those micro-verticals with less than 1000 employees were also often more vulnerable to phishing.

The 2019 version of the study brought some new contenders to the forefront. While SMBs still remained more phish-prone (with a few exceptions), the construction sector became the most susceptible in the small and medium spaces, while hospitality capture the enterprise slot with the highest rate of phishing vulnerability in the study. The overall percentage of employees that fell for a simulated phishing test also rose from the previous year's rate to 29.6 percent.

Employee Phish-prone Percentage
KnowBe4 defines susceptibility to phishing according to their Phish-prone Percentage (PPP) formula. This metric measures how many employees were successfully deceived by a simulated phishing test. The 2019 study submitted over 20 million test messages to approximately 9 million employees across 18,000 organizations. The baseline PPP across all industries was approximately 30 percent; a total of 19 industries were surveyed this year, with seven new additions from the 2018 study.

Size Matters in Cybersecurity
On top of industry, size was the next best indicator of an organization's PPP. While hospitality businesses with more than 1000 employees experienced the single greatest phish-prone rate (48 percent), overall, larger businesses remained at or were well below the PPP average – transportation enterprises captured lowest rate at 16 percent.

In contrast, SMBs were more likely to have a higher than average PPP across the board, the only exception ironically being mid-sized hospitality companies. A few other industries experienced sporadic percentage drop-offs in the medium range, including utilities and legal services, with others actually seeing slight increases like banking and consulting practices.

However, the greatest trend was of businesses becoming more phish-prone the smaller they were, with only a scant few exceptions going the opposite direction. Examples of the former includes the professional and financial services, insurance, and manufacturing sectors, which remained on the list of highly phish-prone industries from last year's study. This trend reflects the overall PPP for SMBs being noticeably higher than that of enterprises at 32.7 percent versus 27.9 percent.

Construction Employees Always Vulnerable to Phishing
No matter the size, employees in construction firms retained a higher PPP, with only a slight drop-off from SMB to enterprises less than a percentage point between each segment. Those under 250 employees featured a 37.9 percent PPP, under 1000 saw 37.1 percent, and 1000+ were at 36.7 percent. This translates to those businesses having a close to 40 percent chance of being successfully phished.

Smaller construction organizations were by far the most susceptible to phishing out of all the SMB verticals, and the second most susceptible out of all of those surveyed after hospitality enterprises. The most common trend among the most vulnerable verticals is the amount of client data (especially on the financial side) they manage – and the lack of widespread controls they have in place to protect it, especially on the SMB level. Construction and manufacturing firms have consistently been targets of cybercriminals because of this, and will likely to continue to until the disconnect between operational security and individual practice becomes less widespread in the industry.

Prevent Phishing by Training Your Employees
Employees are both your weakest link and your best defense when it comes to network security. That is why the best way to fight phishing or any other cyber scam is to train your personnel to be able to spot the red flags from a mile away.

Learn more about our employee awareness training through Phishing Defender to prepare your business for the next phishing scam.

Discreet Cybercrime the Biggest Cybersecurity Threat to SMBs

Continued from page 1...

Criminal Penetration Testing
In response to diminishing returns from mass volume cyber attacks, some skilled hackers are taking advantage of the gap between preventive and reactive network security to quietly form a new racket. It is essentially a cybercriminal's form of penetration testing and is only notable because it goes against historical hacker methodologies of executing attacks post-breach. Instead, the perpetrator traces their steps and documents the whole process to be able to re-utilize it or sell it to other parties.

The only evidence of this emerging tactic is the eerie similarities between LockerGoga, MegaCortex, Ryuk, SamSam and other ransomware files, as well as the complete lack of a breach footprint in many infections. This trend is worrying for several reasons: it signals not only the ability and commitment to leveraging human intelligence for cybercrime, but the end results of these methods show a frightening efficiency in choosing targets of opportunity.

Cybercrime Automation
What adds to the danger of discreet cybercrime are the technological advancements being deployed that give hackers an edge. While AI is still getting to a place where it can perform cost-effective hacking, machine learning and other automated tools can significantly speed up the data gathering process for cybercriminals. Being able to collect intelligence faster allows hackers to act on exploits before they can be found and patched, opening up a tremendous amount of opportunities to circumvent preventive controls at their leisure.

The Best SMB Cybersecurity Solution is Human Intelligence
Hackers have recognized the weaknesses of automated security controls – so should you if you want to keep your business safe from their depredations. Organizations can no longer afford to passively wait for preventive systems to make an impact. Keeping cybercriminals from breaching your network requires a proactive approach.

Contact SWK to find out how we can improve your network defense using preemptive tactics to stop hackers in their tracks.

Shiny gadget of the month: Reon Pocket

So far the summer of 2019 has been one of the hotter ones in recent memory, it seems that each year we are faced with more extreme temperatures, but left with the same methods for keeping cool. As they say necessity is the mother of invention and Sony has taken this to heart with crowdfunding a portable wearable air conditioner. Yes, you heard that right, a portable AC unit to help keep you cool when you have to be outside in these heat waves of the summer.

The little gadget is named the Reon Pocket, and it is a portable Bluetooth device that is smaller than most cell phones. The way it works is by slipping it into a special shirt that is fitted with a pocket located at the base of your neck, from there you use a special app to control the temperature, hit a button, and you're all set. The technology behind it uses thermoelectric cooling/heating where you pass an electrical current across a junction and heat is either absorbed or emitted. In their testing Sony found that the Reon Pocket can cool a user's body temperature by 23 degrees Fahrenheit on a hot day, or raise their temperature by about 14 degrees Fahrenheit on a cold day. That makes for a pretty nifty gadget if you ask me.

The device will be supported by both Android and iOS and has a battery life of 24 hours and a charge time of 2 hours (however, Engaget reported that the 24 hour charge is for Bluetooth connectivity and the actual run time is about 2 hours). Right now the price ranges from about $117 to $175 depending on which model you choose. The only real kicker right now is that it is just available in Japan starting March 2020, but if it is a success I would be shocked if it doesn't get a global launch eventually (at the time of writing this article it had already surpassed their funding objective with 20 days to go still, so there is clearly a desire for it).

Hopefully this gadget makes its way to the US because if it actually works the uses for it are endless. You could wear it under you suit or dress clothes at work to keep cool on those hot uncomfortable days, maybe you have a sporting event to attend out in the heat and want to stay cool, or maybe you're just running errands but don't want to be a sweaty mess. Even in cold weather to use as a warmer would be great, I'm sure everyone can come up with a long list of situations they would want to use it. For now we will have to wait and see, but this concept is an exciting one.

Zoom Mac Security Flaw Could Put 750,000 Companies at Risk

Jonathan Leitschuh, a software engineer and security researcher at Gradle Inc., made a public revelation this past July about a critical vulnerability in the Zoom application. Zoom is a popular web video conferencing app based in the cloud, with over 4 million users across almost a million organizations. The bug Leitschuh found resided in the MacOS version of the app, and would had allowed an external website to access and control a user's webcam through Zoom.

Zoom Webpage Access and DOS Possibility
According to Leitschuh, the vulnerability originates from Zoom's open meeting joining functionality, which generates a link that anyone can click on to attend the video conference. Leitschuh's research shows that in order to do this, the app connects your device to a web server (with some questionable protocols according to the researcher). A hacker leveraging this remote process can force your computer to join the meeting without you ever knowing, as well as cause denial-of-service (DOS) by repeatedly forcing you to join a non-existent meeting.

App Can Potentially Force RCE, Meetings, and Reinstallation
Leitschuh uncovered many deeply concerning aspects of Zoom's web functions, chief among them its ability to essentially force your machine into accepting its protocols. Though he was unable to completely confirm it, the security researcher theorized that an enterprising hacker could figure out a way to leverage this flaw for a remote code execution (RCE), but at the very least Leitschuh was able to prove that it can force webcam activation if it was installed. He also found that the web server could remain installation on your computer, even if Zoom was uninstalled, and could simply reinstall the app if commanded to.

Zoom 'Quick Fix'
Leitschuh and Gradle reached out to Zoom several times about the vulnerability, and were finally able to get their attention after some time and recommend a few fixes. However, Zoom tried to get Gradle to remain quiet on the vulnerability, which they refused to do, and after the customary 90 grace period Leitschuh revealed the flaw in early July. It is interesting to note that Leitschuh found that the only suggestion Zoom followed up on initially was a temporary quick fix that he recommended as a stop gap, and only took more dedicate measures once he released that knowledge soon after the first disclosure

Apple Patch for Zoom on Mac
Apple, on the other hand, did not waste much time in releasing a security patch for Mac computers only a few days after Leitschuh disclosed the vulnerability in Zoom's update. Apple's fix ensures that users receives a prompt asking if they want to join a meeting, rather than forcing them as before.

Zoom Security Vulnerabilities
This is not the first time Zoom has experienced a flaw like this – a similar vulnerability was found in August 2018 that affected Windows and Linux machines along with MacOS. There has been no word on whether this recent bug is present in other operating systems, but Leitschuh did point out that all of the white-labeled services which copy Zoom's code can also be affected.

Carefully Monitor Remote Access
While bugs always appear in software, the Zoom debacle illustrates how serious these vulnerabilities become in a remote cloud environment. With how many employees are joining the distributed workforce, it is important that for your business to stay protected, you must learn how to secure all remote connections and prevent hackers from silently infiltrating your network.

Download our white paper here to find out how to fortify your organization's remote access connections.

Gift Card Trivia!

This month's question is:

KnowBe4's study found that _____ were more likely to have a higher than average PPP across the board (Hint: The answer is in this newsletter.)

a. Enterprise Level Companies
b. Government Institutions
c. Fortune 500 Companies
d. SMBs

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **August 30th**, 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

Can Your Business Recover from a Hurricane Disaster?

Superstorm Sandy, Hurricane Maria, Hurricane Harvey – the list of destructive storms that have hit the US goes on and on, and will continue to grow. Are you prepared for the next hurricane? What happens if a storm takes the power and crashes your system – will your data survive? Surviving the next storm's impact on your business operations means having a disaster recovery (DR) plan in place to ensure business continuity.

Determine Recovery Hierarchy
Certain parts of your IT infrastructure are more mission-critical than others. Ask yourself which systems or data must be recovered in minutes, hours, or days to get your business back to running efficiently.

For example, you may find that recovering sensitive customer information and eCommerce systems take priority over recovering your email server. Whatever the case may be, prioritizing your systems ensures that the right ones are recovered quickly after a disaster.

Pay Attention to Location
Your backup site should be in a hurricane-free zone. Ideally, your off-site facility should be located at least 100 miles away from your main location. If this isn't possible, make sure it is built to withstand wind speeds of 160 mph (as fast as Category 5 storms), and is supported by backup generators and uninterruptible power supplies.

You should also request an upper floor installation or, at the very least, keep critical IT equipment 18 inches off the ground to prevent water damage.

Use Image-based Backups
Unlike fragile tape backups, image-based backups take "snapshots" of your systems, creating a copy of the OS, software, and data stored in it. From there, you can easily boot the virtual image on any device, allowing you to back up and restore critical business systems in seconds.

Take Advantage of the Cloud
The cloud allows you to host applications and store data in high-availability, geo-redundant servers. This means your backups can be accessed via the Internet, allowing authorized users to access critical files from any device. Expert technicians will also watch over and secure your backups, allowing you to enjoy the benefits of enterprise-level backup facilities and IT support.

Back Up Your Data Frequently
Back up your data often, especially during disaster season. If your latest backups were created on the 15th of September and the next storm makes landfall on the 28th, you could lose nearly two weeks of data. Get in the habit of replicating your files at the end of each day, which should be easy if you've opted for image-based backups.

Test Your Disaster Recovery Plan
After setting up your backups, check whether they are restoring your files accurately and on time. Your employees should be drilled on the recovery procedures and their responsibilities during and after disaster strikes. Your DR team should also be trained on how to failover to the backup site before the storm hits. Finally, providers, contractors, and customers need to be notified about how the hurricane will affect your operations.

As cell towers and Internet connections may be affected during this time, make sure your company forums are online and have your employees register with the Red Cross Safe and Well website so you can check their statuses.

SWK Can Make Sure You Recover from Almost Any Disaster
It's nearly impossible to experience little-to-no disruptions during disasters like Sandy or Maria, but with the right support, you can minimize downtime. If you're concerned about any natural disasters putting you out of business, browse some of our free resources to learn more about how to ensure business continuity.

Download SWK's Natural Disaster Survival Guide here for more information.