IT Strategy Brief

ISSUE 10 | VOL 5 | October 2019

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:

SMBs Can Lose Business from Lack of Cybersecurity .....Page 1

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

The Latest Phishing Scam Uses Deepfake AI Voices .....Page 2

Law Firm Cybersecurity Tips .....Page 2

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

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

Food & Beverage Manufacturing at Risk of Cyber Attack .....Page 3

TRIVIA .....Page 3

Services we offer.....Page 4

10 Keyboard Shortcuts for Your Windows 10 Computer .....Page 4

SMBs Can Lose Business from Lack of Cybersecurity

Over a third of enterprises are enforcing some form of cybersecurity compliance for their contracts with SMBs, according to a recent study. Security platform developer, CybSafe, repeated a survey they conducted in 2017 and found an increasing level of scrutiny in enterprise-level organizations of data compliance requirements for their suppliers. CybSafe claims that this trend has appeared in response to tightening cybersecurity regulations as well as the potential for lost business for not securing their digital infrastructure.

Security Compliance Contractual Obligations

The study results reflect a growing trend among public and private institution of imposing more stringent demands on their partners for established network security practices. The former in particular has begun to strengthen obligations for third parties, especially for defense contractors in the wake of growing nationally-backed hacking campaigns. However, even businesses without government contracts will feel the pressure as well from mounting regulatory obligations in addition to direct scrutiny from law enforcement, intelligence agencies and legislative bodies at all levels.

State governments have followed the lead of Congress and other federal bodies in passing bills that take greater measures to protect personal data. Many of these impose restrictions directly on commercial entities as well as more impactful penalties for noncompliance, all in an effort to enforce stricter society-wide standards for cybersecurity that would prevent the types of breaches that have become all too common – and the type of long-term ripple effects they could eventually lead to.

Shift of Responsibility for Cybersecurity

Companies were once seen as the victims whenever a data breach occurred, but that perception has fundamentally changed – both in public opinion and legally. Modern courts see data-holding businesses as the inherent custodians of personal information. Any risk customers are exposed to because of a vulnerability is seen as the company's responsibility, and penalization for noncompliance should correlate with the amount of risk clients face to their products, service or data.

The only good news for SMBs is that the size is taken into account when assessing damages, but only relatively, and risk and value of data exposed can supersede that. For example, a mid-sized 501(c)(3) nonprofit medical network based in Marlton, NJ was fined over $400,000 for a data leak a third-party service caused. The vendor's employees created a network vulnerability that exposed patient files, but because the nonprofit owned the data and employed the third party, the responsibility – and the financial penalty – fell on them.

Continued on page 2...

What our clients are saying: BCA Watson Rice LLP

"When we got infected with a virus, SWK worked immediately to restore all of our networks. The response and recovery time was superb. Most of our IT issues are answered and resolved as soon as possible with very little time lost."

Gina Bidaisee-Santo
BCA Watson Rice LLP

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.

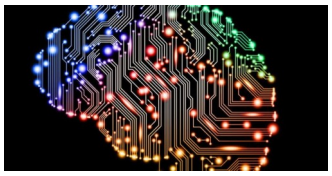
3. What are the biggest benefits you've received or experienced since hiring us?

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 **November 4th** to get your name in the hat.

You could win a $25 Gift Card!

The Latest Phishing Scam Uses Deepfake AI Voices



What some observers are calling the first reported AI heist occurred this past September, when a British subsidiary was tricked into sending over $200,000 to a fraudulent account. The scammers achieved this by leveraging an artificially generated version of the voice of the victim's German parent company's chief executive to convince the subsidiary's CEO to wire the money to a supplier in Hungary. The British CEO only became suspicious once the hackers attempted a second theft and the "deepfake voice" contacted him at the same time his actual boss did.

Spoofing, Spear Phishing, Whaling - Several Avenues of Attack
The subsidiary was represented by insurance firm, Euler Hermes Group SA, who first brought the story to light. A Euler spokeperson later spoke to the Washington Post about how their client was fooled, saying, "[t]he software was able to imitate the [German CEO's] voice, and not only the voice: the tonality, the punctuation, the German accent." Despite suspicions about the nature of the request, the phone call and a follow-up email were enough to convince the subsidiary's CEO to comply.

The fact that the call was accompanied by a spoofed email only reinforces the case that the hackers did an extensive amount of research into both the British company's chief executive and his boss. This is typical of an even more directed form of spear phishing termed whaling, which typically displays much more sophisticated methods of attack. Cybercriminals that employ whaling are putting in considerably more effort into how they catch a victim off-guard, all in the hopes of a bigger reward than they would get from any random target.

Deepfake Audio & Video Development
This type of AI-generated media is widely known as a "deepfake," a name that reflects the worrying connotations of combining the concept of machine "deep learning" with fraud. While supporters of AI-generated voice technology often point to potential benefits, deepfake software has increasingly been used to involuntarily depict female celebrities in pornographic videos, as well as create targeted hoaxes and fake news campaigns.

Public trust and privacy concerns have not stopped the technology behind deepfakes from being continuously developed and proliferated. One such example is Google's Duplex AI, which can allow Google Assistant to make calls for reservations, car rentals and more using a convincingly human-like voice. The various face-swapping applications also fit into this category, such as the now-infamous FaceApp, which critics often point out have worrying long-term implications for privacy breaches and personal data being siphoned off by bad actors.

AI Being Used by Hackers?
As the FaceApp controversy indicated, it can be hard for most people to predict where their data will end up. Numerous regulations have been and continue to be introduced to combat this reality, but the speed (and anonymity) of the digital age make it near impossible for every piece of information to be tracked. If this deepfake phishing scam signifies anything, it is that resources, time and effort make the difference in capturing and executing on data.

Research has revealed startling implications for what type of cyber attacks AI could allow, but until this particular attack, there was no evidence that it was actually a tenable strategy in the real world. While machine learning dwarfs human intelligence in data aggregation automation, it is not as cost-effective in execution for traditional cybercriminal objectives. The technology that powered the deepfake phishing scam was not anything new – the possibility of such an attack was being raised at least a year before it was proven.

Deepfakes have generated a great deal of fear and paranoia, but the real danger lies in something that hackers have always exploited: human complacency and ignorance. Many will want to rely on technology to protect against this new threat, but the best defense against any manipulation attempt is knowledge and best judgment. AI may have put video and audio alternation into everyone's hands, but these types of cases are not more common because of a human's ability to spot fake media – as long as they are aware and prepared.

Contact SWK Technologies to Learn How to Beat Spoofed Media
Deepfakes are just the latest in a long line of altered media, and phishing at its core will always be about making you lower your guard through some kind of emotional trigger. SWK can help you prepare everyone in your organization for whatever new avenue of attack hackers are leveraging by reinforcing your best and last line of defense – the human element.

Contact SWK Technologies to learn more about our cybersecurity solutions and how we can help you strengthen your network.

SMBs Can Lose Business from Lack of Cybersecurity

Continued from page 1...

Supply Chain Management – Third Party Security
A 2018 Ponemon Institute study found that 61 percent of US companies that suffered a breach had it originate with a vendor or supplier. It also found that on average, American businesses worked with almost 600 third-party partners. This constitutes a huge attack surface with an extensive amount of endpoints to monitor and no focal point for network security controls to be implemented.

Cybersecurity is increasingly becoming a team sport due to the connected nature of many value chains. Specifically, the proliferation of network endpoints means that any hacker looking for access to a larger system would have an easier time going after their suppliers with less protection. Cybercriminals only have to go so far down the supply chain to find a business with an overlooked exploit in their software, and trace through established vendor channels featuring two-way communication nodes until they reach an undefended gateway.

Ironically, perhaps the most useful example of this comes not from a damaging external attack, but from the internal breach at Capital One. Though few would consider Amazon Web Services a small vendor, it still illustrates the risk inherent in shared security, and the impact the data breach will have on Capital One will likely affect business negotiations for years – if not decades – to come. A lack of clearly defined cybersecurity guidelines and roles will always lead to one party facing greater risk, and greater risk means there are more chances to lose revenue and ROI.

Protect Your Business with Cybersecurity Best Practices
Compliance with industry and government information security obligations will becoming increasingly integral to maintaining your business as trade associations and legislative agencies try to limit the widespread damage unsecured networks can cause. Get ahead of the curve by learning and implementing the latest cybersecurity best practices.

Download this free eBook from SWK to catch up on the best tips and tricks for your company's cybersecurity.

Shiny gadget of the month: Surface DUO

Earlier this month Microsoft made a big splash by announcing their dual screen device named Surface Duo. While there have been more and more foldable screen phones announced in the past year many of them have had serious problems. The technology for a folding screen has just not quite been perfected it seems, and while the idea is really exciting, it is not worth the investment for a device that can break or have flaws.

Microsoft has other plans. In fact, they've been developing this for three years, before all the failed attempts. Their plan is to skip the single display folding screen and go with a proven strategy by using two screens and a hinge. The Surface Duo is making another improvement from past Windows phones and adopting Android as it's OS instead of Windows. By doing this they can offer the full Android app library and have the support of developers for the new dual screen technology.

The Surface Duo does work as a phone, but Microsoft doesn't want to label it as such. They believe that while this is similar to smartphones it is really a new and unique product category, so they are resisting calling it a phone. The device is made up of two 5.6-inch displays that fold out into an 8.3-inch overall screen and is 4.8mm thin. Thanks to its 360-degree hinge it can be folded over fully or opened flat. While it may sound like it will be large, when it is folded up it should fit nicely into a pants pocket.

Having the two screens should open up all sorts of new possibilities. Microsoft has a short video on their website showing some of the potential of the device https://www.microsoft.com/en-us/surface/devices/surface-duo. They show lots of multitasking, like opening a PowerPoint from an email and being able to view it alongside the email or making a video call while reviewing the PowerPoint. If you're into games they show using one screen for the game, the other as a controller so it is not displayed overtop the gaming screen. Maybe you just like a keyboard for typing, well one screen can be the display and the other the full QWERTY keyboard.

This seems like it could be the first dual screen/foldable "phone" to really work. Even though they announced the product now it will be about a year before launch with a "holiday 2020" estimate. Part of the reason for the early announcement is to try and get developers to start working now so that come next year they will have some nice polished software available. It will be interesting to see how things look in a year from now when they are ready to launch and see how the tech landscape is. Until then we just will have to wait and see.

Food & Beverage Manufacturing at Risk of Cyber Attack

Industrial control systems (ICSs) in the food and beverage industry face a growing exposure to cyber-attack, according to a report by the Food Protection and Defense institute (FPDI). The study was supported by Department of Homeland Security and was the result of at least two years of research into ICSs in the food industry as well broader network security vulnerabilities present in industrial systems worldwide.

The study concluded that the food and beverage sector faces drastic risk of a cyber attack due to gaps in technology controls, and the lack of development in this area inviting exploitation by bad actors. The consequences of a successful hack of a manufacturer or processor here could also dwarf those in other markets, as disruptions can not only bankrupt the victim, but create contaminated products that directly harm consumers as well.

Here are the factors that make food and beverage manufacturing vulnerable to cyber-attack, and how these risk factors may be addressed:

Food & Beverage Industrial Control Systems
The study centered on the ICSs most commonly used in food processing and manufacturing, as well as additional technology and processes surrounding these systems. These included not only operational technology (OT) items and procedures, but the knowledge and understanding (or lack thereof) of their connection with IT environments at the decision-making level. The researchers found that leaders in food processing and manufacturing typically were unaware of the extent of the cyber risk present in their industrial systems and OT/IT networks.

Legacy Food Processing Control Systems
One of the largest contributors to cyber risk in the food industry is the widespread presence of outdated ICSs in processing plants. Legacy manufacturing software and hardware inherently generate cybersecurity risk when introduced into networks as they are not configured for modern threats. These systems present such a danger to the supply chain that national security agencies have had to release public warnings for far-reaching vulnerabilities.

Legacy food and beverage systems are often unsecured and have rigid controls that rely too much on physical security alone. However, even new ICSs are absent of long-term cybersecurity thinking and are unprotected from external access attainable through built-in vendor channels.

Food & Beverage Supply Chain Attack Surface
The food and beverage sector is one of the most routinely targeted for theft by organized crime, which, according to the study, is often facilitated by cyber attacks exploiting credential and transport data. The food industry's supply chain is littered with disparate, often legacy system-powered endpoints that attackers can leverage to infiltrate connected networks unnoticed.

The cybersecurity danger in food and beverage is present in all ICSs – most people are ignorant of cyber risk in manufacturing and other industrial sectors. Human error accounted for over half of all ICS network incidents in 2019, according to a separate study by Kaspersky. However, that same report also discovered that security vigilance levels are reflective of industry adoption, so the examples of vulnerabilities found by the FPDI may even be more widespread throughout food processing and manufacturing.

Changing Digital Landscape
The reliance on decades-old legacy ICSs is symptomatic of the greater problem in the food and beverage industry, as outlined in the FPDI study. The stagnation of OT networks echoes the lack of awareness from equipment operators up to the executive level of changing security realities. Outdated coding, operating systems, and other components have been allowed to languish even as hackers have rapidly expanded and streamlined methods for breaking through such weaknesses.

Part of food and beverage organizations' complacency is due to the impression of being ignored, at least in comparison to what has befallen higher profile targets in finance, healthcare, etc. However, it has already been illustrated how international criminal syndicates are exploiting this weak network security – it is only a matter of time before other hackers extend their efforts to such an easy group of targets. As long as a security gap exists between your OT and IT, or between you and your supply chain partners, cybercriminals will always be able to find a way to breach your system.

Lack of Knowledge Creates the Biggest Risk of Cyber Attack
The cloud has created a more connected world, and any software you use can be linked to the Internet with access to an integrated application. Hackers rely on your ignorance to get in and out with no repercussions, but you can both protect your network and move your technology into the modern age by migrating to the first SMB cloud service monitored around-the-clock by our strategic partner CyberHat a Security Operations Center (SOC).

Watch our on-demand webinar here to learn how you can migrate to a cyber-secure cloud for FREE with Secure Cloud Hosting by SWK Technologies.

Gift Card Trivia!

This month's question is:

What percent of US companies that suffered a breach had it originate with a vendor or supplier according to the 2018 Ponemon Institute study? (Hint: The answer is in this newsletter.)

a. 50%
b. 61%
c. 28%
d. 72%

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **November 4th**, 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

10 Keyboard Shortcuts for Your Windows 10 Computer

If you're using Windows 10, here are 10 new keyboard shortcuts you need to know:

Windows Snapping
If you've never used Windows Snapping, you're missing out on one of Windows 10's key features. Previously known as Aero Snap on Windows 7 machines, this renamed feature allows you to snap windows vertically on top of each other. You can even snap windows to a 2×2 grid for better multitasking.

To use Windows Snapping, simply use these keyboard shortcuts:

- **Windows Key + Left** – Snap current window to the left side of the screen
- **Windows Key + Right** – Snap current window to the right side of the screen
- **Windows Key + Up** – Snap current window to the top of the screen
- **Windows Key + Down** – Snap current window to the bottom of the screen

You can also combine some of these shortcuts to snap your current window into a corner like top left, top right, and more.

Task Views
Task View is a window management feature that allows you to see all your opened windows so you can quickly return to a specific program or document. This is particularly useful if you have multiple windows open at once.

In addition to clicking the *Task View* button on the taskbar to open it, these keyboard shortcuts will do the trick:

- **Windows Key + Tab** – Open a new Task View interface with windows from your current virtual desktop appearing in the Task View list. To switch between virtual desktops, simply use the virtual desktop switcher at the bottom of the screen.
- **Alt + Tab** – While not a new keyboard shortcut per se, it allows you to switch between open windows on all virtual desktops.
- **Ctrl + Alt + Tab** – This is similar to Alt + Tab but the thumbnails stay on the screen even after you release all the keys.

Virtual Desktop
The Virtual Desktop feature lets you use an unlimited number of virtual desktops so you can dedicate each of them for certain functions. For instance, one could be used solely for work with all your business software and the other for entertainment.

Some keyboard shortcuts to help you quickly manage your virtual desktops include:

- **Windows Key + Ctrl + D** – Create a new virtual desktop and switch to it
- **Windows Key + Ctrl + F4** – Close current virtual desktop
- **Windows Key + Ctrl + Left/Right** – Switch to the virtual desktop on the left or right

Contact SWK Technologies for More Windows 10 Tips, Tricks and Support
SWK can help you get the most out of your Microsoft system with the latest tips, tricks, product news and updates.

Contact SWK Technologies to find out to get the best value from your Windows computers.