IT Strategy Brief

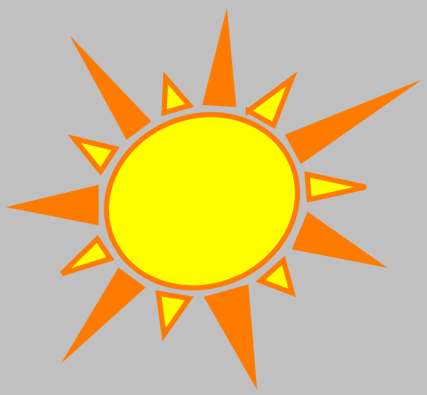
ISSUE 6 | VOL 4 | June 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:



Manufacturers Vulnerable to Cyber Threats

New realities are gradually transforming the manufacturing sector, including developing technology and emerging consumer and social trends. Wireless applications are increasingly penetrating personal and enterprise spaces by delivering quantifiable benefits in time and monetary cost management. However, extended connectivity also generates additional cybersecurity concerns as vulnerabilities progressively appear with the expansion of communication networks. Employees in the manufacturing industry were found to be some of the most likely to be susceptible to a phishing attack, and new methods of connectivity on both the factory floor and in customer-facing locations might provide new openings for hackers.

Manufacturers have considerable opportunities to streamline operational procedures and costs by deploying wireless tools, including Internet of Technology (IoT) capable devices. Industrial-level IoT applications can permit greater visibility, improved reaction times and faster decision making depending on how they are implemented. This and other Internet-connected technology provide the means to communicate more efficiently in production facilities as well as with external parties (consumers, trading partners, etc.).

All networked technology is vulnerable to hacking, and several factors can lead to manufacturing tools becoming bigger targets for cyber attackers. One of the most important will be that equipment's role in generating and processing data within the production value chain. Hackers will seek to penetrate network points that can either deliver immediate value or provide access to deeper gateways that can. The blurring of the lines between cybercriminals and state actors adds additional danger as attackers may seek instead to cause more immediate and physical damage to production spaces.

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:

Jerry Ramirez
beth ward studios

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 **July 6th** to get your name in the hat.

You could win a $25 Gift Card!

Manufacturers Vulnerable to Cyber Threats

Continued from page 1...

Roel Schouwenberg, Director of Intelligence and Research at Celsus Advisory Group, told attendees at the 2018 IndustryWeek Manufacturing & Technology Conference & Expo that worsening geopolitical circumstances will lead to greater threats of cyber attack. Cybersecurity is connected to everything, he pointed out during his keynote address, and foreign powers may consider U.S. companies legitimate targets in cyberwarfare. "You are both a target for attack and a vehicle for attack," said Schouwenberg.

Even without political motivations, there is still ample incentive for hackers to target manufacturers to obtain valuable data or access to funds directly, including from a ransomware deployment. Cyber attackers have several avenues to derive value from a successful network penetration, and emerging digital technology provides new and potentially overlooked entry points into systems. Manufacturer associations and government agencies are increasingly recognizing the threat and beginning to take steps to prepare the industry for the growing level of cyber attack.

To maintain security and keep up with emerging industry best practices, you must implement a proactive network solution that covers all bases when it comes to cyber defense. Contact us to discover what managed service solution might best serve your needs.

Guide to Business Cyber Resilience

Cyber resilience is a new buzz term being thrown around regarding organizational cybersecurity. It specifically refers to an enterprise's ability to respond to and continue to function during a cyber attack. Increasingly, cyber resilience is being mentioned in regard to how well every employee can contribute to their company's continued network security, and how well security resources leverage these contributions to ensuring critical business component continuity.

While the general outlook on enterprise cybersecurity is gradually becoming more optimistic, experts stress that cyber resilience can currently only be measured against targeted cyber attacks as opposed to probing breaches. According to Accenture Security, there has been significant improvement in this area since 2017 with faster breach detection rates by a majority of security teams. However, there is still room for growth, especially in the capability of other departments to identify threats and notify the proper personnel.

In modern times, a growing number of organizations rely on networked technology to streamline their operations or even just for basic functions. This increasing connectivity unfortunately also makes everyone more vulnerable, and the mounting number of cyber attacks indicate that hackers have fully tried to take advantage of this phenomenon. Cybercriminals utilize weak points in networks that often exist within two-way communication nodes that are necessary for interacting with customers, partners, and other stakeholders.

The first line of defense for protecting these checkpoints are the personnel who operate them on behalf of their organizations. This does not mean that you should substitute non-security resources for a true cybersecurity team, but enabling your employees to recognize their role in building cyber resilience for your business could make the difference between a successful and unsuccessful cyber attack. With the right instruction and training, your employees will be able to note the signs of a pending or completed intrusion, take steps to prevent compromising their workstations and tools, and notify the correct authority as to the issue within a timely manner.

Contact us if you would like more information and guidance on how to improve your business' cyber resilience and conduct a review of your network security programs in place.

Shiny gadget of the month: Keeping Cool in June

Summer is here and that can mean only one thing. The need for cold beverages! If you are looking for a unique gadget to show of this summer look no further than the Cooper Cooler Rapid Beverage Chiller. This device can cool a warm can in just a minute or a larger bottle of wine faster than any freezer could.

I'm sure we have all been there when you either forgot to chill something or maybe you just didn't have room in a cooler or fridge for it but you really wish you could drink it now. The rapid beverage chiller can grant you your wish. You can also rest assured that carbonated beverages will not foam or explode from this process. The chiller uses a revolutionary cooling system to rotate the beverage while simultaneously spraying it with ice water.

Sure this might not be the most amazing or practical thing in the world if you have patience to wait for something to cool down the old fashioned way, but you can be sure if you showed this off to your friends they would think it is pretty cool.

Check it out on Amazon for yourself http://bit.ly/rapid-chiller.

If you are looking for something else to cool down sometimes there is nothing better than some ice cream. What if you could easily make your own on demand? With the Hamilton Beach Ice Cream Maker you can do just that. The best part is you can add all your favorite ingredients to really make your own unique ice cream flavors.

Something that surely you (and your kids) would enjoy for a fun summer activity.

Check this one out on Amazon too http://bit.ly/make-icecream.

Ad Blockers Infect Over 20 Million Google Chrome Users with Malware

AdGuard, a provider of ad blocking programs, revealed in their blog in April that approximately 20,000,000 users of the Google Chrome web browser had downloaded fake ad blockers that likely contained malware. These malicious ad blockers were available on the Chrome WebStore and were often clones of legitimate ad blocking applications. These duplicate programs utilized the names of the originals to capture keyword search traffic in the WebStore.

The practice is nothing new according to AdGuard, which claims that Google has periodically overlooked potentially malicious ad blockers featured in their web store. These programs were also routinely poorly vetted, and Google often took considerable time to remove them, which gave the malware additional time to proliferate among users. Many of these fake ad blocker extensions were downloaded by thousands to millions of users before they were removed.

The creators of the ad blockers used code from existing applications and modified key portions to allow themselves to directly access the data of users who downloaded the program. In addition to spamming the WebStore descriptions of these products with keywords, they often leveraged modified names of the original programs (adding additions such as "Plus" or "Pro" to the title) they were copied off of to trick users into believing they were simply upgraded versions. Several of these malicious ad blockers had tens of thousands of downloads per program, with the largest being AdRemover at over 10 million users.

AdGuard found that AdRemover contained scripts hidden within an image file that would allow whoever designed it to track websites users had visited and even affect their web browser's behavior. These types of fake ad blockers connect the infected computer to a command server that can control the machine remotely.

Third party applications are one of many avenues attackers use to exploit vulnerable digital touchpoints and breach further into the system. Hackers can leverage the need to utilize the Internet to fulfill organizational tasks to place malware traps in popular tools, such as Chrome extensions or company emails. Protecting a network against these threats requires both proactive and reactive defense measures, such as scrutiny when surfing the Web and regular examinations of your system.

Contact us if you would like to learn more about protecting your network against malicious third party applications.

Gift Card Trivia!

This month's question is:

An enterprise's ability to respond to and continue to function during a cyber attack is called what? *(Hint: The answer is in this newsletter.)*

a. Cyber Stability
b. Retaliation
c. Business Readiness
d. Cyber Resilience

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **July 6th**, 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 TECHNOLOGIES

Team SWK Joins Walk for a Lifetime 2018

Members of the SWK team recently participated in Spectrum360's Walk for a Lifetime 2018, including Mark Meller, Ian Meller, Antonio Carrion, Katherine Dominguez, Diana Kyser, Seyla Stone, Patricia Salvia, and Beth McNeill, along with many of their loved ones and pets.

The Walk took place on May 6 in Verona Park in Verona, NJ, from 10 am to 1:30 pm. Diana announced in late March that SWK would be sponsoring the event and that a team led by herself would also be taking part in the Walk. SWK was one of 26 sponsors of Walk for a Lifetime 2018 and joined over 50 other teams participating in the event.

The team was able to raise several thousand dollars over from the end of March to the first week of May, which allowed them to eventually join the list of top 10 fundraising teams by the time of the event. A list of donors could be found on the SWK Tech Team Page.