IT Strategy Brief

ISSUE 7 | VOL 7 | July 2021

INTEGRATE SEAMLESSLY

SWK MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

3 THINGS HACKERS DON'T WANT YOU TO KNOW ABOUT CYBERSECURITY

Hackers are lurking around almost every corner of the internet and most rely on the same set of basic tactics to breach your network. After gaining access, cybercriminals will steal your assets, data, and revenue before you even realize it, or hold your systems hostage with ransomware. By simply knowing a few of these strategies, you can take steps to better defend yourself and your company against a cyber-attack.

THEY USE YOUR SOCIAL MEDIA ACCOUNTS

What might seem like an innocent post could turn into exactly what a hacker needs to acquire your credentials. Uploading images of your loved ones on their birthdays or your childhood home could hold the answers to security questions, which a malicious actor can then bypass to reset your password. Additionally, there could be an open computer in the background of your post, containing sensitive information which can be used to help hijack your network.

Always double check what you are posting on social media, and make sure to limit who follows you. Don't allow random strangers to view your profile by setting it to private, and by routinely checking your followers list and removing anyone whom you don't recognize.

Even inactive accounts from your past can be used against you if they contain personal information which can be used for security questions. Just because you no longer post on these does not mean there is no one looking. The possible benefits from deleting an inactive account should vastly outweigh any desire you may have to keep it on the internet.

THEY CAN HACK YOUR WI-FI

As vaccine rates are going up, the option to work back in the office is becoming more of a reality. This means that you need to prepare your business for potential attacks stemming from a hacker gaining physical access to your property. Make sure to change your router password from the factory default. This is an easy, yet often forgotten tactic to ensure network security. Another step for protecting yourself onsite is to create a guest Wi-Fi network for non-employees to connect to, creating a further level of separation between those who are actually part of your company and those who are not.

THEY ARE EXPERTS AT FORGING EMAILS

One of the most common ways hackers gain access to your network is through a tactic called phishing, which is when a malicious actor creates a fake email and/or website in an attempt to trick someone into clicking on a link. This link could lead to a landing page asking for login credentials, placing your entire network in a compromising position. Phishing emails can look identical to the countless number of emails you typically receive from within your company, from customers or from third-party vendors, so knowing where and what to look for can make a huge difference.

Continued on page 3…

What our clients are saying: Meeker Sharkey & Hurley

"I've been happy with SWK's service and they have always been able to resolve my issues. I like that requesting a service ticket is a seamless process and SWK is very quick to respond. I recently had a problem with Nitro Pro not allowing me to view PDF's to import docs into ImagaeRight. I had to use a time consuming end around to fool it into working. SWK 's tech logged into my desktop and had Nitro working after a bit of diagnostics which made my day. No more fighting with Nitro!"

Mylene Lawton
Meeker Sharkey & Hurley

MEEKER SHARKEY & HURLEY
Insurance and Employee Benefits

Get More Free Tips, Tools, and Services on Our Website: www.swknetworkservices.com

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner! We've had lower than normal submissions lately, so your chances are very high for winning.

Last Month's Contest Winner:

Cindy Daley
Friendly Planet Travel

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 **June 7th** to get your name in the hat.

You could win a $25 Gift Card!

WHY MFA IS THE MISSING LINK IN RECENT CYBERSECURITY NEWS

Multi-factor authentication, or MFA, is a simple yet effective method of preventing data breaches – it is also one of the most common links between much of the breaking cybersecurity news coverage of 2021. In particular, the absence of this additional layer of security has been apparent and increasingly noted as a repeated pattern between some of the most prominent victims of cybercrime. Most importantly, it is something which is progressively being (more strongly) recommended by experts and regulators, and quite a few of the latter already require it for compliance in certain industries.

The question remains, however, why have so many companies and institutions have been caught without MFA (or still in the process of slowly implementing it) if it is so useful? This leads into a greater conversation about the different requirements of modern cybersecurity, but the simplified answer is that it can be challenging for organizations to change their operational thinking. Businesses that are more intimately familiar with contemporary security concerns have taken authentication very seriously, while many others have remained with legacy cyber defense stances and have paid for not keeping up with the times.

Here is an explanation of MFA and how its presence or absence has impacted the cybersecurity news of 2021:

WHAT IS MFA AND HOW WOULD IT PROTECT ME?
Multi-factor authentication is, in simplified terms, a process in which the user provides another layer of evidence that proves they have access to the system they are trying to log into. Through a variety of methods, the user would be able to respond to a prompt provided by your organization's specific MFA tool and submit their additional credentials, allowing to complete the login. Different solutions provide different options for facilitating this extra layer of security, with various levels of complexity with everything from a simple added passcode to actual biometric scanners straight from a science fiction movie.

THE SIMPLICITY OF TWO- AND MULTI-FACTOR AUTHENTICATION
The definition of multi-factor authentication and its process can make it sound much more complicated than it actually is, and many tools offer incredibly simple yet secure procedures that offer minimal disruption. These are similar in function to any other login method where you require an extra PIN, such as an ATM withdrawal, and can be done with a few clicks if your smartphone. In fact, SWK Technologies uses our own MFA internally and can attest to the simplicity of using a downloaded mobile app for push notifications and passcodes that allow us to login quickly and securely.

A LOOK INTO THE CYBERSECURITY NEWS OF 2021
To understand why multi-factor authentication can play a decisive role in entry-level cyber attacks, this article will review some of the recent cybersecurity news from this year and dive into the common trends between each story:

COLONIAL PIPELINE HACK AND RANSOMWARE INFECTION
The Colonial Pipeline hack is perhaps best known for leading to infamous social media images of individuals hoarding gas in plastic bags, but the case is much more infamous among security experts as clear-cut example of MFA importance. Colonial's systems were brought down by a ransomware infection that was made possible by the attacker's using the credentials of a former employee to break into a legacy VPN that lacked any additional login controls beyond a password. Though the Pipeline's CEO tried to save some face by emphasizing the complexity of the password, this only illustrates how dangerous and widespread the complacency with traditional cybersecurity methods is.

JBS MEATPACKING PLANT SHUTDOWN
JBS, a huge Brazil-based meat supplier, had their packing plants in the US taken down similar to Colonial Pipeline, being targeted by a ransomware gang linked to the same attackers that hit the former. They also ended up paying a ransom ($11 million to Colonial's $4.3 million), and similarly recovered most of their systems without the decryption keys provided by the hackers.

NYC LAW DEPARTMENT HACKED
The New York City Law Department, which handles most of NYC's legal issues, announced in early June 2021 that it was the victim of an attack that forced administrators to quickly take their systems down. Spokespeople claimed this prevented a widespread ransomware infection and that no citizen files were compromised, however, when asked specifically about the use of MFA in the Department to prevent exactly this occurrence, the question went unanswered.

FLORIDA WATER TREATMENT FACILITY AND WINDOWS 7
In February 2021, a water treatment facility in Oldsmar, Florida discovered it was the victim of a breach when someone attempted to change chemical levels to lethal dosages. In the news that was revealed in the aftermath, it was discovered that the plant was still using Windows 7 machines – well past End of Support by Microsoft and consequently vulnerable to cyber attack – as well as sharing passwords between users.

FREQUENT RANSOMWARE INFECTIONS OF SCHOOLS
Schools and universities have often been victims of ransomware for a variety of reasons, from the lack of extensive IT resources to the amount of data they hold (there is also the fact that they must report a breach, unlike some private entities). The University of Massachusetts Lowell has to cancel classes June 8, 2021 because of an attack that occurred while the campus was already trying to implement MFA to prevent such an intrusion.

THE LINK BETWEEN MFA AND SCARY CYBERSECURITY NEWS
It is easy to see why the stories where MFA was directly referenced would be linked to this topic, but what about all of the others? Well, you may have noticed that one of the other most common trends was the discreet nature of these specific ransomware infection incidents, as well as in many similar stories of malware attacks. Credentials are one of the most readily available commodities on the Dark Web, going for rates as cheap as $2 for billions and billions of records.

The Oldsmar, Florida water treatment facility hack is a perfect example of many themes in cybersecurity, and the whole incident sits in the middle of a Venn diagram of bad security practices. The usage of systems past End of Life coupled with weak and widely available passwords – some of which were already leaked in past breaches – came only a hair's breadth from creating a "perfect storm" scenario, and it was only the lack of hacker skill and of financial gain that prevented a devastating cyber attack. The Colonial Pipeline and JBS stories are much indicative of the type of disruption that could be caused with basic login information.

MULTI-FACTOR AUTHENTICATION IS THE FIRST STEP TO CYBER DEFENSE
MFA should just be your first step to cyber defense, but it is one of the most critical in establishing a modern cybersecurity stance. The gap between sophisticated and amateur cybercriminals is wide, but there are many more of the latter and even the former will go for an easy target if you leave your network poorly defended. No matter how complex your passwords are, that login data may very likely be available in cyberspace, and it is only an of issue of when someone will try to use it.

DISCOVER HOW TO USE MFA TO FIGHT PHISHING
SWK Technologies will help you learn all you need to know about multi-factor authentication and start your implementation process when the time comes, helping you to seamlessly integrate it with your existing processes. Begin your journey by downloading our free

SHINY GADGET OF THE MONTH: RADIUS ZONE MOSQUITO REPELLENT

Now that we are well into the summer you've probably spent your fair share of nights outside barbequing, relaxing by a fire pit, or just sitting on a porch, whatever your activity may be it can easily be ruined by mosquitos. We've all been there, it is a perfect night and you just want to relax outside, but as soon as you get comfortable the bugs come in and you spend your time smacking mosquitos until you surrender and go inside. Well Thermacell has created a solution to your problem.

The Radius Zone Mosquito Repellent is not a brand-new technology, but they have made some improvements over the years. There are a number of bug repellent options out there, but a number of sources including Wirecutter named this one the best. The way it works is by using the compact gadget to heat up a repellent stored inside which radiates out and forms a "zone or protection" around you. So no matter where you are, at home, camping, on vacation, you have a portable mosquito barrier that can come with you. It is also battery powered and can operate for 6.5 hours on a charge providing you with more than enough coverage for the night.

If you're someone who enjoys the outdoors this seems like it could be a pretty cool little gadget. It retails for $49.99 and if you're interested in learning more you can find it on their website.

3 THINGS HACKERS DON'T WANT YOU TO KNOW ABOUT CYBERSECURITY

Continued from page 1…

When clicking on a link from your email, make sure that there isn't anything inherently off about the URL when you hover over it. For example, if something is misspelled or there appears to be a hyphen/character in an unusual spot, don't click the link just yet. Oftentimes, hackers will try to emulate your company's or a partner's official domain, but because they lack access to the website typos become a dead giveaway (i.e., "skwtech.com" or "swk-tech.com" VS "swktech.com").

Another easy step would be to contact your IT team directly and forward them the email. They are more likely to notice anything suspicious and can more confidently confirm the legitimacy of the email. If you lack a full inhouse team, or they're already overloaded with requests, talk to someone at SWK today about co-managing your IT.

Sometimes cybercriminals will use a fake email account mimicking the name of someone your work with. To avoid being tricked, try contacting this person on a separate platform, like Microsoft Teams, and double check that they actually sent you that message. These emails are specially designed to be as convincing as possible, so there is no harm in being overly cautious when navigating through your computer.

The vast majority of hacking starts with a social engineering attempt in order to have a person make some sort of mistake. Hackers are not sitting behind a computer screen looking for flaws in lines of code, but actively learning and excelling at manipulating humans into giving them their information.

LEARN MORE ABOUT HACKERS AND CYBERSECURITY GAPS WITH SWK
If you're looking for tips and solutions to protect yourself from hackers, contact SWK to learn all the ways we can help.

HOW CLOUD BACK-UP CAN PROTECT YOU FROM RANSOMWARE

Many stories of cybercriminals hijacking a company's data and holding it for ransom have inundated news feeds since before the 2020 pandemic, and this trend has continued into 2021. From the Colonial Pipeline attack to a series of hacks on Kaseya earlier this month, ransomware is quickly becoming a household topic that has very serious effects on the real world. One method that businesses can use to protect themselves from these attacks is having the ability to back up data in the cloud.

WHAT IS RANSOMWARE?
Ransomware is a type of malware used by cybercriminals in order to hijack and encrypt data. This data will be left effectively useless as long as it is encrypted until ostensibly a sum of money is paid. As seen in the news, companies will pay millions to regain access to their data, yet often still must rely on their own backups to recover from disaster. Larger companies aren't the only ones at risk either, as thousands of small to medium sized businesses (SMBs) get hit by hackers each year.

WHY BACK UP DATA IN THE CLOUD?
Choosing to store data in the cloud is becoming the industry standard for companies wanting to protect their assets in a post-pandemic world. Not having any way to recover data makes your company even more vulnerable to malicious actors and natural disasters, both of which already pose a serious threat to your business. By using the cloud, you get the security that if something were to happen your data, you would be able to access it quickly and effectively before any serious harm can be done to your company. Disasters can happen at literally any time, and when they do occur, having your data already backed up protects you from major losses.

HOW YOUR NETWORK IS VULNERABLE
Hackers displayed increasing sophistication during the pandemic and a refined professionalism when it came to stealing data and infiltrating networks. Knowing their strategies is an important first step to protect your business. The most common tactic cybercriminals use to hijack your data is a method called phishing. This is where the hackers create a fake email in an attempt to get you to click on a compromising link. This would then prompt you to give up private information, like secure log in credentials, and places your network at risk. Cybercriminals are extremely adept at creating these fake emails, so knowing the signs to look out for is crucial.

UTILIZING CLOUD BACKUP AGAINST RANSOMWARE
As discussed previously, having a proper system for data back-up in the cloud can be essential in the fight against ransomware. Where your data is left effectively useless after a hacker infects it with the malware, the stored copy in the cloud is still accessible. This eliminates much of the leverage cyber criminals have on your business and removes the urgency to pay them. Additionally, after recovering your data from the cloud, you are now in a position to address how the hackers gained access into your network and find solutions to improve cybersecurity.

However, even with data recovered there still remains a risk if an intruder has breached your network. If the hackers managed to access anything containing private information about your customers or partners, then reporting the hack to all potentially affected parties and the appropriate authorities is the next logical step. Failure in doing this could result in fines, especially in certain states , as well as a huge loss of reputation for your brand.

WANT TO LEARN ALL THE ADVANTAGES OF DISASTER RECOVERY
Whether you already have Business Continuity and Disaster Recovery (BCDR) in place have been considering implementing one, now is a good time to re-evaluate your current risk. Watch our Webinar here to learn all the ways disaster recovery can benefit your business.

We can help you with:

- Cybersecurity
- IaaS
- 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
MANAGED CLOUD SERVICES

HOW TO PROTECT YOUR ERP DATA SECURITY FROM CYBER THREATS

Cybercrime is growing exponentially, and after various attacks on businesses such as Colonial Pipeline, the benefits of proper cybersecurity are getting clearer each day. Companies with ERP must ensure data security in order to maintain operations and prevent profit losses from malicious cyber-attacks. Enterprise Resource Planning software contains incredibly sensitive information on both the credit and debtor side, being supplier records and customer records, respectfully.

WHAT TOOLS AND METHODS ARE HACKERS USING TO HACK YOUR ERP?
Hackers are becoming more proficient at attacking your data, adopting a litany of strategies specially-designed to break into your company network. To ensure ERP data security, the first step to take is to learn about and better understand the most common cyber attack methods to watch out for:

SOCIALLY ENGINEERED STRATEGIES:
Most hackers do not need to be an expert with workstations or operating systems (OS) to break into your network – they just need to trick a single unaware employee. Social engineering is the method of manipulating a person into giving access to private information, like login credentials or other sensitive data. All it would take for a cybercriminal to obtain this information is a fake email with an unsecured link and convince the employee with access to either log into a fake website, or give up other information protected by the company such as your accounts payable banking information. This particular method is called phishing, and is one of the most common cyber attacks committed across the world.

DDOS ATTACKS:
Also common against ERP, a distributed denial of service attack, or DDoS, is where the cybercriminal makes a network resource temporarily (or, if left unaddressed, indefinitely) unavailable by disrupting services of a host connected to the Internet. A hacker can then hold the network for ransom, halting all operations until a certain amount is paid.

PHARMING:
Pharming is similar to phishing attacks, yet focuses more on sending traffic to a fake website in order to steal information. This website could look exactly like your company's login page, and by submitting your regular credentials, you just put your ERP at risk.

TIPS FOR ERP DATA SECURITY
Looking back at the most-used methods, one common theme can be made clear: the human element. Each attack has a role that needs to be filled by an employee, a fact that should be addressed when attempting to improve ERP data security. Companies can protect against this by giving proper training and tools to their employees, as an active way to fight against cyber-crime.

KEEP SOFTWARE UP TO DATE
In the modern world, security technology is constantly evolving, and what may have once worked to protect your assets could now be out of date. By keeping your software updated you can ensure that you have the latest defenses to protect your ERP data. This not only applies to OS updates, but especially the latest updates to your enterprise applications.

MFA
Multi-factor authentication (MFA) is a tool designed to protect your log in credentials, and therefore access to your data. MFA acts as a second form of verification that makes sure the person logging into an account is really who they say they are. If a hacker managed to gain someone's information through a phishing attack, they would still not be able to gain access to the network if the extra level of identification was put into place. Multi-factor authentication is a simple tool that provides a large amount of value to your ERP data security.

ACCESS RIGHTS
If everyone in your business has the same level of access to files and data, hackers have a large pool of people to try and scam. The larger the pool, the higher the chance is that someone accidentally falls for their attack and give up sensitive information. Consider limiting employees access rights to only what they need in order to get their personal job done. By doing this, you are limiting the size of potential victims that hackers actually want to target, meaning the likelihood of an attack will go down.

REMINDERS
You can't expect every single person working for your company to constantly have cybersecurity on their mind. It is up to decision-makers to make sure reoccurring programs are put into place that will remind employees about the strategies hackers use, and what to look out for in suspicious emails. One program at the beginning of their tenure will not make them data security expert, but perhaps a monthly or bimonthly training session could give you the peace of mind that your employees know how to practice proper cyber safety methods.

KEEPING ERP DATA SECURITY AS YOUR TOP PRIORITY
Covid-19 has taught us a lot about how people respond to conflict. Unfortunately, some people took advantage of the need to work from home and discovered many new data security and privacy gaps, leading to many companies having to place cybersecurity as a bigger priority in 2021. Using the tips from above, you can better enforce ERP data security practices, ensuring your company's place in the modern workforce.

ASK SWK TECHNOLOGIES ABOUT ERP CYBERSECURITY
As both an award-winning managed service provider (MSP) and value-added reseller (VAR) of multiple enterprise applications, SWK Technologies brings the knowledge and experience you need to successfully protect your ERP data. Reach out to us ASAP to let us show you some of our cybersecurity solutions tailored for systems like Sage 100, Sage X3 and Acumatica, and find out how we can secure your network whether you are hosted on-premise or in the cloud.

Contact SWK Technologies today to learn more about our solutions for ensuring your ERP data security.