IT Strategy Brief

ISSUE 12 | VOL 6 | December 2020

INTEGRATE SEAMLESSLY

SWK MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

10 Top Cybercrime Predictions for 2021

Hackers showed no sign of slowing down in 2020, and SWK's cybercrime predictions for 2021 rest on the patterns displayed mostly consistently within the past year. The most interesting trend observed is that bad actors continued to rely on the same general category of techniques, eschewing new leaps for refining the old proven methods. Though the pandemic undoubtedly exacerbated many factors, the signs seen so far indicate that the new year will bring escalation of existing cyber attacks, yet featuring more sophistication.

Here are the top 10 cybercrime predictions for 2021 from SWK Technologies:

1. Cybercriminals Will Target Remote Worker Personal Devices
The growth of digital tools allowed for BYOD (bring your own device) policies to emerge among more prepared workplaces, but those that were unprepared when the pandemic hit cybersecurity gaps quickly appeared. Personal computers connected to your network bring cross-exposure to cyber threats and often do not have the same level of security controls that business machines must have. Organizations with employees working from home for the first time have had to make do, and even if COVID-19 cases begin to dissipate, hackers know that there will be enough victims to exploit in the time left.

2. Phishing Remains a Top Data Breach Vehicle
If phishing was the prince of cybercrime tactics in 2019, the events of 2020 made it the undisputed king as attacks escalated exponentially trying to take advantage of people's fear and uncertainty. Email compromise and similar methods will likely still reign supreme for the near future, and groups with more resources will test more sophisticated techniques to breach networks.

3. Ransomware Gangs Continue to Steal Data
Ransomware gained a new level of notoriety this past year as some gangs went as far as attacking hospitals in the midst global pandemic. Though the most nefarious demonstration of their ruthlessness, it was far from the only sign they displayed of increasing their efforts to generate whatever funds they could. The most important factor for future predictions is the trend of data theft that saw a doubling down on convincing victims to pay, including publicly data shaming online.

4. Hackers Leverage Legacy Systems for Backdoors
Unpatched legacy software and hardware have played a key role in allowing some of the worst data breaches; however, the scramble caused by COVID-19 saw many outdated systems be overlooked or introduced into ad hoc networks. Exploits for misconfigured devices and programs are only going to proliferate through the Dark Web, and remote desktop protocols can grant backdoor access without the right updates.

5. Financial Services Cyber Attacks Are Going to Grow
Besides healthcare, financial services saw one of the greatest surges in cyber attacks over the past few years, and banks and firms are a target precisely because of the role they fulfill. Not only do they preside over significant transfers of money, but also of personal data that can be exploited for direct gain or in a ransomware attack for an easier payout.

Continued on page 3...

What our clients are saying: Family Resource Network

"My favorite thing about SWK is the peace of mind I have when logging into my remote server and knowing that someone is just a phone call away that can help me with an IT issue. If I do have an issue the technicians are not only knowledgeable, but also friendly, patient and easy to speak with."

Barry McManaman

Family Resource Network

The Family Resource Network
Providing families with access, answers and action

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

You could win a $25 Gift Card!

9 Cybersecurity and Business Continuity Tips for 2021

BCDR and Data Security Planning for the New Year
To help you continue to protect against cyber threats in 2021 and beyond, here are several tips for your cybersecurity and business continuity planning in the new year from SWK Technologies. With this advice and SWK's support, you will be able to better position your company to manage and defend your IT assets amidst the uncertainty and disruption of your evolving market. With real-time network monitoring, comprehensive user training, secure data backups and disaster recovery solutions, SWK will ensure that you have the right resources and guidance to maximize your business resilience.

COVID-19 and the new normal exponentially accelerated the push into a more digital world, and this transformation of traditional processes amplifies the importance of good data security. To get the most out of the advice in this article, and your IT, consider engaging a managed service partner like SWK Technologies to gain a better understanding of your digital assets and how your endpoints could be best protected.

Here are the nine top cybersecurity and business continuity tips for 2021 from SWK:

1. What the Pandemic Taught Us About Business Continuity

Coronavirus caused massive operational shifts that forced many to rethink their processes, while reinforcing lessons for those that had already distributed workforces and networks. If you have deployed remote workers for the first time, then this pandemic has undoubtedly presented a challenge in discovering how to restore and resume your business activities seamlessly. This demonstrates that business continuity requires more than just a basic data backup and your IT infrastructure is a mission-critical resource that must remain top of mind in disaster planning.

2. Cybersecurity Training for the New Decade

The intersection of so many employees working from home for the first time and the transforming realities of endpoint protection have made good user security practice paramount. Comprehensive cybersecurity training is a must - zero trust policies cannot be scaled to every single activity and eventually the safety of your network will fall back on personal cyber hygiene. Deploying informative education based on real-world examples will ensure your last line of cyber defense remains your strongest and most consistent countermeasure.

3. Will You Continue Working from Home Beyond 2021?

No matter when social distancing will finally end, having faced the advantages and disadvantages of a distributed workforce, your business is better equipped to leverage this model in 2021 and beyond. If and when the pandemic stops being the driving factor, will you continue to capture value from having some, many or every one of your employees working remotely? There are ample opportunities in telecommuting, but you must have a clear and structured cybersecurity policy for personnel working from home.

4. Data Risk & Compliance Audit

Data has accelerated the evolution of business, including the growth of the cybercrime ecosystem around capitalizing on its importance to you with tools like ransomware. Regulations have also been reinforced to address the increasingly porous nature of digital information collection, with a variety of consumer privacy protections at multiple government and industry levels. Your company must assess the risk of a breach and be able to audit your compliance processes to prevent one from happening, taking steps to identify and plug any gaps in your network.

5. How Secure are Your Backups?

Backing up your data is the first step in any business continuity plan (through far from the only one), but are you absolutely certain your backups are completely foolproof and cybersecure? Traditional methods have many vulnerabilities to human error and natural disaster, and often will either impede or outright prevent a full restoration of your system. Additionally, your software can significantly impact the type of solution you actually need to successfully capture every byte of information - make sure to talk to your reseller about what your version requires.

6. Ensuring Recovery from Disaster

The next step in business continuity is ensuring that you can actually recover from a disaster whether manmade or natural, and this requires more than just having a backup in place. Most importantly, you must ask yourself just how fast your company can migrate your saved data back into your system and restore your network - then ask how much business you could lose in that time. This requires a lot of measuring and testing to determine if your recovery solutions and processes are efficient enough, and what you can do to lessen the impact downtime has on your business.

7. The Right Tools - MFA, Encryption, and More

Real cybersecurity has moved well past the days of just deploying antivirus software, and there are many tools that help you provide additional layers of protection to deter hackers that get past one. Multi-factor authentication (MFA), encryption programs, virtual private networks (VPNs), email filtering, anti-malware and more help create a padded cyber defense when combined with the right support and training. Which solutions will work best for you, however, depend very much on your specific circumstances, and you should audit your network vulnerability to determine where extra security is most needed.

8. SIEM and SOC as a Service

Security information and event management (SIEM) technology closely watches the data flowing through your network and uses it to identify potential malicious activity. When leveraged by an experienced SOC (security operations) team that can recognize hacker footprints quickly, this creates a comprehensive cybersecurity monitoring and incident response solution that reacts to threats in real-time. Engaging this service will augment your static defenses and internal training with human cyber intelligence - reach out to SWK Technologies to learn more about our Smart SOC and its proprietary endpoint protection.

9. On-premise Servers VS Cloud Hosting

Where your data and IT assets live can make all the difference when it comes to your business continuity planning, and servers on-premise or in the cloud each require their own steps to cybersecure. However, it is not simply a matter of one or the other - we live in an increasingly "multi-cloud" world, not to mention the growing migration to hybrid systems where resources are divided between onsite and digital. Even if all you have is a Microsoft Office and QuickBooks installation, some or all of your files live in a hosted or cloud-adjacent environment and require their own cybersecurity protocols.

The Cybersecurity & Business Continuity Planning Essentials

Business continuity and cybersecurity are inextricably linked together, demonstrated by how both were impacted often simultaneously during 2020. Prepare better for 2021 by reviewing your BCP and determining where you have to room to improve and where you could be most vulnerable if downtime occurs.

Download our free ebook here to learn the 4 Business Continuity Essentials and let SWK help you move into 2021 with confidence in your cyber defense.

Shiny gadget of the month: Roku Streambar and Ember Mug

Winter is almost here and so are the holidays. To give some extra gift ideas we're featuring a couple gadgets that fit right in with this time of year.

The first is the Roku Streambar. It combines a Roku 4k streaming device with a soundbar with Dolby Audio technology to instantly upgrade any TV that could use a little boost. Not only will it play audio from your TV but will also work as a Bluetooth speaker for a connected device like your phone to stream music.

Considering a Roku streaming device alone can run you anywhere between $30 to $100 this combination device for $130 is a pretty good deal and uses the streaming tech of the higher end stream only devices. So, if you're looking for an all in one upgrade for a TV this could be a good choice. Take a look for yourself on Roku's website.

If you're all set on your home entertainment maybe you are looking for an upgrade for your home office. The Ember Mug is a mug that will keep your drink hot, especially in these colder months where letting your morning coffee sit out will end in a cold disappointing sip after only a little while. The Ember Mug does more then just keep it warm though, it will allow you to set an exact temperature using an app, so you can have it exactly the way you like it for a long time.

It comes in a 10oz or 14oz style and is safe to hand wash and submerse in a meter of water, so no need to worry about damaging your fancy mug when washing. The built-in battery will last up to 1.5 hours, or if you leave it on the charging coaster it will stay warm all day if you so choose. There is an LED indicator to let you know when the beverage has reached its set temperature and will intelligently turn itself on or off.

While this is not a cheap mug with a price tag of $130 for the 14oz mug and $100 for the 10oz, it is certainly a cool gadget and would get good use. Check it out for yourself on their website.

10 Top Cybercrime Predictions for 2021

Continued from page 1 ...

6. Digital Transformation of Traditional Processes Will Continue
Even with the all the scarier predictions pointing to technology, the fact is that the shifts brought on by the pandemic only highlighted the need for digital transformation as an accelerator. Manufacturers, distributors and even some service industries that had been hit hard by social distancing were able to keep business going by taking advantage of apps and other solutions.

7. Cybercrime Will Become More Expensive (and Lucrative)
Cybercrime has grown so much that it has built its own economy ranking behind only the world's superpowers, and this is trend that will continue feeding into itself until the opportunities die out. This parallels the increase of cost a cyber attack will bring, not only from hackers stealing or demanding payment, but from recovery operations and privacy compliance fines.

8. Human Cyber Intelligence Provided by SOC and SIEM Takes Point
The static cyber defenses of the 1990's and early 2000's have proven easy to overcome by today's cybercriminals, and businesses like yours require much more than traditional antivirus. Human cyber intelligence delivered by a SOC (security operations center) and real-time monitoring provided by SIEM (security information and event management) technology is becoming the key adaptive solution to cybercrime.

9. Cloud Security Will Take Precedent for Enterprises
The cloud has enabled business continuity and working from home at an unprecedented scale, and just as past investments allowed this new normal, future ones reflect the direction of enterprise strategy. Many businesses are focusing even more on their digital infrastructure deployments by investing in additional cloud security solutions to defend them.

10. User Cybersecurity Should Be the Focus for 2021
Most of the above factors point to a changing world that will bring greater speed and flexibility, but also a greater number of distributed endpoints, bigger potential attack surfaces and increased importance on user security. Cybersecurity training will be required to provide the most effective level of defense these digitized networks will need, reinforcing cyber hygiene for the standards of the new normal.

Learn the 10 Ways Hackers Get Past Firewalls to Fight Cybercrime
To fight against these cybercrime trends predicted for 2021 and beyond, you must start from the ground up and focus on the last line of cyber defense until you work your way up to the first. Read through our guide, ***The Top 10 Ways Hackers Get Around Your Firewall and Antivirus to Rob You Blind***, and discover how you can best prevent a data breach. **Download the guide here** and learn how to better protect your business from all types of cybercrime.

Holiday Shopping Tips

The Holiday Season is upon us and with COVID disrupting how normal life has been for many of us online shopping has become even more prevalent. Since just about all of us will be doing some form of shopping we compiled a list of tips to help keep you safe. These tips are not only useful for online shopping but are a great general rule of thumb for good cyber safety.

As you have likely seen us mention before, always use caution when clicking links from emails, especially from an unknown source. Even from known sources you should always hover over the link and make sure it goes to a legitimate website. A big threat during this time of year are emails that appear to be from legitimate companies that ask for personal information such as asking you to verify user names and passwords. Companies shouldn't ask for that information directly in an email. If they try to redirect you to a website to input information pay attention to the website (and its URL) itself. Using fake websites can be a way to lure you into inputting credentials.

Another popular scam is to send emails that claim to be "Urgent". If you see emails coming in that are asking you to quickly take action or are marked urgent that should be a red flag for you. With the holidays and COVID this year it has become a more popular scam to use, preying on panic and urgency. If you get an email that appears to be from someone you know, like a co-worker, that is asking for something urgent it is always better to ask them directly to verify that they sent the email.

Email and websites are not the only threats. Social media scams are on the rise as well. People are sending private messages to try and obtain your personal information. Like the fake emails mentioned above social media sites will never ask you for a user name and password through private messages.

Beyond looking out for scams you can take some additional measures to try to make things as safe as possible. For instance, if you are unsure of a product from an unknown website, try comparison shopping and see if it can be from somewhere you trust, or to make sure it is not "too good to be true".

You should also never use a debit card online; you should always use a credit card when possible since it is not tired directly to your bank account and is easier to combat fraud charges. When making purchases online, you should make sure there is a "SSL" which is a secure connection usually indicated by a padlock in the browser bar next to the URL. Last but not least, in this particularly trying time for local businesses go shop somewhere locally, it will help support the community you live in and you don't have to worry about a cyber scam.

When in doubt, if you ever have any questions about your cybersecurity or best practices contact us. We are here to help and support you with the knowledge and tools to keep you and your business safe.

Gift Card Trivia!

This month's question is:

What industry saw one of the greatest surges in cyber attacks over the past few years? (Hint: The answer is in this newsletter.)

a. Financial Services
b. Food Service
c. Manufacturing
d. Logistics

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **January 4th,** in order to be placed in the running for this month's gift card prize!

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

Why Cloud Hosting Will Prepare Your Business for the Future

Hosting your software and IT in the cloud will prepare your business for a future in which network resources and data storage will increasingly live in digital environments. On-premise servers, desktops and other traditional pieces of hardware were progressively being scaled back even before a global pandemic forced many into working from home for the first time ever. Investments in web-based application and infrastructure models were growing before COVID-19, and the flexibility granted by those decisions after the mass shutdowns around the country only reinforced them.

All of this should come as no surprise to anyone who has paid attention to how cloud technology has infiltrated the consumer world. As our personal tools continue to migrate to SaaS and hybrid environments, your business must begin to develop a strategy around how and where to take advantage of web-hosted platforms.

Here are the top reasons why cloud hosting will prepare your business for the future:

Reducing Onsite Servers and Costly Upgrades

Traditional hardware deployments rely on a lot of capital expenses that only grow as you add locations, users and additional touchpoints down the line. On-premise servers are expensive and cumbersome to scale, as well as to perform regular maintenance and upgrades just to keep your systems running at capacity. Migrating data during renewals can also be a precarious venture, while moving to SaaS or IaaS gives you more redundancy for protecting your information, and peace of mind during updates.

Hybrid Cloud Environments Allow Flexibility

The conversation around web-hosted applications in the past obfuscated one of the most beneficial factors - hybrid cloud environments are not only very possible, but they also deliver incredible value return for SMBs. It can be costly to wholesale replace and migrate from an existing IT set up that represents a big investment for a small business, but the ability to slowly introduce new digital resources grants significant flexibility. This gives you options for security by segmenting data, avoiding on-premise upgrades by bringing in additional assets through the cloud, and many more advantages that transcend the traditional narrative of choosing one option or the other.

Hosted Infrastructures Enable the Work from Home New Normal

There were tremendous investments made by many enterprises in hosting their IT infrastructures online, and these paid off in a big way when the pandemic hit. As millions of workers across the country were forced to work from home for the first time, cloud hosting enabled the transition and quite a few were able to adapt as seamlessly as was possible. The technology allowed an unprecedented facilitation of business continuity as businesses were able to quickly pick up where they left off without having to manually migrate their data.

Preparing for the Multi-cloud World

All the talk of private and public clouds has also obscured another growing trend - we live increasingly in a multi-cloud world, where the resources of different publishers feature some level of collaboration. Microsoft, Apple, Google, Amazon and all of the other hosted services have their own databases, yet users frequently move data between their applications and take advantage of limited integration. As the technology becomes more widely adopted, providers will have to deliver options to link these silos to allow customers to unify their software and IT stacks, granting you additional opportunities to scale.

Users Are Accustomed to SaaS Technology

Millennials are called the first "tech-savvy generation" and Gen Z follows in their footsteps when it comes to leveraging digital tools for accelerating productivity. Many of the streaming services that have proliferated the consumer world are much more seamless (and singular purpose) versions of the workplace apps we leverage, like the Microsoft Office suite. The reality is that your network users are only going to become progressively used to the experience delivered by these SaaS systems, and your technology stack should replicate that representation to capture the best value.

Cybersecurity is Making the Difference for Cloud

Cloud security is the chief overriding concern for the decision to migrate, and even as past anxieties have been overshadowed by the benefits, this scrutiny persists. Yet even as the worry persists, publishers and cloud service providers (CSPs) have only increased efforts to secure cloud environments for customers and reduce user gaps. Migrating to hosted platforms requires a change in cybersecurity posture, and human cyber intelligence services (like the SOC, or security operations center) are making the difference for incident response solutions.

Talk to SWK Technologies to Develop Your Cloud Hosting Strategy

Cloud hosting for your software and IT assets will be the standard of the future as more and more users become comfortable with web-based features and performance capacity. Do not let your business be left behind as your competition outpaces you - talk to SWK Technologies today to start building your migration strategy.

Contact SWK here and discover how you can best move to the cloud at the pace that delivers the most value to you.