IT Strategy Brief

ISSUE 1 | VOL 7 | January 2021

INTEGRATE SEAMLESSLY

SWK MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

Why You Need to Download the 2020 Ransomware Report

Discover why you need to download the 2020 Ransomware Report and how you will be able to leverage these findings to help protect your business against the top cyber threat of the new year. Datto has compiled survey results from over 1000 managed service providers (MSPs) to catalogue the discoveries of the previous year as told directly by the IT professionals and the SMBs they serve. The responses echo predictions made earlier and indicate a similar surge in cyber attacks in 2021 - get the Report and discover what to watch out for and how to better prevent a data breach that could encrypt your critical files.

Here are the biggest takeaways from the 2020 Ransomware Report:

Ransomware Was the # 1 Malware Threat of 2020
Despite (or because of - see below) the disruptions the COVID-19 pandemic created around the globe, the growth of malware continued virtually unabated in the past year and eventually surged due to the circumstances. Ransomware rose above all other types as the undisputed number one threat above all others and seems poised to maintain that crown in 2021. The cybercriminal ecosystem - already large enough to have its own economy - has grown around time-tested methodologies such as file encryption, which relies on proven user behaviors to guarantee a beneficial risk to reward scenario.

- **94% of MSPs surveyed predicted ransomware would continue at the same or increased pace YoY**
- **52% of victims were affected by CryptoLocker and 26% by WannaCry**

How the Pandemic and Working from Home Changed Cybersecurity
The 2020 Ransomware Report does reveal some good news for cybersecurity during the pandemic - while attack rates did grow, the increase was not as bad as it could have been. The main dividing line appears to be between those businesses that have or have not enforced clear policies against personal devices used by employees who work from home and connect to the company's network. What may be most telling is that the industries most often hit are those where data is most critical, and individual users can be leveraged for broad backdoor security access.

- **59% of respondents attributed ransomware growth to the mass remote work shift**
- **50% said Finance and Insurance are the most targeted sectors**

Phishing Emails Still Top Ransomware Vector
Asked to select their top three answers, a majority of MSPs surveyed clearly identified phishing as the top culprit for allowing ransomware to infect their clients' networks. Unsurprisingly, examples of bad employee cybersecurity practices were also included in these results, as these factors and the chosen vector go hand in hand in many cases. Many gangs employ social engineering specifically to identify and learn how to exploit the best victim that presents the right amount of gateway access and susceptibility to answering urgent emails.

- **54% of those surveyed blamed phishing emails for successful ransomware delivery**
- **26% and 27% attributed infection to bad user practice and lack of cybersecurity training, respectively**

Continued on page 3...

What our clients are saying: C. Abbonizio Contractors, Inc.

"SWK Technologies services have been very prompt and they always have a solution. A few months back a tornado came through the area and our server went down because we had lost electricity. Within an hour of calling SWK someone was at our office with a smile and cupcakes to get us back up and running."

Maureen Cleary
C. Abbonizio Contractors, Inc.

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:

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 **February 5th** to get your name in the hat.

You could win a

What SWK Managed Cloud Services Will Do for You

SWK Technologies' Managed Cloud Services (MCS) division will provide your business with the tools, guidance and support you need to navigate the complex modern cybersecurity world. Your application stack and IT assets are mission-critical in today's age of digital, and only dynamic solutions will mitigate downtime from either hackers or natural disasters. Read through the list below to discover just a few of the technology solutions MCS provides, and reach out to ASAP for a free consult to understand the full scope of value SWK will generate for your business.

Here are 11 examples of the technology and support solutions Managed Cloud Services will deliver to you:

Cybersecurity for the Cloud
Cloud-hosted environments are progressively infiltrating back office spaces, from storage platforms like Dropbox to the Microsoft 365 Office suite of apps. However, web-based endpoints bring significantly different user security concerns than traditional on-premise deployments, and which require good cyber hygiene to defend. SWK's own cloud service offers you the ability to secure your digital infrastructure with real-time protection built specifically for this new reality, with proactive intrusion monitoring.

Software & Infrastructure Hosting
Managed Cloud Services provides your business with options for deploying your applications in an online environment, letting you decide how your system consumes IT resources. Experience with both network security and software implementation allows the SWK team to customize your environment while maintaining SSAE 16, SOC 1, SOC 2 and HIPPA compliance. Choose how much of your system is hosted through our datacenter while maintaining complete control and ownership of your critical data.

Human Cyber Intelligence with SOC/SIEM
MCS enables cybersecurity in fast-paced, web-based networks by deploying a security operations center (SOC) staffed with veteran cyber intelligence and incident response (IR) professionals. Introducing this dynamic human element allows for real-time monitoring that can identify hacker footprints with accuracy and react decisively. SWK's SOC is technology-agnostic and can work with any security information and event management (SIEM) solution, in addition to being scalable to your business size and scope.

Microsoft Office Support & Guidance
Microsoft 365 (the new Office 365 for SMBs) is the widely used cloud service in the business world, and chances are you already have a license allowing for every employee to download on their devices. However, are you sure that you are capturing the best value from all parts of your installation, or are there features still untapped by your users? MCS will not only help you manage your Office deployment, but will also guide you on using every app in the suite, the web-hosted databases in OneDrive and SharePoint, and the Teams communications platform.

Business Continuity & Backup for ERP
Having a thorough business continuity plan (BCP) is critical as your processes go through digital transformation, but are you certain your current strategy is fail-safe? Even the most basic (but integral) step, backing up your data, requires that you choose the right solution(s) for the software where your files live. With SWK's in-depth knowledge of the IT needs of various ERP and industry-specific applications, we can help you track and deploy a BCP that fulfills your requirements, including for compliance.

Disaster Recovery from Ransomware
Disaster recovery solutions allow your business to survive the impact from several threats, but one of the most important factors is the ability to restore your systems after a ransomware infection. These types of attacks have been growing in sophistication as well as persistence, and the gangs that use them have put in increasing effort to prompting victims to pay. The only two effective solutions have been to prevent one and to ensure data can be backed up - SWK will help you maintain regular backups as well as redeploy clean files in the event of a breach.

Malware Protection & Antivirus
Modern business continuity and cybersecurity require more than traditional antivirus, but that does not take away the value of having these programs in place as a first layer of defense. MCS provides comprehensive and advanced antimalware solutions that will help keep your network protected against multiple types of attacks and user-level intrusions. These firewalls are designed to fight against modern cyber threats in the background without disrupting work, leveraging automation to streamline incident response.

User Security Tools & Training
User security can often the final line of cyber defense, yet so many employees remain in the dark about their vulnerability to various forms of cyber attack, including phishing and remote code execution (RCE). SWK will arm you with the tools you need to establish multiple layers of cybersecurity, as well as training that empowers everyone in your organization to spot red flags. With solutions such as multi-factor authentication (MFA), virtual private networks (VPNs) and email encryption along with the right education, your business will be able to defend your data.

Network Vulnerability Testing
Penetration testing of your IT systems not only offers a good accounting of your security posture, but has become a compliance with several consumer privacy regulations. To help you determine if you are at risk of a data breach, MCS can conduct a Network Vulnerability Test that will map and scan up to five public IP addresses. A detailed report of our findings will help you discover any potential concerns before they become a liability, with follow-up support and strategy discussions to address those issues found.

Virtual Desktop & Server Deployment
Desktop and server virtualization enable you to consolidate hardware while scaling the available amount of interfaces for each user in your network. SWK will host your resources offsite or on-premise and provide continuous support for your environment that includes health monitoring and data recovery. We will work with you to design and deploy a solution that fits your needs, tailored to the devices you use and condensing touchpoints to those you require.

Co-Managed IT Support from Managed Cloud Services
Even if you have an existing in-house IT department, your business undoubtedly still has a hard time addressing every issue in your system, especially during periods of growth. SWK can augment the efforts of your existing internal team with expert guidance, fast network support and the resources of a larger, dedicated firm. Our co-managed IT service grants you the ability to plug in the gaps that your technicians are often too stretched to address day-in and day-out, and ensure that your infrastructure is handled with care .

Contact SWK MCS Today
Technology accelerates your business, but also added a whole host of new IT assets you either need to manage, or need to acquire to keep your systems running. SWK Managed Cloud Services will handle the breadth and depth of your stack from software applications to hardware to hosted environment, cybersecurity and support for each and every piece of it. Let SWK Technologies help your team manage your network with efficiency and pivot for the future.

Contact MCS today to discover what we can do for you and your mission-critical assets.

Shiny gadget of the month: Razer's Project Hazel

Each year the Consumer Electronics Show (CES) takes place showcasing some of the latest tech for the upcoming year. There are always lots of cool gadgets to look at, but one that stood out due to today's "new normal" was Razer's "Project Hazel" face mask. Razer, normally a gaming focused company has designed a face mask that is reminiscent of their gaming offerings with lights and a sleek design.

The mask itself is packed with tech too, it is not just a cool looking gadget, but a useful one too. It has a N95 surgical respirator for protection and a detachable ventilator to regulate airflow. The design for the face shield is transparent so people can actually see your mouth and with a low light mode it will light up the interior when it is dark. Something that is really unique to Project Hazel is it has a built-in mic and amplifier combo to project your voice so you are not muffled. Since Razer couldn't resist adding some flair to this cool gadget, they added customizable lighting offering over 16 million colors and a suite of effects for you to give some individuality to your mask.

If you're concerned about something like this inhibiting airflow they've taken steps to prevent that. With replaceable filters and optimized airflow that allows cool air to come in and release heat produced from exhaling and CO2 build up it promises to give you a great experience. It also has an air-tight seal and has adjustable bands to ensure it fits comfortably on your face.

One of the coolest features of this mask is that it has a dual-purpose charger. When you are home and ready to take your mask off you place it in a wireless charging case that not only charges it up, but sanitizes it with a UV sterilizer.

Unfortunately, Project Hazel is not quite ready for distribution and does not have a price associated with it or a release date set. However, based on the prototypes and the amount of detail they've put into this hopefully it will not be far off. You can check out more along with a video on their website https://www.razer.com/concepts/razer-project-hazel.

Why You Need to Download the 2020 Ransomware Report

Continued from page 1 ...

The Cost of a Data Breach and Downtime
The majority of survey respondents in the 2020 Ransomware Report made it clear that clients that experienced infection saw serious impacts to productivity, and quite a few experienced much more severe consequences over time. Data and devices had to be discarded, profits were lost, and many had to shut down their entire systems. Downtime costs rose exponentially as well this past year, increasing the damage done by a successful data breach.

- **62% of MSPs said victims saw a serious loss of productivity while 39% experienced downtime**
- **Downtime costs from ransomware increased 94% since 2019**

Windows Systems Are Top Targets of Ransomware
Given the popularity of Microsoft products across the world, it should be no surprise that Windows PCs made up the vast majority of infected machines among the respondents. Additionally, many servers were also impacted by ransomware as well as deployments of Office 365. Cybercriminals will use their malware to infect as many systems as possible once they have successfully breached a network, and legacy endpoints - as well as improperly configured cloud connections - can provide them with backdoor access opportunities to spread it outward from one victim.

- **91% of those surveyed said Windows PCs were targeted**
- **76% said Windows Servers were infected and 64% said the same for Microsoft 365**

Gangs Are Refining Methods to Bypass Security Controls
The Report revealed that MSPs saw noticeable signs that ransomware gangs were modifying their malware to bypass traditional IT security controls. This reflected a trend of increasing of sophistication among both the perpetrators and their attack vehicles, including more refined social engineering tactics.

- **59% of respondents said antimalware solutions were averted by ransomware breaches**
- **42% said legacy antivirus software was bypassed by infections**

SMBs with Business Continuity Averted Downtime
Perhaps the best news out of the 2020 Ransomware Report was that SMBs with business continuity and disaster recovery (BCDR) solutions in place managed to avoid serious downtime. The majority were able to restore their systems with some form of data backup, while only a fraction paid the attackers a ransom. Other effective measures were also highlighted by the respondents, including employee cybersecurity training and patch management.

- **91% of MSPs said that clients with BCDR solutions avoided significant downtime**

Download the 2020 Ransomware Report
These are only a portion of the takeaways from the Report - the past year has provided a wealth of data to review and quantify to gauge the threat that ransomware poses in 2021. Download the full survey results and leverage these findings to begin refining your security strategies for fighting malware.

Download the 2020 Ransomware Report here and reach out to SWK Technologies ASAP for help in building your cybersecurity strategy.

What You Need to Know About Cyber Insurance in 2021

Here is what you need to know about cyber insurance not only if you are considering a plan in 2021, but even to be able to secure an effective policy at any point in the near future. The growth rate of data breaches established in previous years only escalated during the COVID-19 pandemic, and 2020 is expected to have a significant impact on future policies. Insurers offering coverage plans for cyber incidents must adapt to these lessons, and reinforce clients' obligation to meet a cybersecurity standard to preserve policy value.

Here are a few things you need to know about considering cyber insurance for 2021:

Traditional Insurance Offers Little Respite for Cybersecurity
Cyber liability coverage emerged because traditional insurance policies address little, if any, of the damages resulting from a network disruption. This reflects the harsh game of catch up many industries have had to play in pivoting to the age of digital transformation and widespread Internet connectivity, but the impact here is felt on the customer side most. This means the only economic respite for your business after an incident will typically be with a specific type of coverage policy offered by a select number of providers.

Cyber Insurance Requires Risk Assessment and Management
Cyber insurance policies, like all coverage plans, are developed based on the risk a client will statistically face and that the insurer will take on financially. Cyber risk in particular, of course, has risen steadily year after year and virtually exploded in 2020 with the mass shift to work from home environments along with the growth of phishing scams. Providers will have to further reevaluate liability for potential customers in 2021 and are guaranteed to demand greater cybersecurity enforcement on latter's end.

Read the rest online here https://www.swknetworkservices.com/what-you-need-to-know-about-cyber-insurance-in-2021/

Gift Card Trivia!

This month's question is:

According to the Ransomware Report. 91% of MSPs said that clients with ____ solutions avoided significant downtime. (Hint: The answer is in this newsletter.)

a. Macs
b. BCDR
c. Antivirus
d. Firewalls

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **February 5th,** 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

When is the Right Time to Consider Cloud Hosting?

If you are unsure when is the right time to consider **cloud hosting**, then reading through the 10 signs below will help you determine when your business is ready to take the next step and begin your migration. Bringing your software and IT into a digital infrastructure will present many opportunities to mitigate your traditional pain points and consolidate costs, time needed to execute on tasks and the number of touchpoints decision-makers must go through to access data. Hosted environments deliver better flexibility, scalability and speed than on-premise deployments, which enables you to streamline your processes and propel your operations into the modern age.

Here are the 10 signs that it is the right time to consider cloud hosting for your mission-critical assets:

Competitors Are Outpacing You with Cloud Hosting
Investments in digital transformation are growing YoY (year over year), including in SaaS (software-as-a-service) technologies, and some of your competitors are likely within this grouping. If you find yourself being regularly outpaced in speed to market, there is a good chance those businesses have already begun migrating away from older systems, optimizing their operations around their new deployment and leveraging the boost in productivity. The increased access to real-time data, in a world where information velocity outweighs volume, also provides a competitive advantage to disruptors seeking to edge past historical players with more innovative ideas.

Your Systems Are Much Older Than Your Workforce
Whether you believe it began with Millennials or Gen Z, the global market is being progressively taken over by **digital natives** who have considerably different expectation of technology than previous generations. If your legacy systems were in use before this incoming workforce was even born, then you will undoubtedly have issues with user experience that will translate to a lack of efficiency. The UX and functionality of your user-facing IT should mimic what your employees see in consumer spaces, with web-based applications leveraging browser interfaces and seamless data delivery.

Servers or Other Hardware Need Costly Upgrades
Perhaps the most obvious sign it is time to consider cloud hosting is that your hardware capital expenses are eating into your budget, especially costly server upgrades. Having to replace expensive machines you already much in - just to repeat the cycle again in a few years - will begin to impact your margins, while moving to a digital environment will remove this toll on your business. Even hybrid infrastructures require fewer physical resources onsite, meaning there is less of a maintenance burden on your part and pricing will be reduced to operating overhead instead of upfront expenditures.

Current Cloud Applications Live in Disconnected Silos
If you have a subscription to Microsoft 365, Dropbox, or any other number of online services, then you are already hosting data in the cloud. However, having your mission-critical applications living in separate silos eliminates a huge benefit of migration, as without any native integration or customization those files will still have to be transferred manually between systems. A single provider will be able to unify your disparate databases and ensure your users will be able to seamlessly access their information with the right role-based permissions.

You Lack the Internal Resources to Handle Cybersecurity
Cybersecurity within web-based environments has been consistently scrutinized, but the truth is that you already have remote endpoints within your network (misconfigured RDP, legacy systems, online apps etc.) that must be covered. If you are hard pressed to handle all your obvious IT needs with your existing internal resources, then you are especially vulnerable to these backdoors and it is only a matter of time until they are discovered (by hackers OR regulators). Cloud service providers (CSPs) can deploy proactive security monitoring over your hosted infrastructure that will methodically identify gaps and potential intrusions before they impact your data.

Software Updates Cause Too Much Downtime
On-premise server deployments by definition require manual interaction for maintenance, which means that your IT team must meticulously go from machine to machine to upgrade your existing hardware AND software. This inevitably will cause downtime across your network as workstation computers have to be forced offline in order to complete the process, which will of course cut down your productivity. Yet with cloud-hosted applications these updates can be performed in the background and with minimal disruption to your network users, letting work continue seamlessly and uninterrupted by burdensome system requirements.

Your IT Team is Stretched to the Limit
Having to bounce between every single touchpoint within your systems, from servers to workstations to every other mission-critical asset, will eventually take a toll on your in-house IT team, if it has not already. Stretching your internal resources too thin eventually leads to issues being overlooked, which with the amount of manual oversight on-premise systems need will create endless fires to put out and continuously extend the cycle. Consolidating those touchpoints through cloud hosting grants some breathing room as well as allowing you to leverage real-time backend support from your provider.

Remote Workers Need to Be Connected to Your Network
The COVID-19 pandemic demonstrated the value of having a distributed workforce strategy, however it also revealed the consequences for relying on remote workers without policies in place for IT oversight. If employees are working from home, they need to be able to interact with their data either through remote desktop access or through cloud connectivity. The latter enables you to obtain additional cybersecurity and support for all of the additional endpoints those users will contribute to your potential attack surface and protect them in real-time.

You Are Falling Behind Your Ecosystem in Migrating to Cloud
As the rate of cloud adoption grows, you will undoubtedly see progressively more deployments among third parties throughout your value chain and within your partner ecosystem. You will also inevitably run into issues attempting to connect your legacy software with their hosted applications, if you have not already. Lagging behind does not only impact your standing with your competitors, but among all of your stakeholders as well, and continuing to employ outdated systems will eventually disrupt these relationships.

Regulations Move Faster Than Your Compliance Can Keep Up With
Recent years have seen considerable reinforcement of existing regulations, including a strengthening of data privacy across US states and international collectives, expansion of transparency rules throughout manufacturing, and crackdowns on ransomware payouts. This is to say nothing of the regular updates made to tax law details every year, and having to manually update your systems annually only adds to your Year-End accounting tasks. A hosted software environment will ensure your compliance data is updated in the background based on preprogrammed rules that prevent disruption and inaccuracy equally.

Contact SWK to Find the Right Time for Secure Cloud Hosting
If you are experiencing any one of these signs - or the dozens of other red flags signaling your legacy set up is on its last legs - then it is the right time to consider Secure Cloud Hosting by SWK. Reach out to us to learn more about this comprehensive service, including how we can provide real-time data protection and network support for your hosted environment.

Contact SWK Technologies today to learn about our cloud hosting and support services, and discover how to bring your technology into the future.