IT Strategy Brief

ISSUE 3 | VOL 7 | March 2021

INTEGRATE SEAMLESSLY

SWK MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

HOW THE BIDEN ADMIN PLANS TO CHANGE US CYBERSECURITY

One of many challenges facing the new presidential administration is national cybersecurity, and Joe Biden's team has revealed a few plans in motion to add some change to policy in this area. However, there are many political and economic factors at play that will greatly influence how this strategy is executed on.

The SolarWinds Orion hack which first came to light in December 2020 is suspected to be the biggest data breach of the US government in history. This has been followed by yet another audacious attack uncovered in the Microsoft Exchange Servers that power email communication around the world. Although the new president's admin has avoided drastic changes to his predecessor's cyber policies, these incidents reinforce the impetus for strengthening cyber defense at the federal level down.

Here are a few ways that the Biden administration is planning to change US cybersecurity policy and the developments that will drive these changes:

CYBER POLICY CHANGES FROM TRUMP'S TERM

Former President Trump deprioritized protecting cyberspace as a government initiative, eliminated roles and offices that oversaw cyber defense and diplomacy, and lost several officials in charge of driving cyber policies to political infighting over the course of the four-year term. Despite this, there were efforts by several members of the cabinet to revitalize a federal cyber defense program, including the creation of the Cybersecurity and Infrastructure Security Agency (CISA) in 2018. Yet this was one of the departments hardest hit by the turnover – even CISA's director was fired after a public election fraud claim dispute.

Since at least the SolarWinds hack came to light, Biden has worked to position himself as taking a much different approach, albeit without making too many explicit promises (yet). The new president has stressed a return to process and a procedural approach to fighting cybercrime and nation-state hackers, with consistent emphasis on the latter.

THE BIDEN CYBERSECURITY DREAM TEAM

Part of the refocused efforts on cybersecurity will include the hiring of a "dream team" of appointees with extensive experience in combating cyber threats and navigating the complexities of discreet cyberwarfare. Among this assortment are veterans of both the Trump and Obama administrations, including the leader of the response to the SolarWinds attack, Anne Neuberger, who serves in a newly created position. Congress has also passed legislation for the creation of a National Cyber Director which will directly oversee policy in both the public and private sectors.

Continued on page 3...

What our clients are saying: Pee Jay's Fresh Fruit

"SWK's response time has been great. There have been many times we've submitted an email with an issue and received a call back within 5 minutes. Very impressive!

Shay always goes above and beyond. Earlier this year we had an email issue with an outside vendor, and he got involved - even contacted the outside vendor himself - and made sure to stay on top of the situation. When I put it on the back burner, he still was working on it and even though it was not a quick fix, he helped resolve it!

Our biggest benefit by working with SWK is that we have confidence that if any IT issues arise, they will be dealt with quickly. If it's not a quick fix, it will be thoroughly examined and diligently worked on until it's completed."

Anthony D'Agostino
Pee Jay's Fresh Fruit

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:

Christine Chiaravalloti
American Asphalt Company

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 **April 9th** to get your name in the hat.

You could win a $25 Gift Card!

9 WAYS CYBER RESILIENCE KEEPS YOU COMPETITIVE

There are many ways that implementing and enforcing cyber resilience throughout your business will give you a competitive advantage in your market, chief among them the ability to ensure your company's continued survival. A complete lack of cybersecurity or relying on an outdated security posture will inevitably lead to unsustainable losses in one form or another, often resulting in a combination of consequences. There are many very expensive ways that a cyber attack could impact your business's well-being and eventually force you into bankruptcy.

Beyond protecting your bottom line revenue, there is still much benefit to maintaining a brand synonymous with being cybersecure in an era of rampant data breaches, digital theft and ransomware lockdowns. Communicating with your customers your commitment to preserving the integrity of their personal information will go a long way to building trust and strengthening those relationships, especially when your competitors are unable to guarantee the same.
Here are nine of the ways that investing in your business's cyber resilience will keep you competitive in your market:

1. HAVING NO CYBERSECURITY WILL PUT YOU OUT OF BUSINESS
The world has gone well past the point where anyone could believe they will be safe from the tens of thousands of new cyber threats that appear every day, including in the SMB space. Too many smaller and medium-sized businesses have found out the hard way that not only are they a target, and a preferable one at that, but that they are more likely than larger enterprises to have to shut down after a cyber attack. Between noncompliance fees and lost value from data stolen (including IP to competitors) or damaged, network shutdowns and disgruntled customers, a successful breach will mount so many costs that a firm like yours will simply be unable to absorb.

2. REDUCING DOWNTIME PRESERVES REVENUE
One of the biggest dangers from a malware infection – especially with ransomware – is from downtime that will block system access to internal and external stakeholders. Employees will be unable to access the tools and data they need to fulfill their roles, and customers will be unable to interact with any forward-facing digital assets, such as your websites. Without an effective business continuity plan in place, you risk losing all productivity during the time your network is down as well as taking a hit to your brand reputation (especially if hackers manage to take control of your web properties).

3. AVOID DATA PRIVACY COMPLIANCE FINES
If you need a reminder that data privacy compliance is intensifying across the country and the world over, then you should consider performing a risk assessment of your systems in case of an audit as soon as possible. Regulations are playing catch up with how commodified personal information has become, putting your business in the firing line for the next example to be made demonstrating the seriousness of these laws. There is a double irony in that any customers you lose to mishandling a breach will make the fines that much more impactful, and your cyber resilient competitors will receive a boost to their brand at your expense.

4. LEGACY SYSTEMS CREATE NETWORK VULNERABILITY
This is an age of technological growth, yet many smaller firms have chosen to squeeze every ounce of productivity from software bought years or even decades prior. Investing in new applications (and the IT infrastructure to run them) can be a tough decision to make, especially when you know something like QuickBooks is too small for your needs, but you cannot afford to migrate to a better product every year. Unfortunately, these legacy systems represent a huge network vulnerability that can be exploited with the right external factors as well as provide diminishing returns in productivity, and both factors can impact your relationships with your customers.

5. EMPLOYEES WITHOUT CYBERSECURITY TRAINING CAN EXPOSE YOU
Your network users are your first and last line of cyber defense, yet too often employees lack comprehensive cybersecurity training that would enable them to protect your systems. This includes leadership as well, as C-suite executives are the biggest targets of corporate-level cyber attacks, but too frequently are just as uninformed as anyone else in the company. Investing in proactive education on cyber threats and best practices for your user base will ensure that your business will lose to random breaches and be able to maintain data integrity.

6. DIGITAL TRANSFORMATION NEEDS CYBER RESILIENCE
If you have made plans to migrate away from legacy systems to more modern applications, then you still need to implement new cyber resilience policies to handle the security impact of new technologies, such as the cloud. Digital transformation brings many potential benefits as well as drawbacks if not handled correctly, including the introduction of new endpoints that could expand your attack surface if employees lack cybersecurity training. To maximize the value your migration to modern technology will bring, you must educate users on and enforce cyber hygiene so as to safeguard the growth facilitated by these new tools.

7. CONTINUE WORKING FROM HOME WITH CLOUD SECURITY
The COVID-19 pandemic forced a new normal on businesses around the globe, but research suggests that the next normal will look like a (more comfortable) hybrid of the telecommuting environments social distancing created. However, to ensure your employees can continue working from home safely, you must take steps to maintain your cloud security controls to be able to allow the remote connections that make it possible. A hosted infrastructure that is protected against the cyber threats that target this deployment model will be able to deliver the best ROI and enhance your competitive advantage.

8. YOU NEED DATA SECURITY FOR INTERNAL CYBER THREATS
While external cybersecurity is important, it is also critical to secure internal access to defend against either potentially malicious insiders or prevent human error from causing damage to your sensitive files. Hackers can be so bold as to walk into your workplace in a traditional office setting, and even while working remotely there are always backdoors that can be exploited by an intruder trying to pass themselves off as someone known to your system. Your information controls should be able to segment user permissions based on role as well as provide redundancy in case an attacker gets past one layer, or your business could face the consequences of your data being compromised.

9. EDUCATING CUSTOMERS ON CYBER RESILIENCE BUILDS TRUST
The list of internal value points for investing in cybersecurity goes on longer than the one presented here, but another area where cyber resilience will provide external benefits is with your customer relationships. The uncertainty around cyber threats affects them just as much as you, if not more, and providing guidance and education will go a long way towards strengthening their trust in your brand. Everyone is looking for the right information in these unpredictable times, and sharing what knowledge you have earned within your ecosystem will ensure that you are both all protected, and equally committed to preventing the data your share from being exposed.

DISCOVER HOW TO PROTECT YOUR BRAND WITH CYBER RESILIENCE
Cyber resilience requires practice, repetition and a lot of patience, but ultimately maximizes your ROI on your software and IT infrastructure by ensuring the value of both your network assets and brand is secured. Hackers will be a reality as long as the Internet is around, but you can avoid becoming another victim of cybercrime by implementing time-proven tactics and the right cybersecurity support and service.

Download SWK's free ebook here to learn more about the steps to fighting back against cyber threats and how to leverage these techniques to remain competitive.

Shiny Gadget of the Month: Meater Plus

Spring is officially here and after a winter of being couped up everyone is ready to get back outside and enjoy warmer weather. That also means that it is grilling season. Grilling just makes everything taste a little bit better, but the trouble with grilling can be getting things cooked just right. Overcooking or undercooking something can totally ruin it (or just be plain unsafe). It is a total disappointment to sit down to eat your meal, cut into your food and find out it is undercooked. Then you have to go back out fire up the grill again and finish cooking it.

The days of meat that hasn't been appropriately cooked are over! Meater is here to save the day with a truly wireless meat thermometer that not only works with you smartphone, but will also help you determine how long it will take to cook as well as set alerts to notify you when it is done. Sure, you can get a simpler meat thermometer, but you have to wonder what the temperature is and constantly check on it. Let's just be honest it is more fun and convenient with modern technology.

Here's how it works. The Meater Plus uses built-in Bluetooth to extend the range of the probe up to 165 feet so you don't have to hover over the grill and you can go and enjoy yourself. It uses two sensors that monitor the internal temperature of the meat as well as another to monitor the ambient temperature. Using the guided cook system in the app it will walk you through the process and estimate based on the temperature readings how long it will take to cook. It literally takes all the guess work out of cooking and you will get perfectly cooked meat every time.

The Meater isn't restricted to just the grill either. Since it is wireless you can use it in the oven, a smoker, a skillet for example. This little gadget will save you time, stress, and save food from being ruined. Guessing when your food is done has always been a challenge, but this makes things easy.

Right now the Meater Plus comes as a single probe and charging station, but there is a more expensive option if you wanted multiple probes too. At $99 for the Meater Plus it is by no means a cheap meat thermometer, but the technology and versatility of it makes it an intriguing buy for anyone who can relate to the struggles in this article. It could be the perfect gadget for this Spring and Summer for any grilling (or cooking) enthusiast. You can see it in action for yourself on their website meater.com.

HOW THE BIDEN ADMIN PLANS TO CHANGE US CYBERSECURITY

FIRST SOLARWINDS NOW MICROSOFT EXCHANGE EMAIL SERVERS HACKED

Biden's cybersecurity team will have a lot to contend with no matter what form their jobs take, as this latest breach may dwarf the one that was uncovered in December. While the SolarWinds hack was estimated to affect at most 18,000 businesses, the Exchange attack could impact at least 30,000 organizations (the number continues to climb at the time of this writing), but there were "hundreds of thousands" of email servers breached according to multiple sources. The hackers seemed to have purposefully waited until the situation on January 6, 2021 distracted the government to leverage bugs in a March 2020 patch.

HACKERS BEING SPONSORED BY RUSSIA AND CHINA

Complicating the news of these two major cyber attacks are the accusations that their signatures can be traced to groups that are allegedly sponsored by rivals abroad. The SolarWinds breach has been attributed to Russian cyber spies while one of the groups involved in the Microsoft email hack are believed to be employed by China. Additional revelations make the situation even worse, as it is now suspected that the former incident also included Chinese hackers working in tandem with Russia's nation-state actors.

These disclosures have only reinforced the aggressive stance Biden's team has communicated repeatedly regarding these two nations. Now, however, foreign policy will extend into cyber defense and diplomacy, and perhaps even cyberwarfare in response to the blatant espionage.

BIDEN VS TRUMP ON CYBERSECURITY

Despite the more inflammatory sound bites, Biden's interim policies on cybersecurity are similar to what the Trump team proposed in 2018, which but for wording and language focus on all but one of the same general points. The facilitation of direct government aid and involvement is the biggest differentiator between the two presidents' cyber plans, followed distantly by the inclusion of Russia in the list of targeted enemies. It is also important to note that Neuberger herself is a holdover from the previous administration, and CISA and the State Department still retained some career officials with expertise in this area, so the continued course is at least partly due to the makeup of the current team.

However, this strategy can and should be expected to change – at least somewhat – in the face of various challenges. Even without a political need to separate themselves from Trump's policies, the new White House find themselves in battle that could progress into full-blown cyberwarfare.

PRESIDENTIAL AND CONGRESSIONAL SECURITY POLICIES IN MOTION

There are several proposals in motion as well as bills being pushed through legislation in response to the nation's cybersecurity situation, as well as quite a few actions already underway to combat the more immediate threats. Here is a list of all of those we have been able to find compiled for your convenience:

- **Plans to pass at least 8 additional executive orders addressing gaps made apparent by SolarWinds hack**
- **$10 billion of funds included in the February COVID-19 relief package earmarked for investment in IT security**
- **Executive order directing federal agencies to conduct a two-part supply chain security review, with a mandated assessment of communication and information technologies**
- **New trade restrictions have been added to Chinese tech companies such as Huawei and ZTE**
- **Clandestine action to be taken against Russia, followed by the imposition of additional economic sanctions**
- **A bill proposed by Rep. John Katko (R-N.Y.) centralizing CISA's role for incidents in industrial control systems (ICS) in the manufacturing sector**
- **Passage of The Internet of Things Cybersecurity Improvement Act in the House**
- ***The Homeland and Cyber Threat Act proposal, which would allow alleged victims to take international hackers to court***

YOUR BUSINESS SHOULD AUDIT YOUR CYBERSECURITY

Time will tell how effective the Biden administration's plans will be at combating these new cyber threats, but in the meantime, you must take whatever steps you can to enforce your own internal cybersecurity. The Cyber Cold War that has persisted is inevitably heating up, and businesses in the US of every size will be caught in the crossfire (and have already). Even the smallest of organizations will be a legitimate target in this type of conflict, as the connected nature of networks means every piece contributes to the health of the overall system, and adversaries will be looking to do damage before tensions cool down again.

CONTACT SWK TECHNOLOGIES TO SUPPLEMENT YOUR CYBER DEFENSE

SWK Technologies has a host of cyber threat protections available that empower you to create additional layers of defense against attack, from basic MFA to a military-grade SOC. Reach out to us ASAP to let us help you discover the level of cybersecurity you need to deploy to keep your business network secure, and prepare for whatever may happen in the future.

Contact SWK today to learn more about our cybersecurity services and how we can help you strengthen your cyber defense against all manner of threats.

Gift Card Trivia!

This month's question is:

Reducing ____ preserves revenue. (Hint: The answer is in this newsletter.)

a. Employees
b. Downtime
c. Security
d. Resilience

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **April 9th,** 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

8 REASONS WHY SMBS NEED CYBERSECURITY PROFESSIONALS

Between the variety of cyber threats out there and the significant impact they can have on your business, there are many reasons that SMBs need cybersecurity professionals who can help spot and fight back against malicious activity. Cyber risk appears in many forms and can attack from multiple angles with the right knowledge, whether a sophisticated hacker leveraging a detailed social engineering campaign, or an insider that intimately knows where your network is vulnerable.

Most employees are not trained to see the red flags from all but the most basic cyber scams, or even to avoid actions that could expose your data to external dangers. Even if you can afford an internal IT team, they are likely already overwhelmed and cannot handle everything coming their way, let alone recognize intrusion from skilled hackers. With the rate at which malware and other threats continue to evolve, only committed experts and robust solutions will be able to cybersecure your business.
Below are eight reasons SMBs need cybersecurity professionals, and a few ways they can protect against these same cyber threats:

WHAT CYBERSECURITY PROFESSIONALS CAN OFFER TO SMALL BUSINESS
Traditional managed service teams may have had to fulfill security roles in the past, but this is ultimately a stopgap approach. Many types of modern cyber attacks are well outside of the expertise of all but the most well-trained and experienced IT technicians, and even they are ill-equipped to identify more sophisticated hacks. The cybercriminal ecosystem is filled with many amateurs, but also contains several highly-skilled enthusiasts and cyber warfare veterans that prey on targets of opportunity.

Trained cybersecurity professionals versus traditional IT personnel fits into a "doctor VS bodyguard" dichotomy – one maintains your health while the other protects it from outside threats. A medical specialist may be able to treat an illness, but you need close point protection in the moment if someone is trying to cause you physical harm.

1. SMB IT TEAMS ARE OVERWHELMED (OR LACKING)
With the shift to work from home environments with the pandemic, network engineers that were already overwhelmed now had to manage a remote workforce lousy with personal device usage and bad cyber hygiene. Then there are those SMBs that cannot afford an internal IT team, and have been forced to rely on anyone with a little bit of technical knowledge to fulfill the role – the danger of which should become obvious as you continue reading. Without the bandwidth to do so, even the best equipped team will need the help of professionals to catch cybersecurity gaps that can fall out of notice.

2. YOUR EMPLOYEES NEED CYBERSECURITY TRAINING
Employees are the first and last line of cyber defense, yet too often this fact is overlooked or just deprioritized in favor of other activities, usually until it is already too late. You can implement one zero-trust policy after another, but sooner or later network and data access will be required to allow someone to fulfill their role. It is much more cost-effective in the long run to ensure every one of your exposed endpoints has a defender, which is why users must receive training from professionals that know what they are doing.

3. INTERNAL NETWORK SECURITY IS OFTEN OVERLOOKED
While you can spend all day worrying about external cyber threats, the biggest danger to your system is from anyone with insider access. There are many worst case scenarios where an employee – or someone who has gained access to or is posing as one – can steal data without tripping any alarms because they know how to get past the controls. However, often the real peril lies in how much damage a user can do even when not being intentionally malicious, and without proactive cybersecurity monitoring you will likely not know until it is too late.

4. DATA PRIVACY REGULATIONS AFFECT SMALL BUSINESS TOO
It may be easy to look at the language of policies like Europe's GDPR and California's CCPA, among others, and assume that they are meant exclusively for enterprises. That can be a costly mistake, as even small businesses will end up collecting huge amounts of personal data and privacy regulations specifically target this practice and all who participate in it, including SMBs. At even the most basic level of compliance, you will require some kind of security controls in place to demonstrate that you have committed resources to protecting your customers' information.

5. CYBER INSURANCE PREMIUMS CAN BE IMPACTED BY YOUR CONTROLS
Cyber insurance may seem like the cost-effective answer to fighting against the financial impact of hacking, but it is important to note that it is still a system based on liability. Firms have had to adapt to the surge of cyber threats and data breaches, and your business's cyber risk will have a significant impact at your premium rates, if you are even able to meet the minimum cybersecurity standards to acquire a policy.

6. CLOUD SECURITY REQUIRES PROACTIVE DATA BREACH MONITORING
Having cloud security is only going to grow in importance as technology goes increasingly in the direction of web-based functionality, with benefits that were made obvious during the pandemic. So many popular systems connect with external networks at one stage or another that it will eventually be impossible to avoid the risk of exposure at some point. Your cybersecurity posture must be proactive to protect yourself in this reality, or you must engage professionals that are able to fill this gap.

7. THE COSTS OF HAVING NO CYBERSECURITY IN PLACE ARE GREAT
When all is said is done, investing in a dedicated security solution can seem like an expensive proposition for a SMB, but the truth is that the price of doing nothing can be much, much worse. Noncompliance fines from a data breach, stolen IP, frozen productivity during downtime, and lost customers are just a few of the ways that just one hack can hit your wallet hard. The cost of cybersecurity may seem like considerable from a smaller business standpoint, but often not having it can end up being exponentially more expensive.

8. PHISHING AND RANSOMWARE ATTACKS ARE GROWING
Research revealed that many of the worst cyber threats – including phishing emails and ransomware infections – grew in attack rate during 2020. Even as the COVID-19 vaccine is distributed and some businesses decide to return to the office after working from home, there are few signs that these trends will dissipate. The lessons learned by hackers during this period have only armed them with proven methodologies that can be used again and again.

DISCOVER PROFESSIONAL CYBERSECURITY SOLUTIONS TAILORED FOR SMBS
Investing in a dedicated network security deployment may seem like an expensive proposition, but the cyber threat protection solutions offered by SWK Technologies have been designed to deliver cybersecurity professional help at SMB and midmarket prices. Do not let your business fall into the crisis hackers create for small and medium-sized companies around the world – discover what to watch out for and how to best fight back.

Download our free white paper on the cybersecurity crisis and learn what you can do to protect your business better with the help of the professionals at SWK.