IT Strategy Brief

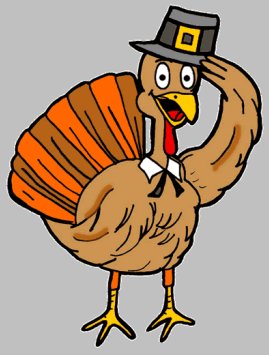
ISSUE 11 | VOL 5 | November 2019

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology Ideas for Your Business"

What's Inside:



The Cost Benefits of Having Cybersecurity

You are probably used to hearing about how scary the whole topic of cybersecurity is (we take some responsibility for that…), but adopting better security brings many benefits as well. The number one advantage, of course, is saving money on what could otherwise be a significant (and reoccurring) expense. However, network and information security have value beyond even the preventive measures, including granting your business a competitive advantage in a time of increased SMB hacking.

Here are the cost benefits to your business of having a cybersecurity solution in place:

Security Delivers a Competitive Market Advantage
In the many examples of phishing scams today, a common theme is the victim being frauded by someone posing to be a vendor or customer. This is no coincidence – hackers know that supply chains are both vulnerable and fast moving, with endpoints freely sharing data yet lacking security transparency and often any breach disclosure practices. Trading with anyone these days brings cyber risk, but it increases substantially when a partner is complacent about their cybersecurity.

No enterprise wants to suffer from someone else's negligence, and many have already taken steps to enforce better risk prevention. This is likely to intensify as larger US businesses continue to be exploited through supplier or vendor access points. Those SMBs that implement a security solution sooner rather than later will get ahead of this trend and ensure they stand out as a valuable partner.

Cybersecurity is a Business Requirement
As the above illustrates, cybersecurity is long past being a luxury for small businesses. Having network security practices in place is as integral as any other IT requirement, and necessary to mitigate inevitable cyber risk. Additionally, the growth of data protection regulations means that your business is already obligated to protect personal information, and future legislation will only reinforce that responsibility.
It is important to note that the core concept of these laws mirrors what would be expected for storing physical copies of personal files. Just as keeping a locked filing cabinet protects you from what would happen if that information was stolen, a cybersecurity solution ensures that your data is being similarly defended.

Protect Your Business Costs with Security Best Practices
Cyber defense is not an added expense – it is the most cost-effective approach to avoid increasingly expensive data breaches and phishing scams and stay compliant with information security regulations. Implementing modern cybersecurity practices is the best way to get ahead of the inevitable costs of doing business in the digital era, as well the steep price of not being protected.

Download our free e-book, Cybersecurity Tips for Employees, to learn more about the best methods to protect your network.

What our clients are saying: Family Resource Network

"My favorite thing about SWK is the piece 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

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!

Last Month's Contest Winner:

Peggy Harrington
LM Service Co Inc

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 **Dec 2nd** to get your name in the hat.

You could win a $25 Gift Card!

Executives Increasingly Becoming Liable for Cybersecurity

Legal and IT experts warn executives, and both nonprofit and corporate boards, to prepare for increasing liability being placed on their shoulders for cybersecurity breaches. Bodies such as the Securities and Exchange Commission have repeatedly called on business leaders to take charge of their network security controls and report potential breaches much more promptly. However, it has largely been left to the state level to impose regulatory pressure on these mandates.

This may change, even as states begin to directly penalize directors for data breaches. The SEC is taking a greater responsibility for information security best practices, and some independent institutions believe that the federal level as a whole should be enforcing more stringent breach disclosure requirements. The momentum is building for legislation as comprehensive as the EU's GDPR to be implemented in the US, and any form that law takes will likely be aimed at regulating the security role of leadership positions.

How Executive Practices Affect Network Security
All employees are cybersecurity liabilities, but executives are the most valuable targets of any hacker. Whether for corporate espionage, political objectives or simple theft, business leaders represent the best opportunity for unprecedented data access many bad actors seek. C-level officers, depending on their exact position, can provide a gateway to finance, operational, engineering, human resource and many other types of confidential information that can be profitable for many types of cybercriminals.

Director Liability for Data Breaches
A growing number of public and private organizations are insisting that business leaders and corporate boards take greater control over cyber risk monitoring. The impact of network security complacency has become readily apparent to observers, with breach scandal after breach scandal demonstrating that data exposure brings considerable costs. Whether to comply with present or future government regulations, industry best practices, or maintain consumer trust, stakeholders are going to continue demanding that executives prove cybersecurity is being taken seriously.

Regulating C-Level Cybersecurity Compliance
Every US state and almost every populated territory has some form of data breach notification law on the books. Just as with other widespread regulations, such as sales tax and gun laws, the exact requirements can vary from state to state but all create the basic obligation for protecting personal consumer information (AKA personal identifiable information or PII). Of course, the discrepancies between jurisdictions and lack of united federal oversight has allowed some companies to attempt to challenge the interpretation of their liability when it comes to breaches originating with third parties.

As can be seen in other cases, however, this has only been allowed to fly when businesses such as Monster explicitly state the data will be in someone else's hands. This is a loophole that regulations such as GDPR do not allow, and also does not protect against consumer backlash or the actual consequences of these breaches. If and when federal agencies begin implementing universal data breach disclosure laws, executive leadership will likely be directly tasked with demonstrating security compliance.

Enforce Cybersecurity from the Bottom Up
Cybersecurity compliance and even just general network protection requires strengthening your human element. Educating yourself as well as your employees on what types of regulations and threats to expect goes a long way towards ensuring you avoid the consequences from either.

Download SWK's white paper on global IT security compliance to learn what regulations to watch for, and how to prepare to face them.

Hackers Continuing to Target SAP, Oracle, Other ERP Users

64 percent of SAP and Oracle ERP users have been hacked the past two years, according to an IDC report. A survey of hundreds of IT decision makers, about half of whom used either SAP or Oracle software, revealed this and several other developing trends pertaining to enterprise application security. Despite regular security audits and patches, most of those surveyed (62 percent) felt that their systems still contained serious cybersecurity gaps.

SAP and Oracle ERP Vulnerabilities
This is not the first time that SAP and Oracle applications have been found to have critical security vulnerabilities. The study's sponsor, Onapsis, has repeatedly highlighted major exploits existing in the majority of SAP products, including the 10KBLAZE bug alert earlier this year. Previous warnings were even echoed by national security agencies, with the Department of Homeland Security's cybersecurity division alerting users of Dark Web chatter building around recently found ERP exploits.

Transactional, Personal Data Most Sought by Hackers
The survey's subjects that had been hacked most often had several different types of data compromised per breach. However, the majority of information that was sought by attackers came from sales, employee or customer files, with engineering specifications, intellectual property and accounting data following close behind. Being that ERP acts as a library for all of this data, it appears that hackers are specifically targeting enterprise software to collect any and all potentially valuable files they can find before vanishing to avoid detection.

Cost of an ERP Data Breach
Any data breach can have a high cost, from both short-term and long-term damage, but hacked ERP applications can especially sensitive to lingering expenses. According to Onapsis, much of the data included in enterprise software (and which is subsequently being stolen) is some of the most regulated information today. This means that businesses can face even more losses from an ERP breach if they are found liable for data security damages.

Continued on page 4...

Shiny gadget of the month: Switchbot Curtain

The concept of a smart home is constantly expanding. There are more and more devices being created to make our everyday lives just a little bit easier and automated, who knows in a few years we may not ever have to get up to do anything anymore. The SwitchBot Curtain is just one step closer to that reality. This nifty little gadget can make any set of curtains smart in a few seconds. If there is one thing that can be a pain to work with it is curtains. A lot of homes have them in some difficult to reach places, or maybe you're just comfortable on the couch and the sun suddenly comes shining in, who wants to get up and close them…

The little robot has been designed to retrofit most curtains on the market. So that means no big expensive devices or special curtain rods are needed. The SwitchBot Curtain also is versatile so there is just one unit that can be modified to fit different style curtains, not different units based on the style. It runs on battery and has an option for a solar panel you can attach so you never have to worry about charging it. It has a variety of features, like a light sensor that you can program to react to the light for opening or closing curtains. You can program it on a cycle to open during the day, close at night, wake you in the morning, or even just open and close throughout the day to thwart burglars giving the appearance someone is home.

You can control the SwitchBot Curtain with an app on your phone, smart home voice assistants like Alexa, Google Assistant, or Siri Shortcuts. It even has physical remote controls if that is your preference. Right now you can find this cool gadget on kickstarter. At the time of writing it has $344,440 of funding and a goal of $20,000 so I think it is safe to say it has surpassed it. Right now the estimated ship date is April 2020 and you can still be an early bird backer for $69 and get one of the devices when it launches.

This is a really neat concept that could be useful to a lot of people. All those backers certainly agree too. What do you think?

66 Percent of SMBs Hacked in Past 12 Months

A survey conducted by the Ponemon Institute found that up to 66 percent of SMBs worldwide had been hacked in the past year. Small and mid-sized businesses in the US fared the worst, with 76 percent of American SMBs saying they had been hacked in 2018 to 2019. 63 percent also experienced some type of data breach during this time.

What Types of Attacks Most Affect SMBs?
Phishing and social engineering were the most common hacking vectors found in the study. These were followed closely by web-based attacks, with basic and advanced malware, credential theft, zero-day exploits, denial of service, SQL injections and more at frequencies varying from 40 to 20 percent for each. Some respondents had experienced more than a single type of cyber attack in the past 12 months, so the percentage of victims were neck-and-neck or equal for several categories.

The biggest takeaway the researchers found was that deception-based attacks continuously gained in popularity. This was only reinforced by the similar rates between different types, with advanced malware infections seeing the same exact frequency as credential abuse, and by the lower recurrences of easier to discover breaches such as script injections and insider threats.

Third Parties, IoT Contribute to Attack Surface
Laptops have risen to become the most vulnerable enterprise software endpoints next to mobile devices and followed closely by Internet of Things (IoT) networks, according to the report. Many of these machines are interconnected through the same systems, and when deployed through unsecured cloud servers, these items spread out your attack surface by adding many more endpoints that can be exploited.

The greatest danger to your ERP system, however, often lies in how these devices connect to third party networks. Most SMBs do not actively track the data and access they share with vendors and partners, which can lead to severe repercussions if this information is compromised.

Cost of Cyber Attacks Rises for Small Business
Though the average cost of a network breach unquestionably rose year-over-year, the study uncovered an interesting – and worrying – trend. While the cost of a security compromise in 2019 actually fell halfway between 2018 and 2017 levels, losses from business disruption rose exponentially from previous rates. Operational interruption from being hacked now often costs companies almost twice as much as the actual data breach itself.

Several factors contribute to this phenomenon, with industries like manufacturing suffering from any stalls in production or quality assurance. However, data security liability often represents the greatest risk factor for SMBs when it comes to cybersecurity costs. Not only can your business be penalized for noncompliance, but enterprises are increasingly demanding stricter security controls for supply chain partners.

SMBs Still Lack Resources to Deal with Cyber Threats
The reason behind all of these trends is simple – respondents said they lacked either the tools, skillsets, money or manpower to respond to every threat, and often faced a combination of all four factors. However, insufficient personnel was cited as the largest by far, followed by budget, technology and expertise. While SMBs were able to make some gains in these other categories between 2018 and 2019, the lack of dedicated IT staff only became worse over time.

How Confident Are You in Your Network Security Tools?
The Ponemon research confirms that SMBs cannot rely on static cybersecurity controls to protect their networks. Hackers rely on smaller businesses not being able to cover the gaps basic firewalls and anti-virus tools leave to get into your system at their leisure. However, working with an MSP like SWK can help bridge those gaps and provide you with a cybersecurity resource that is far more affordable than trying to staff internally.

Download SWK's free report to learn the top 10 ways hackers get past your anti-virus and how you can protect against them.

Gift Card Trivia!

This month's question is:

In addition to protecting your network and data what else can cybersecurity help your company with? (Hint: The answer is in this newsletter.)

a. Employee Retention
b. Competitive Advantage
c. Sales
d. Wages

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **Dec 2nd**, in order to be placed in the running for this month's gift card prize!

We can help you with:

- Complete network management and support
- Troubleshooting and problem solving on all PCs and Macs
- Cloud services and virtualization
- Hardware installation and support
- Virus / spyware removal and protection
- Security solutions
- Employee awareness training
- VPN (Virtual Private Networks)
- Remote access / Mobile computing
- Server installations and upgrades
- Spam filtering
- Hosted email
- Web content filtering
- System backups, on-site and off-site
- Help desk

Contact us

Give us a call for more information about our services and products.

SWK Technologies, Inc.

South Jersey
650 Grove Road, Suite 106
West Deptford, NJ 08066

North Jersey
120 Eagle Rock Ave., Suite 330
East Hanover, NJ 07936

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at www.swknetworkservices.com

SWK NETWORK SERVICES

Prevent Your Laptop from Overheating

An overheating laptop is not an uncommon thing, but it can lead to decreased laptop efficiency and a shorter lifespan if you're not careful. Here are a few ways to protect your laptop from damage due to overheating:

Potential Causes of Laptop Overheating
Obviously, laptops generate heat when in use - that's why they have internal fans that blow out hot air, as well as suck in cooler air to dissipate the excess heat. So, if you notice your laptop starting to persistently shut down or slow down at random times, chances are it's overheating.

Some of the causes of overheating are:

- Damaged or malfunctioning fans due to dirt and grime clogging the interior, preventing the blades from rotating properly.
- Blocked air vents preventing air from flowing into the laptop.
- Old laptop batteries rely on lithium, a chemical that naturally decays over time; as the battery gets older, it becomes less efficient and generates more heat.
- Running too many software programs in the background can cause your processor and fans to go on overdrive.
- Bad habits when using your laptop, such as using uneven or soft surfaces as padding, can block the air vents.

What to Do if Your Laptop's Overheating
If your laptop starts overheating, the first thing you should do is turn your laptop off and check if the fan is damaged in any way. Next, inspect the vents and fan for any dirt, grime, or other possible causes of blockage.

Also, check how many software programs or apps run on startup whenever your switch your laptop on. If your laptop is overheating or shutting down after a while, you may have to disable some of these applications during startups.

Keeping It Cool
Always make sure that there's adequate airflow when you're using your laptop. Avoid using it in bed or on a carpet. And never use pillows as padding as they can block the air vents Better yet, invest in a cooling pad - they lift your laptop and have built-in fans that facilitate better airflow.

Other ways to avoid overheating are limiting the number of programs that run when you start your laptop, changing your settings to power save mode, and shutting down your laptop when you're not using it.

Contact SWK Technologies for Laptop and Other Device Support
Users often take their laptops for granted because they're built as plug-and-play devices. However, with a little extra care and attention, your laptops can last longer.

If you want to prolong the lifespan of your hardware, contact SWK's support services today.

Hackers Continuing to Target SAP, Oracle, Other ERP Users

Continued from page 2…

User Credentials and Privileges
Most data breaches begin with privileged credential abuse, and this is extra true for ERP exploits. Relatively small but critical misconfigurations like 10KBLAZE in SAP NetWeaver allow hackers to mirror or bypass administrator access and gain the "keys to the kingdom" through your enterprise applications. Even amateurs can run rampant with this level of control before being discovered, but experienced cyber attackers will be able to leverage access privileges to erase enough user history to ensure their actions go unnoticed.

Cloud Security Concerns for ERP Applications
Besides these revelations, one of the biggest takeaways from the report is the concern of many IT managers of moving to the cloud, with 77 percent saying their C-suite had security worries. The other findings only reinforce this apprehension, as SAP, Oracle and other traditional ERP systems have been reconfigured for SaaS functionality, but often without adequate security measures for legacy software that was never designed to be connected to the Internet.

Business and IT objectives do not always align, and software hosting in the cloud has become the nexus of many competing decisions from application developers, cloud service providers and network security resources. This does not negate the benefits of application hosting delivered as a service, but doing so requires knowledge, preparation and experience to secure your enterprise software infrastructure.

Protect Your Software in the Cloud with Secure Hosting
Moving your ERP to a digital infrastructure means investing in cloud security - the best way to protect a modern network is by reinforcing the human element to ensure no endpoint goes unmonitored. Your enterprise applications are too important to let your data protection controls slack, and suffering a data breach here can put your business in serious danger.

Download our on-demand webinar to learn how to migrate to a secure cloud solution for FREE with SWK's cyber-secure hosting service.