IT Strategy Brief

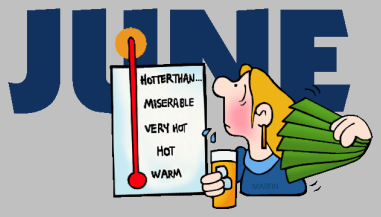
ISSUE 6 | VOL 6 | June 2020

INTEGRATE SEAMLESSLY

SWK NETWORK SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:



The Affordable IT Support Model for Small Business

Traditional IT support models are not cost-effective for what your small business needs in modern times, which means you required a much more evolved network security and helpdesk service. Coronavirus, digital transformation and many more developments have changed the way you do business, but the value of your web assets if offset by sheer market cost of protecting them. The most affordable way to ensure your networked resources are cybersecure is to co-manage your IT with an outsourced managed service like SWK.

Cost-Effective IT Support for Growing Businesses
As your business grows, so too will your IT needs - the more your workforce grows, the more network assets you will need to deploy. With more network assets comes the need for more IT staff or technology to automate related processes - and this still will not eliminate the ultimate need for more staff. Growth ensures your business survives, but technology ensures that your business grows and continues to deliver ROI.

Gone are the days of scraping by with informal IT roles and one-man IT departments. Network assets are everywhere in the modern office (and even more so when working from home), and protection needs to be scaled with your business size - unless you have a partner with the resources to scale your maintenance for you.

Guaranteed Network Security Coverage
No matter how big or small your business is, your network requires some level of security - everyone is a hacker target these days. As expensive as some cybersecurity solutions may seem, the alternative will cost you much more in ransomware payments, wire fraud, noncompliance penalties or system downtime, just to name a few consequences. Investing in your network assets must also include investing in cyber defense to protect their value. There are so many IT items to address that it is easy to let some fall through the cracks for the sake of compartmentalization and prioritization, but every endpoint carries a data breach risk. Hardware and software are made of countless complex components, and hackers exploit the overlooked areas to piggyback on unsecured connections. Small and medium-sized businesses find it hard to commit the resources to address every gap, but co-managing with an outsourced IT partner will help you expand your network security coverage.

Around the Clock IT Helpdesk Resources
It can be tempting to simply try to get more out of your existing IT resources by stretching work hours or the use of your technology applications. However, this not a viable long-term solution and can actually end up causing harm to your network assets once the system breaks down. When you are already overextended is when your cybersecurity vulnerabilities will really impact your business, especially if an enterprising hacker figures out how to infect your database with ransomware.

SWK's helpdesk service and endpoint security program can give around the clock access to support solutions when you co-manage your IT with us. By taking advantage of the resources we have to offer, you can ensure that your in-house IT never becomes overwhelmed trying to solve every problem every minute of the day.

Co-Manage Your IT with SWK Network Services Support
Don't an understaff IT department slow your business growth, or worse, put your network at risk of an expensive breach. Learn how you can both protect your valuable and save costs when you co-manage your IT resources with SWK Technologies.

Download the CEO's Guide to Co-managed IT to learn more.

What our clients are saying: HelloFresh

"SWK's fast and friendly support has been invaluable for our team. I had a data transfer to a new machine on a different operating system which was performed remotely and on my lunch break. When I got back from lunch, my new Mac was totally set up. I've also noticed serious IT efficiencies since we partnered with SWK. Prior to our partnership, there was a serious backlog for all IT related requests. Since SWK has stepped in it is no longer a mess."

Jordan Schultz
Senior Associate/Team Lead, Marketing
HelloFresh

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner!

Last Month's Contest Winner:

Mylene Lawton
Meeker Sharkey & Hurley

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 **July 1st** to get your name in the hat.

You could win a $25 Gift Card!

68 Percent of Businesses to Increase Cybersecurity Spending

An HFS Research study reveals that a majority of businesses plan to increase cybersecurity spending by the end of the year, with 68% of respondents saying it was a possibility. Most of the rest indicated the percentage of spend would remain the same, with just 4% saying they would be spending less. Previous forecasts put future valued expected investments to total $42 billion by 2020, meaning that these new planned increases could significantly surpass that amount by 2021.

Cybersecurity Surges Past All Other Investment Priorities
The study questioned subjects on topics of technology investment from blockchain to IoT and 5G. Perhaps unsurprisingly, plans to invest in technologies that still emerging (augmented reality, edge computing, etc.) were more lukewarm. Most respondents would keep their spending the same in these areas, with the only sizable decreases in AI and automation (also the second highest increase priority) at 23% and 22%, respectively. The biggest unifier was cybersecurity, with plans to increase investments here far surpassing any other plans to decrease or keep spending the same.

Remote Work Creates the Need for More Security Spending
While those new and still being proven technologies like AI saw drops in planned expenditures, cybersecurity beat all other categories solely due to its even greater importance after COVID-19. Many companies have indicated the new normal will become their status quo even after the pandemic allows extended social interaction again, and that means new cybersecurity vulnerabilities to address. Hackers will target remote workers on networks that are not properly secured, so better security policies and platforms will be needed to ensure safe digital telecommuting into the future.

What Does This Mean for SMB Spending?
While the HFS Research study respondents were more likely to have the capital on hand to quickly make these investments, digital transformation is bringing businesses of all sizes into the new normal. Most businesses rely on some kind of network access and IT infrastructure to allow it, and COVID-19 revealed just valuable this technology is for business continuity. However, SMBs will be at a disadvantage without the money required to invest in expensive high-end cybersecurity systems.

Get a Helping Hand for Your Cybersecurity
Your business relies on your IT assets more than ever, whether you know it or not, and you cannot afford to lag behind in implementing security for your network. Let SWK help guide towards more cybersecure practices and policies with our award -winning support.

Request a consultation and get comprehensive visibility into your network as well as personalized recommendations for how you can improve your cybersecurity posture.

52 Percent of Remote Workers Admit Cybersecurity Weakness

A recent study revealed that many remote workers are following weak or no cybersecurity practices while telecommuting. In the State of Data Loss Report by UK firm Tessian, 52% of employees surveyed admitted to ignoring security policies and exposing their companies to cyber risk due to the lack of organizational oversight from their IT department. The report also covered many of the respondents' reasoning for the protocol breaches, which included frequent at home distractions and deadlines that required them to take shortcuts around security steps.

Data Breach Prevention for Remote Workers
The study surveyed over 2200 professionals (about 11% of which were IT leaders) in the US and UK and charted the data management practices of each group. Almost 85% of the IT respondents claimed that preventing data loss was more difficult with remote workers as they lacked the visibility to routinely monitor compliance. Worse, almost half (45%) of US workers surveyed admitted to using personal email accounts for business data, pushing it further outside of internal IT's oversight.

Productivity and Speed VS Cybersecurity
Using personal email accounts and devices is just one area where remote workers can inadvertently expose your network to external channels if they are not careful. Ignoring proper safety procedures when remote accessing shared computers or cloud databases, leaving unsecure apps running in the background and reusing passwords across company accounts all increase cyber risk.

All the current disruptions have left many businesses overwhelmed, but unfortunately that doesn't mean you can afford to take a break from cybersecurity. Your hard work will be for nothing if a data breach exposes you to wire fraud, ransomware or noncompliance with data privacy laws. You shouldn't have to sacrifice your network security for productivity - learn how to balance both with cyber threat protection.

Don't Leave Cybersecurity to Chance When Working from Home
Security practices can be stressful in the best of times, and even more so for remote workers unused to telecommuting on top of managing the distractions from loved ones and pets. SWK can help you protect your network with cybersecure best practices and solutions for everyone in your company working from home.

Contact SWK Technologies ASAP to discover how we can protect your data while your business works remotely.

Shiny gadget of the month: NexFan Ultra: Portable AC with Powerful Cooling

Summer is here and the fight to stay cool is back. Now that now many people are working remotely the cost of air conditioning is sure to go up for many this summer, especially if you would have normally set your temperature higher while you were at the office. Perhaps you just want something to help you cool off by your desk and the fan just isn't cutting it. If you can relate to any of this maybe the NexFan Ultra is the gadget for you.

The NexFan Ultra Air Cooler is a neat little multi-use gadget. First and foremost, it works like a mini AC unit. However, it also functions as an air purifier, humidifier, and aromatherapy machine. Best of all is that you can go completely portable with it by running it off of a power bank. This brings in all sorts of new options for you. You could take it outside to a picnic or an event, sit it on your desk, set it by your bed, even bring it back to the office with you when you return. The ability to bring a mini AC unit around with you is pretty cool.

The way this little gadget works is by taking water you pour into the reservoir on top and using the water to cool the air that it blows out through a filter. You can also add ice to give it an even more dramatic effect. Operation is as simple as add water, plug in and hit the on button. Even though you have to use water they have a leak-proof design to ease your worries about dripping or spillage. If you want to go portable a 10,000 mAh power bank can get you 12 hours of life! So just fill it up, turn it on, and within seconds you will feel the difference.

It is a really neat concept packing the comfort of air conditioning into the compact design of a mini portable unit. The NexFan Ultra would be perfect for someone who needs a little relief at their desk but doesn't want to crank the AC for the whole house to cool down a single room, and doesn't want the hassle or obstructed view of a window unit (or may not even have a window in proximity of their workspace at home). The NexFan Ultra could be the perfect solution.

Right now at the time of writing the NexFan Ultra is in the shipping phase of their indiegogo campaign. While it seems like something that might be a bit pricey you can actually still get one for $45 which seems like a bargain considering most floor fans cost just as much if not more. You can see more about it or order one for yourself at https://www.indiegogo.com/projects/nexfan-ultra-portable-ac-with-powerful-cooling#/. What do you think of this idea? Apparently over 14 thousand people liked it enough to back it at the time of writing. It certainly seems like it could be a handy little device.

Remote Work and Telecommuting Are Changing Cybersecurity

All of your telecommuting coworkers and employees (and you too) are changing the face of cybersecurity. You have probably already heard several warnings before (if you haven't, SWK has plenty of resources to read), but now real-world data is beginning to back the predictions up. Multiple studies reveal that many employees are in fact not following security best practices working from home, and some may have already faced consequences.

Here are a few of the ways the remote work expansion is changing the cybersecurity landscape:

The Same and New Cyber Scams, Telecommuting Edition
It is no surprise that hackers are relying the same tools and techniques they usually do - phishing for credential theft and malware delivery. The end result is also always to separate a victim from their money, either from exploiting privileged access directly or tricking those that have it, or from ransoming access to locked data back. Only two factors have changed - the volume and the messaging.

Spoofed emails and domains have increased exponentially (as high as 600% in some areas), and at least one UN official claims a cyber attack happens "every 39 seconds" currently. Information has become even more valuable in these uncertain times, and with many people seeking it solely relying on digital communication, hackers have many more potential victims than usual. With less layers of authentication while in isolation, bad actors know it is easier to leverage trusted institutions and brands to exploit those who are desperate for updates.

46 Percent of Businesses Experienced a Cybersecurity Scare
A study conducted by Barracuda Networks had almost half of respondents (46%) claim they had been affected by at least one cybersecurity incident during the COVID-19 stay at home orders. 51% said they had recorded an increase in phishing email attacks during this time as well. One of the most revealing findings was that half of respondents (notice a pattern?) also said that employees were allowed to use their own personal devices and email addresses while working from home.

Cyber Risk Management for the Remote Worker
All cybersecurity stances should be built around a quantification of your business's cyber risk - that includes the risk generated by every employee, from entry level to executive. As more people work from home, that raises the possibility that someone may expose your network through bad habits and unsecured access. To calculate your risk, there are a few questions you need to ask yourself, like:

- **How many people do we have logging in from home?**
- **Is everyone connecting to cloud databases or remote accessing company computers?**
- **How many layers of credential security do users have to go through for sensitive data?**
- **How fast would be able to catch an intruder in our network?**

There is No Silver Bullet for Telecommuting Cybersecurity
Even if you are able to fully quantify your company's cyber risk from endpoint to endpoint, there is no sure-fire way to cybersecure every one of your remote workers all the time. There is no zero-trust cybersecurity policy that completely shuts out human error (especially considering executives are commonly the biggest targets - and perpetrators - of security gaps), but with the right resources you can cover the most bases as best you can. Only a proactive and reactive mix of security education, network monitoring and data protection (including backups) will shrink the attack surface remote workers can bring.

Let SWK Help You Cybersecure Your IT
Don't let the new normal of working from home expose you to unnecessary cyber risk. Discover how SWK Technologies can help you to adapt your cybersecurity policies for remote workers with our real-time support services.

Download our CEO's Guide to Co-managed IT to learn how SWK can help you cybersecure your network for telecommuting.

Gift Card Trivia!

This month's question is:

What percent of US workers surveyed admitted to using a personal email account for work purposes? (Hint: The answer is in this newsletter.)

a. 25%
b. 34%
c. 45%
d. 60%

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **July 1st,** 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 NETWORK SERVICES

5 Tips for IoT Device Security

Internet of Things (IoT) devices are tools that utilize remote connections and sensors to automate functions, and are increasingly becoming a ubiquitous part of modern offices. However, when not managed properly, IoT machines - for both private and industrial (IIoT) usage - can create gaps in your cybersecurity that cybercriminals can exploit. Make sure that these devices don't become entry points for hackers into your network with the following tips:

Set Strong Passwords for All IoT Devices
Many users fail to realize that they can set passwords for IoT devices. Failing to do so makes these gadgets easier to hack. You have to make sure to create strong passwords for each device — preferably with a combination of upper- and lowercase letters, numbers, and symbols — and also put a smart and proactive password policy in place. Make use of all security options at your disposal, such as multi-factor authentication (MFA) for added layers of cybersecurity and regular password resets.

Disable Universal Plug and Play and Monitor Connections
Universal Plug and Play (UPnP) helps IoT gadgets discover and connect with other network devices. However, this feature can also be exploited as a gateway for hackers to infiltrate your devices and network. To prevent this, disable this feature on all connected devices immediately, and continue to monitor any active on your network to ensure nothing provides a bridge for outside connections.

Create a Separate IoT Network
It's a good idea to keep your IoT devices connected to a network separate from your main office network. This way, gadgets can connect to the internet, but won't have access to mission-critical files and shared cloud servers. Hackers routinely exploit overextended networks where device volume can create several unnoticed backdoors.

You can also invest in device access management tools. These allow you to control which devices can access what data, and prevent unauthorized access from outside - or inside - the network.

Update Your Firmware for All Devices
You need to keep your software up to date if you want to secure your devices against cyberattacks. Legacy applications run the risk of being undefended against newer hacking techniques and existing bugs that can grant access outside the network. Manufacturers regularly release patches for the latest of these vulnerabilities, so make it a habit to check and install IoT firmware updates regularly.
If you have several devices, use patch management software to automate patch distribution and schedule regular updates.

Unplug IoT Devices After Use
Simply disconnecting your IoT devices or turning them off when not in use can significantly reduce your vulnerability to cyberattacks. It removes potential entry points into your network and minimizes the chances of unauthorized access to your network.

Contact SWK to Enhance Your IoT Security
With the advent of IoT devices in homes and offices, hackers also developed more cunning ways to exploit them. Adopting the abovementioned security habits can prevent a variety of cyber attacks through IoT backdoors, but don't be afraid to seek additional support to help keep an eye on your devices without overwhelming your staff.

Contact SWK Technologies to learn how we can help you cybersecure your IoT devices and networks around the clock and without disrupting your business.