IT Strategy Brief

ISSUE 10 | VOL 6 | October 2020

INTEGRATE SEAMLESSLY

SWK MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

The Essential SMB Cybersecurity Training and Solutions Toolkit

Discover the best cybersecurity training tips and solutions your business needs with the Essential Cyber Toolkit by SWK Technologies and Datto. This eBook is designed to help small and mid-sized businesses understand the cyber threats specifically targeting SMBs, and how to protect against them by enforcing security practice at the user level. Through the right combination of education, vigilance, technology and IT support, this Toolkit will help you chart your path to a cybersecure network and business.

Here are the key takeaways this eBook will impart that will help you provide the best cybersecurity training and solutions for your business:

EMPLOYEES NEED CYBERSECURITY TRAINING TO PROTECT YOUR BUSINESS

Any organization's employees are the first and last line of defense against persistent hackers and cybercrime. Modern networks are user-driven, near-instant data streams that feature many endpoints to facilitate faster communication between machines. Unfortunately, these nodes can also enable discreet cybercriminals to exploit unsecure login credentials if the right steps are not taken to protect individual users and business data.

There are a variety of cyber threats out there, as well as methods to identify and defend against them. Here are a few of the key factors the Essential Cyber Toolkit will help you understand better:

HACKERS USE SOCIAL ENGINEERING ON NETWORK USERS

Social engineering was a facet of crime before the creation of the Internet that was a favorite of con artists, but modern connectivity gives every criminal the chance to pull off their own scheme. The world wide web is an open marketplace of data, including information that could be used to identify and exploit potential victims. Once a hacker has the chance to stalk an employee, they can find ways to leverage their credentials to gain greater access to critical business data or to company funds directly.

Social engineering techniques covered in the Cyber Toolkit:

- ***Phishing***
- ***Baiting***
- ***Quid Pro Quo***
- ***Pretexting***
- ***Tailgating***

CYBER THREATS THAT CAN BRING DOWN YOUR BUSINESS

There are many types of cyber threats as well as methods used to deploy them, though most hackers of various skill levels will stick to the same core categories for easiest returns. Although many diverge on the specific details, there are a few main stages where cybercriminals hit their victims to get what they seek. The most common is infecting a network via user with a malware program, though other techniques also involve using weak remote coding or the user's login credentials as backdoors.

Continued on page 2...

What our clients are saying: Meeker Sharkey & Hurley

"I've been happy with SWK's service and they have always been able to resolve my issues. I like that requesting a service ticket is a seamless process and SWK is very quick to respond. I recently had a problem with Nitro Pro not allowing me to view PDF's to import docs into ImagaeRight. I had to use a time-consuming end around to fool it into working. SWK 's tech logged into my desktop and had Nitro working after a bit of diagnostics which made my day. No more fighting with Nitro!"

Mylene Lawton
Meeker Sharkey & Hurley

MEEKER SHARKEY & HURLEY
Insurance and Employee Benefits

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Anthony D'Agostino
Pee Jay's Fresh Fruit

Please complete our brief survey in order to be placed in the running to win this month's gift card prize!

1. What do you like most about our services?

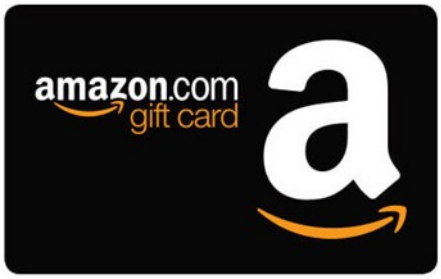
2. Tell us about a specific experience with us that you were happy with.

3. What are the biggest benefits you've received or experienced since hiring us?

4. What can we improve?

Email Jon Stiles (jonathan.stiles@swktech.com) with your responses
OR
Fill out our online form: http://bit.ly/nwsnews-survey before **Nov 6th** to get your name in the hat.

You could win a $25 Gift Card!



The Essential SMB Cybersecurity Training and Solutions Toolkit

Continued from page 1…

Cyber threats included in the Essential Cyber Toolkit:

Spoofing
A phishing email that masquerades the sender as a trusted source to entice the victim to let their guard down. A wide of range of effort has been observed in these types of messages with sophisticated examples appearing virtually indistinguishable from a legitimate branded email. However, even more obvious attempts have proven effective through creating enough urgency to click and optimizing send time for high stress periods.

Phishing Domains
While most hackers rely on spoofed emails with malware attachments to phish victims, some also lay fake domains as traps for downloading malicious code. These can exist as links in messages as well as online adverts and pop-forms.

Ransomware
Ransomware has become a king of malware as it represents an efficient method of ensuring a hacker is paid for their efforts and relies on many of the same tricks as other phishing campaigns.

LEARN HOW TO SPOT THE RED FLAGS
Many might believe they know the red flags of a malicious email, but most are not trained well enough to immediately spot the signs as second nature, especially during periods of duress or laxity. Confirming a cyber threat often requires extra work that the user may not be able – or willing – to complete in that moment, and distractions can divert focus from the hidden danger. Only education – and repetition – can arm your employees with the mindset for sniffing out phishing right away.
A few of the red flags covered in the Cyber Toolkit:

Email URLs
You may think it is easy to spot a typo in an email address, but hackers have gotten better enough at dressing up their spoofing that the incorrect URL will often be the only mistake. This is a critical red flag that can be easy to overlook due to habit, and cybercriminals know this.

Redirecting Domains
This requires more effort on the user's part to confirm, which makes it easy to fall for. Only by carefully hovering your cursor on a clickable link will you be able to identify if the URL is questionable, and many will seem legitimate enough to not ask for confirmation.

Personal Information Request
There are plenty of instances where users are required to submit personal information for it to become a habit, and this is another behavior hackers will exploit. Anyone whose login can be used to bypass permissions can become a target for this.

CRITICAL CYBERSECURITY SOLUTIONS TO HAVE
While cybersecurity training should be at the forefront of your defense strategy, there are several tools that can help shore up weaknesses and automate background security. The Essential Cyber Toolkit outlines many of the critical solutions even a basic plan should be putting in place and why they are necessary to protecting your business. However, it is important to keep in mind that these tools still require you to practice good cyber hygiene to remain cybersecure all around.

TAKE A LAYERED SECURITY APPROACH
Having multiple layers of security ensures that your cyber defense will not hinge solely on each and every individual user's cybersecurity practices every waking moment. This approach takes factors like human error and strokes of luck into account to prevent a single mistake or hacker breakthrough from exposing your data completely. Using this method also helps limit potentially vulnerable network endpoints, shrinking your attack surface at least somewhat.
Layered security tools featured in the Cyber Toolkit:

- ***Antivirus***
- ***Network Firewall***
- ***Patch Management & Regular Updates***

Password Security
IMPLEMENT AND DEPLOY A BUSINESS CONTINUITY PLAN
Having a business continuity plan (BCP) in place is vital for your company's ongoing cybersecurity stance, and the new normal has only reinforced the importance of planning for disruption. The most basic – and critical – requirement of any plan is ensuring the security of data, and the most effective method is a backup. Supplementing this with additional solutions help you transform your BCP into a true BCDR (business continuity and disaster recovery) strategy that helps you prepare for almost any cyber incident.

Business continuity topics covered in the Essential Cyber Toolkit:

- ***Data Backups***

Backing up your data should be one of the top priorities of your cybersecurity planning along with training. In the event that your system goes down or is compromised by an attacker, you must be able to retrieve your business information – especially anything involving your customers' personal data. This latter point is often an essential industry and state regulatory requirement, and could be well on the way to being a federal obligation.

- ***Image-based & Cloud***

Advances in backup technology have made many options available beyond the traditional tape-based systems that are vulnerable to many of the same dangers that an onsite server would be. These include image- and cloud-based backups that help facilitate near-instant uptime after an incident compromises your data.

COMPARE YOUR EFFORTS AGAINST THE CYBERSECURITY CHECKLIST
The ebook contains a quick checklist of essential items to be incorporated into your cybersecurity planning, including many of the topics previously discussed. This concise but comprehensive list will help you keep track of the many actions your business must follow up on to avoid vulnerabilities slipping past your business continuity planning.
Cyber Toolkit Checklist:

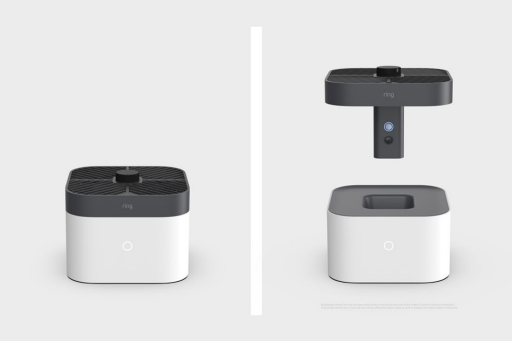
- ***Risk Assessment***
- ***Training Program***
- ***Network Security***
- ***Software Updates***
- ***Clear Cybersecurity Policy***
- ***Backups***
- ***Recovery Plan***
- ***IT Visibility***
- ***Access Permissions & Controls***

Download the ebook below to learn more about which steps your business needs to take to fulfill each point for this cybersecurity checklist.

DOWNLOAD THE ESSENTIAL CYBER TOOLKIT AND IMPROVE YOUR SECURITY
The new normal and digital transformation have further brought the world into wide-ranging and consistent connectivity between every computing device. Leveraging the lessons from this ebook and support from SWK's Managed Cloud Services will help empower you to meet the slew of cyber threats that can impact your business at any time.

Download the Essential Cyber Toolkit and learn more about what you need to do to make your business cybersecure.

Shiny gadget of the month: Ring: Always Home Cam



When it comes to home security, technology has made leaps and bounds over the past several years. A market that used to be comprised of complex and expensive systems has seen more affordable and simple solutions come into play. Ring for example has a wide array of home security devices available that will do a good job of covering your home security and surveillance. However, they have a new gadget coming out that is like something about of science fiction. A drone security camera…

The new Always Home Cam is quite literally a camera that will fly around your home so that no stone gets left unturned. Forget stationary mounted cameras that just give you a single view, this drone cam will seek out disturbances trigged by alarms or go on a patrol for you. The Always Home Cam is autonomous so there is no need to pilot it around (in fact they don't allow you to manually control it), and when it is done its patrol it will dock back in the station to change for the next flight.

The way is works is you set a designated path that you map out manually with the drone, then after that is done it can chart the course on its own. It also is supposed to come with obstacle avoidance technology and the propellers are protected so it should avoid any possible damage inside your home, or an unsuspecting person or pet.

While people may be split on whether this sounds really cool or really invasive to privacy it is certainly a unique idea. Ring is adding end to end encryption later this year for added data security, and when docked the camera is tucked inside the charger so it only records during flight. It was also said that it was designed to make noise from the propellers so that you are aware of the drone and when video is recording.

The concept for this came from finding an affordable solution for those who wanted to be able to have surveillance of their home but didn't want to pay for all the individual cameras it would take to get coverage. Since the drone can move about the home, only one would be needed. It also gives you the ability to check on things for peace of mind, like "did I leave a window open".

The Ring Always Home Cam is expected in 2021 for $249.99. You can find out more and see a little demo video here.

Creating a Cybersecurity Culture at Work

People are the first and last line of defense against hacking, so creating a solid cybersecurity culture among your employees is key to enabling secure remote work. Even after the pandemic, ensuring cybersecure distributed access will remain a big piece of endpoint protection and should be included within your business strategy into the future. Digital transformation has made networked IT infrastructures an increasingly integrated part of growth, and capturing your ROI on technology requires having the right cyber expertise at your disposal.

Here are three ways to help create a cybersecurity culture for your business, including to secure remote work:

BUILDING USER SECURITY AROUND THE SOC
A security operations center (SOC) is a fully staffed cyber defense and network monitoring unit that directly hunts for malicious activity within your system. Leveraging knowledge of hacker footprints and insider threat profiles, a smart SOC can help your business identify every cyber risk that falls through the cracks of your base level protections. It also enables you to supplement technology with real-time human intelligence that can spot attackers trying to exploit automated firewall solutions and permission-based controls.

Deploying this operative component gives you the ability to proactively plan for user security, with dedicated network observers working off of established patterns to highlight anomalies. This practice helps to emphasize bad habits as well, which can create vulnerabilities in your system. With insight delivered by a comprehensive SOC as a service solution, your business can start building your cybersecurity culture around addressing consistent employee weaknesses.

REINFORCE EMPLOYEE CYBERSECURITY CULTURE DURING REMOTE WORK
Speaking of bad security habits, studies found that quite a few have been amplified by the shift to the new normal for COVID-19, with half of remote workers sacrificing protection for productivity. Expanded workloads, home distractions and other pandemic stressors are contributing to this lack of focus and diminishing efforts of establishing a cybersecurity work culture. Even after coronavirus, a lot of business will be conducted through distributed endpoints with mobile devices and home networks, so reinforcing protections for telecommuters and remote access is a must.

The tiniest overlooked detail can create a vulnerability, which is likely why so many cyber attack victims can claim to have never expected being breached. The research shows there are an excess of employees who believe they will never be targets – and that reinforcing vigilance and discipline needs to be emphasized alongside education.

MAKING CYBER TRAINING PERSONAL WHILE WORKING FROM HOME
To combat the potentially dangerous mindset mentioned above, your business needs to implement cybersecurity training that is academically and emotionally accessible for your employees. That means that it must be able to communicate the details needed to fight hacking and cyber fraud without getting too technical, and be able to speak to personal scenarios. To ensure users are protecting the company's data effectively, their individual security needs to be mapped out as it ties into their daily role activities, as well as how a breach could impact them.

Cyber education, like most instruction, is only retained as well as it reflects the instructed's own world and how the subject matter affects their lives. Your cybersecurity training program consequently should not be a pedantic, standardized course, but a dynamic and proactive solution that keeps employees engaged and able to instantly spot red flags like muscle memory.

DEVELOP YOUR REMOTE SECURITY STRATEGY AROUND SWK'S SOC
The responsibility of internal user security conditioning falls upon your business, but you don't have to approach this gargantuan task alone. SWK can provide insight and instruction through our SOC service, as well as 24x7x365 monitoring to keep you protected around the clock.

Contact SWK Technologies to learn more about engaging SWK's SOC and how to leverage it to develop a cybersecurity culture for your company.

Gift Card Trivia!

This month's question is:

What are the three top reasons for why you should have a Business Continuity Plan? (Hint: The answer is in this newsletter.)

a. Cyber Attacks, Ransomware, Email
b. Natural Disasters, Man-made Disasters, Equipment and Utility Failures
c. Hurricane, Tornado, Storms
d. None of the Above

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **Nov 6th,** 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

3 Reasons Why Your SMB Needs A Business Continuity Plan

Implementing a solid business continuity plan (BCP) will help your company prepare for the worst and limit network downtime in the face of disruption. Multiple things can interfere with the operations of small- to medium-sized businesses (SMBs), including natural disasters and cyberattacks. Having a concrete BCP in place will help your business recover quickly after catastrophes whether they are man-made or not.

Here are three reasons why you need a business continuity plan and a few tips on building one:

WHAT IS A BUSINESS CONTINUITY PLAN (BCP)?
A BCP is a predefined set of protocols on how your business should respond in the event of an emergency or natural disaster. It should contain contingency plans for every aspect of your organization, including human resources, assets, and business processes. A good plan should also empower you to reasonably prepare for most eventualities, from hurricanes to a pandemic.
Modern business continuity procedures should revolve primarily (but not exclusively) around keeping communications and data access open. In other words, you should take every step to ensure your IT infrastructure keeps going, including (and especially) if your network goes down for whatever reason. Specific industry compliance requirements for sectors like financial services may also have added obligations depending on regulatory at a given time.

DATA BACKUPS AND DISASTER RECOVERY
The core component of any BCP is a data backup solution which ensures continuity and speedy disaster recovery (also known as BCDR) in the event of downtime. Once an incident hits, the speed at which your business recovers will almost be as important to resilience as preserving every byte of customer information. Both factors can make or break an organization, but regulations make you legally responsible for the latter.

THE 3 KEY THREATS BCPS HELP SOLVE
There are various types of threats that can cause downtime for SMBs. Ensure that your BCP addresses the likeliest of these within your market or region of operations at the least to maintain compliance, although you should deeply consider how each danger could affect different parts of your business. The best (and most cost-effective long-term) forms of business continuity have a provision in place for every statistical likelihood.

Here are the top 3 threats your BCP should solve:

Natural Disasters
These are natural phenomena such as storms, earthquakes, wildfires, and disease spread including pandemics and full-blown epidemics. These types of disasters are commonly widespread, and your BCP should be prioritized for the probabilities against damage to your data storage based on location and severity of the danger. It should also be noted that you should ensure your backups are well removed from primary servers – SWK has had at least one client who lost both in a fire due to human error.

Man-made Disasters
These include cyber attacks, intentional sabotage, and human negligence. Most of these are separated from more natural disasters by being targeted, and even those that are not still require an additional set of protections in place. The danger in other types of incidents is the widespread damage, but these kinds of threats carry a dual risk of discretion and internal access, meaning that your data will be compromised before you can even respond.

Equipment and Utility Failures
These include unexpected power failure, Internet downtime, and disruption of communication services. Being more random than cyber attacks and even natural disasters, system failures can be hard to plan for. Nevertheless, your business continuity strategy needs to keep these types of incidents in mind and prepare against the unexpected.

4 TIPS FOR BUILDING AN EFFECTIVE BCP
If your organization does not have a plan already in place, now is still a good time to put one together. The following steps will help you formulate an effective BCP that will ensure your company keeps running even during and past a major crisis.

- Business impact analysis (BIA)

A BIA will help you determine how a disruption can affect your company's current functions and processes, such as personnel, equipment, technology, and physical infrastructure. This step will help you calculate the potential financial and operational loss from each function and process affected.

- Recovery options

This step will help you identify key resources essential to returning your business to minimum operational levels. Some recovery options you can take include letting employees work from home or operating from a secondary location.

- Plan development

This step involves assembling your company's continuity team, which will be responsible for developing and implementing your business continuity planning.

- Testing and training

Once your BCP is in place, your continuity team needs to perform regular tests to identify gaps and make necessary changes to ensure the plan's effectiveness. They also need to conduct regular training for your employees so everyone knows their respective roles when a disaster strikes.

SWK CAN HELP YOU PLAN FOR BUSINESS CONTINUITY
Having a foolproof business continuity plan is a great way to ensure your business can quickly bounce back after a major disaster. If you are still having trouble figuring out where to start or have more questions, SWK can help you develop your BCP around your needs and discover which options work best for you.

Download our eBook here to learn more about business continuity planning and disaster recovery, and how SWK can help you bounce back from downtime.