IT Strategy Brief

ISSUE 1 | VOL 3 | January 2017

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

Cybersecurity threats to look out for in 2017

2016 is now a thing of the past. Last year we saw new cyber threats emerge and existing ones on the rise. Unfortunately 2016 does not appear to be a fluke and now 2017 is primed to face even more threats. Luckily that does not mean that all is lost, we can use the trends and knowledge from last year to help predict threats and be prepared for the coming year to protect ourselves and our businesses from hackers.

Looking at 2016 hacking became more of a mainstream and regular occurrence in the public eye. Between the ransomware attacks and talk about it throughout the election you could not avoid the topic even if you wanted to. 2017 is likely to be the year where hacking becomes more creative. Since more people are aware of threats it becomes more difficult for hackers to break in through traditional methods. New technology and connected devices open new doors, and this, along with some creativity could become a focus for exploiting new ways to gain entry into your computer systems. New ways that could put more people at risk...

Continued on page 3...

What our clients are saying: Procacci Development Company

"You guys are absolutely the best. I would recommend the services of your organization and staff to anyone who needed excellent IT Services."

Michele Mertz
Procacci Development Company

PDC
Procacci Development Company

Two ways to WIN a gift card!

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

Last Month's Contest Winner:

Carla Rudow
Camp Veritans

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

1. What do you like most about our services?

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

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

4. What can we improve?

Email Jon Stiles (jonathan.stiles@swktech.com) with your responses
OR
Fill out our online form: http://bit.ly/nwsnews-survey before **February 3rd** to get your name in the hat.

You could win a $25 Gift Card!

2017 IT essentials: disaster recovery plan

When disaster strikes, organizations need to put their business continuity plans into action and recover their IT systems as quickly as possible. Failing to do so can mean serious financial and reputational repercussions. Despite this, investments in disaster recovery are set aside each year for high-tech IT investments, and every year companies and employees continue to suffer for it. Here are some reasons why disaster recovery is well worth your time, effort, and resources in 2017.

DR isn't a huge investment
A common misconception about disaster recovery is that it's a large, bank-breaking investment. Expensive secondary data centers, networks, and server maintenance usually come into mind when a business owner is confronted with the idea of business continuity. And while that may have been true in the past, establishing a strong disaster recovery plan today is as simple — and as cheap — as going to a cloud-based disaster recovery provider and paying for the data and services that your business needs. Subscription pricing models are actually incredibly low, meaning you can have minimal downtime while still having enough to invest in new tech.

Business disasters can be man-made, too
Even if your workplace is nowhere near frequent disaster zones, cyber-attacks and negligent employees can leave the same impact on your business as any natural disaster can. Setting a weak password, clicking on a suspicious link, or connecting to unsecured channels is enough to shut down a 5-, 10-, or even 50-year-old business in mere minutes.

Sure, installing adequate network security is a critical strategy against malicious actors, but last year's barrage of data breaches suggests that having a Plan B is a must. A suitable disaster recovery plan ensures that your data's integrity is intact and your business can keep going, no matter the malware, worm, or denial-of-service attack.

Downtime will cost you
A business without a DR plan might come out unscathed after a brief power outage, but why risk the potential damages? Either way, downtime will cost your business. First, there's the general loss of productivity. Every time your employees aren't connected to the network, money goes down the drain. Then there's the cost of corrupted company data, damaged hardware, and the inevitable customer backlash. Add all those variables together, and you end up with a business-crippling fee.

So, if you want 2017 to be the best year for your business, make the smart choice and proactively take part in creating your company's business continuity plan. Your business will be in a better position financially with it than without it.
Keep your business safe, recover from any disaster, and contact us today.

Office 365 reveals new security features

Office 365 has given business owners access to online organizational programs and collaboration tools for years. In an effort to become more user-friendly, Microsoft recently added new features to Office 365, including two security upgrades and the addition of productivity tracking. Keep reading to find out more about Office 365's new Azure Information Protection, Enterprise Mobile Device Management and Productive Insight features.

Continued on page 4...

Cybersecurity threats to look out for in 2017

Continued from page 1...

As mentioned before ransomware will continue to be on the rise. Throughout the past year we've had various articles about ransomware with new and different methods and targets featured in our newsletter. That is unlikely to end. In fact a recent article we had about the San Francisco Municipal Transport Agency where their systems were frozen and they had to let people ride for free. This is an example of where ransomware might lead, a trend in delivering virus payloads that can infect hundreds of machines quickly.

There is also the threat of IoT (internet of things) connected devices as we have talked about too. We saw the attack that shut down part of the internet by using these devices vulnerabilities. This is certainly a concerning area of security because it is hard to protect ALL of the devices out there, and new ones are coming out all the time leaving the manufacturers to provide the security measures for their own devices. Consumer devices are not the only ones susceptible to attacks either. More industrial organizations are using internet connected devices to drive their operations as well.

As we are finding ways to protect us from external threats there is also the possibility for hackers to find different ways into a network. This could come in the form of internal threats. It might not be someone internally who is in fact the hacker, but hackers could exploit individuals with threats they can use to manipulate someone (such as something that could compromise their employment) or through social engineering.

No matter what year it is the threat of hackers is always a little scary, but there are measures that you can take to in order to better protect yourself and your business. Having a plan and security measures in place can help to secure your network as well as vulnerability tests to see where weaknesses might lie. If you are ever concerned about the security of your network let us know we are here to help.

Shiny gadget of the month: Dot: The Physical Push Notification

It is now 2017 and smart devices and technology just keep coming out, each more exciting than the last. It seems like there is always a new device coming out to help us make our dumb homes, smart. I personally think it is exciting and have been slowly accumulating smart home devices over the past year, some of which have been written about in our newsletter (WeMo switch, Amazon Echo, etc). The Dot is yet another extension for home and workplace automation. It can make excellent use of smart devices you already have, or can be functional all on its own.

They call it Dot: The Physical Push Notification, but it can be so much more than that. The way that it works is by working with your phone and Bluetooth technology to communicate and give instructions based on parameters you set. So you can use the dot to send you notifications relevant to your surroundings, or command your smart home based on your location. For example you can use it as a digital post-it note (and if you are like me this would be awesome), so if you are out in the middle of something and have a thought like when I get home I need to remember to do ____. You can send a note so then when you walk in your door your phone notifies you of that reminder. How cool would that be! Same could be used in reverse to make sure you bring a certain something with you when you are heading out the door (how many times have you run out the house and forgot something you needed).

It can be used for more than just notifications too. As I mentioned before if you have smart home devices you can use the dot to control them as well. So if you have smart lights you can have the dot turn them on and off as you move throughout your house. The same concept can be used with smart plugs or even Spotify music to move throughout the house with you. Some other examples given was to arm your security system when you go to bed or leave the house, even adjust the temperature using a smart thermostat.

This is not just a gadget for your home either. You could use it for work too. Have the dot set to notify you if your boss emails you with a colored light indicator or have notes pop up when you sit down at your desk.

The dot is a fascinating concept that could have so many different uses. They are aiming for a March launch and currently have pre-orders on their kickstarter page of $20 for a single dot, $55 for three, or $85 for five. They have raised over $115,000 which far surpasses their $20,000 goal. I look forward to seeing how these are adopted in the market and what uses people find for them.

Take a look for yourself at http://bit.ly/newsletterdot.

Gift Card Trivia!

This month's question is:

What method did the hackers use to infect the San Francisco Municipal Transport Agency? *(Hint: The answer is in this newsletter.)*

a. Social media
b. Deliver virus payload
c. Had a spy infiltrate the MTA
d. Spam

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **February 3rd**, 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
- 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
1120 Crown Point Road
Westville, NJ 08093

North Jersey
5 Regent Street, Suite 520
Livingston, NJ 07039

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at
www.swktech.com

SWK TECHNOLOGIES

Office 365 reveals new security features

Continued from page 2...

Azure Information Protection
Using Office 365 protection technology, also known as Azure RMS, this feature allows business leaders to mark sensitive documents and control who has access to information in various documents. The protection travels with the data, whether it is online or provided through another device. Business owners can mark a document as internal and keep it from being sent outside the company. Drop-down menus also allow users to apply trackable data protection in order to identify potential leaks and gain insight into how a business is structured.

Enterprise Mobility + Security Suite
Re-branded from the Enterprise Mobility Suite, this feature adds more security potential to sensitive data while allowing business owners to manage apps on any device from one location. Users have more control over identity-driven access and also encrypts data to allow secure collaboration among employees.

Productivity Insight
This feature, an addition to Delve Analytics, tracks an employee's time management at the office. MyAnalytics for Outlook allows business owners or managers to see who has read, replied, and forwarded their email while also providing them with information on the email sender. The feature also acts as a storage receptacle for shared files and contact information so they can be accessed quickly.

As Office 365 expands its services to include security and productivity features, companies using cloud-based servers have an advantage over old-school computer users. Not only do they have access to the technology to keep their data safe and accessible to employees, but they also have the management software to see where their efforts are paying off by way of productivity programs. If you need to know more about the new features of Office 365, give our professionals a call. We can answer your questions and help you get the most out of the new Security and Productivity Insight additions.