# IT Strategy Brief

ISSUE 3 | VOL 4 | March 2018

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

## What's Inside:



## Majority of Businesses Fail Cyber Readiness Tests


The Hiscox Cyber Readiness Report 2018 – released early last month – revealed that 7 out of 10 of the organizations surveyed were not able to meet cybersecurity readiness standards. The report surveyed executives and IT personnel from more than 4000 companies in the U.S. and Europe. Approximately 1000 of those were based in the U.S., and for the largest of these the survey also found that costs from a cyberattack could reach up to $25 million.

The sectors that are targeted most often according to the report are financial services, energy, telecommunication and government entities. Technology and communications sectors were more likely to have personnel knowledgeable in cybersecurity, while professionals had the least. The study also found several correlations between company size, IT budget, and cyber readiness. Generally, the more that an organization had devoted to improving their cyber defense, the higher their readiness. Despite this, those the survey deemed "cyber experts" were just as likely to suffer from an attack as those labeled "cyber novices."

The report makes several conclusions from these facts, including that the introduction of the General Data Protection Regulation (GDPR) and similar legislation that mandates breach notifications as a legal requirement will cause a significant paradigm shift. It also found that one of the big differences between cyber experts and novices was the level of response to network incidents they had suffered and the steps they took to prevent future occurrences. Hiscox made several recommendations for improving cybersecurity, including for businesses to improve training and processes in addition to IT budget spending, as well as for smaller organizations to consider delegating their network monitoring to outsourced IT firms.

The Hiscox report represents the reality of modern cybersecurity, in that current trends are constantly shifting faster than many organizations are able to adapt to. Modern network defense requires a proportionally greater amount of commitment and effort to be able to successfully thwart breach attempts. Those that are not prepared for this evolution might find the level of time and resources necessary to defend against every conceivable threat to be staggering.

MSPs such as SWK Network Services will able to remove some or all of that burden for SMBs and enterprises by providing external IT support in a timely and cost-effective manner. Our focus on managing your network allows us to put all of our energy into you and protecting your network so that you do not have to divert time away from managing your business. Contact us to learn how you can accurately determine your cyber readiness with a Network Vulnerability Test.

## 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:

**Peggy Harrington**
**LM Service**

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 6th** to get your name in the hat.

## You could win a $25 Gift Card!


# Insurance, Manufacturing, and Tech Most Likely to Be Victim of Phishing

A study carried out by cybersecurity firm KnowBe4 earlier in 2018 was able to discover which industries were most likely to fall victim to a successful phishing attack. The survey of 12 industries and services included testing of employees within those sectors at regular intervals to determine their likelihood for succumbing to phishing attempts. In total, six million personnel in approximately 11,000 organizations of various sizes were surveyed, and about 30 percent of those tested in each industry were found to be susceptible to phishing attacks.


The industries studied were divided into 12 categories: Insurance, manufacturing, technology, Not for Profit, Retail & Wholesale, Energy & Utilities, Healthcare & Pharma, Education, Business Services, Financial Services, Government, and Other. The sector found least likely to fall for a phishing attempt was Government with approximately 25 percent. The public sector performed a full percentage point better than the next private industry, Financial Services, which stood at 26.3 percent. The worst by far was Insurance with 32.7 percent of employees found to be vulnerable to phishing attempts. It was followed by Manufacturing at 31 percent, Technology at 30.1 percent, Not for Profit at 29.9 percent, and Retail & Wholesale at 28 percent.

The study also found that size also had a significant impact on employee phishing readiness. Smaller and medium-sized Insurance businesses performed worse than those with over 1000 employees, with 35 percent, 33 percent, and 29 percent, respectively. Insurance was the only industry to perform consistently badly across the board, but it was still followed closely by Manufacturing and Technology. Not for Profit was the next sector where organizations with under 250 employees were phish-prone, as well as the most likely for organizations with over 1000 personnel to become a victim of an attack. Business Services were the least likely larger organizations to be phishing-prone with just under 20% of employees found to be susceptible, followed closely by Government at 20.8 percent.

Phishing has become one of the most common hacking attacks and developments over the past few years indicate that hackers are increasing the amount effort they put into entrapping their targets. Some cybercriminals often now devote more time into researching potential phishing victims, especially if they are perceived as having access to something valuable. There are even breach attacks tailored just for executives and other gatekeepers of sensitive corporate information. As the study shows, however, these types of cybercrimes do not affect just commercial businesses, but extend to government agencies and not for profit organizations (NPOs), such as religious institutions and consumer protection departments.

If you are in one of these phish-prone industries, or are just worried about phishing in general, then you should look into our Phishing Defender employee security awareness training. We provide testing for your network and training for your employees to help you be prepared for next inevitable phishing attempt. Check out https://www.swknetworkservices.com/phishing-defender/ or contact us to learn more.

## Shiny gadget of the month:
## Loomo – Robot Sidekick and personal transporter

Every year we seem to get closer and closer to having personal robots integrated into our lives. Segway Robotics, the company who mastered the art of personal transportation, has taken their devices to a new level by introducing AI to their already popular concept of upright transportation. Loomo is the name for their robotic sidekick who also serves as a mode of transportation. Simple to ride, 22 mile range on a charge, an advanced computer vision and emotion engine, and with the ability to auto follow and capture video with voice/gesture controls makes Loomo a handy little companion. It uses powerful AI to execute these functions along with the self-balancing technology of Segway to function as a transporter.

Loomo is designed to be more than just an AI Segway device, it has a loveable personality and expressions that will be sure to impress. You can get a taste for this in their video on the Indiegogo page http://bit.ly/loomogadget. You can even take the helm and go into avatar mode where you can use your mobile device to control Loomo and see the world through its eyes. It also can take pictures, be equipped with a tray, and many other things. Oh, by the way you can ride on it too.

If you hurry you can snatch one up for yourself with an expected May 2018 shipping date while it is still on sale for the early bird price of $1299, which considering the technology is not as bad as you might have expected. It will be cool to see if this product becomes a success or not and how it might start to shape the future of personal robot assistants.

Would you use something like this? Let us know.

## Businesses Overlook Mobile Data Security

A report from Verizon released last month revealed that several businesses forfeited the data security of their company's mobile devices to ensure speed to market performance. This was influenced by a general lack of cybersecurity awareness concerning mobile platforms. Over 30 percent of the 600 organizations surveyed for the reported admitted they had ignored their mobile data security for the sake of performance, and almost 80 percent said that they considered operational disruptions to be a bigger threat that data thefts. However, nearly all of the respondents claimed they now see mobile devices as a growing vulnerability.

Mobile devices for corporate use are becoming increasingly common, and many examples of emerging technology are dependent upon connections to smartphones and tablet computers. Internet of Things (IoT) devices often work in conjunction with mobile phones or tablets remotely controlled through a wireless connection. Advances such as these provide new opportunities to streamline operations, but also may create network access points for attackers.

Data security for mobile will gradually become an integral part of cybersecurity as they continue to proliferate in the workplace. Mobile devices can be just as vulnerable as personal computers to external cyber threats, if not more. Lax physical mobile security can also allow anyone who is able to interact with it directly to gain entry into sensitive data stored on the device, including corporate login information.
There already exists several types of malware that have been created specifically to infect smartphones or tablets. Many of these malicious files are hidden in third party apps that may even get past publisher app stores, especially if your device is not using the latest update. Yet there is also a chance to download malware while browsing mobile versions of desktop websites.

It is important to include your mobile devices in your company's cybersecurity strategy, as they represent an ever-present reality of the modern workplace. Even personal smartphones can become a threat if employees use them for internal functions, such as directly accessing your company's web assets or carrying digital transactions. Hackers may use individual devices as loopholes to penetrate deeper into your system.

If you are unsure of how your company or personal mobile devices may be affecting your cybersecurity, or if you suspect that one may have compromised your network, then contact us right away. We can help protect you and educate your employees on how to use their devices correctly.

## Gift Card Trivia!

This month's question is:

____ out of 10 organizations surveyed were not able to meet cybersecurity readiness standards *(Hint: The answer is in this newsletter.)*

a. 7
b. 5
c. 8
d. 3

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

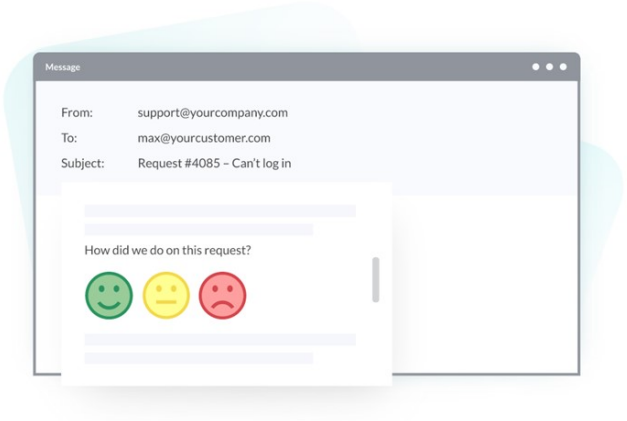
Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at
www.swknetworkservices.com

SWK TECHNOLOGIES

## Were you left with a smile?

In case you have not noticed SWK Network Services has recently implemented a one-question survey to all closed support tickets. Now, at the close of each issue, you will receive an email letting you know that we've completed your ticket. In that email there will be three smiley faces like this:




We would really appreciate if you'd click on either the green, yellow, or red smiley face to let us know how we did. Green = positive, Yellow = neutral and Red = negative. It'll only take a second! You'll then be able to leave a comment if you'd like to detail the reasons behind your reaction.

This will help us to ensure that you're satisfied at the end of every service ticket and that we're offering you the best possible service. We had previously been using the ConnectWise survey's before and barely getting any responses because you would have to read and rate about 5 questions.

Since implementing SmileBack our response rate has increased significantly. We would like to encourage you to submit your feedback after every ticket. We are looking for constant feedback to make sure our clients are happy with our service delivery.