Ashton
TECHNOLOGY SOLUTIONS

This Issue:

Our Top Tweets

@ConnectWise Keep your clients protected from ongoing threats with protection from ConnectWise vendor partner, Sophos. **http://bit.ly/2ybFse8** Ashton Solutions added, Looking for more info about **@Sophos** security solutions? Read the article, and then contact Ashton Solutions.

@AshtonSolutions Getting ready for **#PalsInMotion #Parkinsons** race **#CLE** …

@arstechnica Kaspersky software banned from US government agencies http://arstechnica.com/tech-policy/2017/09/kaspersky-software-banned-from-us-government-agencies/ … by **@joemullin**
@AshtonSolutions Retweeted Ars Technica
We dont have 1st hand experience with Kaspersky, but do you trust your security coming from a provider banned by the US govt? **@Sophos** works!

@AshtonSolutions We get called in to fix a lot of IT messes. This is work done by a global comms company who works with militaries and governments. Really??

Our Sales Team Contact Info

Jim Abbott
jabbott@ashtonsolutions.com
216-539-3685

Peter Bunevich
pbunevich@ashtonsolutions.com
216-223-7010

Visit us **online** at:
newsletter.ashtonsolutions.com

Mobile Cybercrime Puts Your Business at Risk

The opening ceremonies of the Olympic games are always a spectacle, and the people of Pyeongchang County in the Republic of Korea didn't disappoint. While the world watched, behind the scenes there was a cyberattack going on. The attack, carried out by Russian hackers, seemingly retaliating for a nationwide ban placed on their athletes at the games, paralyzed LAN and Wi-Fi communications, prevented tickets from being printed from the Olympics website, and took until 8 a.m. the following day to restore.

We reference the Olympics because for the past three Olympic games, the Pyeongchang games, The 2016 Summer Olympics in Rio De Janeiro, Brazil, and the 2014 Winter Olympics in Sochi, Russia have all been marred somewhat by cybersecurity issues. If an event that is planned for years in advance--and has the cybersecurity budget the Olympics has--what does that mean for you and your smartphone? This month, we will take a long look at mobile cybercrime, its increased relevance, and what you need to know to combat hackers that target mobile.

Mobile Is Just the Next Step

When you consider just how much people depend on Internet-connected computing, and how many applications are developed that require Internet access, it can't really be a surprise that Internet-related crime increases at similar rates. The problem is that the rate is substantially higher that many people were ready for; and it is causing a lot of problems for computer users all over the world.

Cloud Storage Offers Benefits to Small Businesses

With businesses dealing with and storing more data, cloud storage platforms have begun to be extremely important for the modern small business. It took a while for small business decision makers to implement cloud storage solutions for their businesses, which is largely to blame on the stigma of insecurity the cloud had. Today, however, cloud platforms are used for all types of utility. Today, we'll go into the types of cloud storage, and their benefits to a small business.

The most common types of cloud storage constructs available today are:

- **Public** - The public cloud is perhaps the most accessible form of cloud storage for both individuals and any type of business. This is because it's generally implemented with the consumer in mind, often being either free or much cheaper than other alternatives. To this end, the public cloud can be a convenient way for a business new to cloud storage to take advantage of it. It provides most functionality that any other cloud can provide, but has its limits in terms of customizability and flexibility. For example, you might have to pay extra for additional cloud storage space or security measures.
- **Private** - The private cloud is typically reserved for businesses that want a more hands-on approach to managing their cloud data storage. Whereas the hosting company is responsible for hosting and managing the public cloud storage, the private cloud would be managed by technicians of your choosing. This affords you many technical freedoms that you wouldn't otherwise get with your cloud storage solution, including the ability to

"Technology, like art, is a soaring exercise of the human imagination."
– Daniel Bell

Are Healthcare Providers Meeting HITECH Standards?

Compliance can be difficult for some businesses. They might know that it's a necessity--and may even know what they have to do--but they just have trouble implementing practices that are designed to guarantee the meet their regulatory responsibilities. HIPAA and HITECH compliance laws in particular are difficult to navigate, and the results of failing to adhere to them can be dire.

Just a few years ago in 2016, the Office for Civil Rights (OCR) and the Department of Health investigated data breaches; the results of this investigation led to identifying several violations of these laws. A total of 12 settlements were the results of this investigation, as well as one civil penalty, that amounted to claims of approximately $25,505,300 in fines.

The numbers in 2017 are slightly more optimistic. This past year, there were only nine HIPAA settlements and a single monetary civil penalty paid totaling $19,393,000 in fines. While it's clear that something is working, it's not clear what exactly is or isn't, but we know one thing for sure. Businesses don't want to pay money for failing to adhere to compliance laws, but this doesn't stop everyone from meeting their requirements.

The types of violations that led to these penalties aren't particularly varied. Most of them stemmed from a failure to protect protected health information, or PHI, but there are a couple that come from different reasons. Here are a few other reasons:

- Insufficient ePHI access control
- Impermissible disclosure of ePHI
- Careless handling of PHI
- Multiple HIPAA violations
- Delayed breach notifications
- Lack of security management process
- Lack of a business associate agreement

> *Compliance can be difficult for some businesses. They might know that it's a necessity--and may even know what they have to do--but they just have trouble implementing practices ...*

Another notable trend can also be seen in the failure of organizations to secure their mobile devices in a way which complies with HIPAA and HITECH. Furthermore, there is also a failure to implement proper security processes and delaying notification of breaches at the heart of these fines.

Recently, a well-publicized lawsuit was filed in federal court against 60 Indian hospitals over a failure to adhere to the HITECH Act. These hospitals had allegedly failed to provide records and documentation for as many as 50% of their patients within three business days of the request. As one of the requirements of receiving funding from the HITECH Act, this is a big issue for hospitals.

As a result of these failures, these hospitals face charges of well over $1 billion for failing to provide healthcare documents when asked to produce them. They obtained $324 million through the HITECH Act, but failed to adhere to its laws. Additionally, the hospitals violated the Anti-Kickback Statute and the False Claims Act for claiming falsely that they met the requirements of the HITECH legislature.

While it's true that not all businesses need to consider healthcare compliance, it's more likely than not that your organization works with some sort of sensitive information that is subject to compliance laws. To find out now if your organization is in trouble with compliance laws, reach out to us at 216-397-4080.

Share this Article!
http://bit.ly/2I2RCuC

Cloud Storage Offers Benefits to Small Businesses

implement additional security measures.

- **Hybrid** - A hybrid cloud solution for cloud storage can often be an ideal compromise between the public and private cloud. It's a great way for businesses to ensure that they get the services that they need, at a cost that makes cloud computing viable.

Benefits of Cloud Storage
So why would you choose to utilize cloud storage? For one, the functionality and availability to create the cloud platform that is right for you. If you have IT management staff online, or you have a trusted outsourced provider like Ashton Technology Solutions, a private cloud is the most secure and manageable, but the cost and effectiveness of many public cloud offerings can go a long way toward allowing you to reduce your upfront technology costs.

Beyond cost, there are several benefits that cloud storage affords a small business. For one, the availability of the data on the server provides great value for any business because today's work often calls for mobility and collaboration. Another main benefit is that cloud platforms have a continual sync, which ensures that when you save work, it's the same work when you go to retrieve it. Finally, the scalability that cloud storage offers allows your organization to get the storage space you need; helping avoid cost overruns, while allowing you to scale up when needed.

Does your business need help understanding which type of cloud storage is most effective for your specific situation? Ashton Technology Solutions can help. To learn more, call us today at 216-397-4080.

Share this Article!
http://bit.ly/2InkwsK

Ashton TECHNOLOGY SOLUTIONS

Mobile Cybercrime Puts Your Business at Risk

(Continued from page 1)

When we talk about mobile cybercrime, however, we are mostly talking about the act of using mobile devices as a revolving door in which hackers access secure networks, steal data, and personally identifiable information by the terabyte. In a study conducted by Nokia in 2016, over 1.3 of every 100 phones has some form of malware on it, a whopping increase of 400 percent over 2015. The percentage is growing, and fast. Now four-in-every-five malware infections happens on a smartphone.

Mobile constructs are being infected, and hacked, and data is being stolen, repurposed, and sold. There are several ways that people are able to accomplish this. They include:

Data Leakage

Mobile apps have transformed the way that computing constructs work. They are so effective that the largest software company in the world, Microsoft, altered the way they go about application development when developing Windows 8. Using the format used by mobile platforms developed by Apple and Google, the "app" allows developers to utilize the touchscreen to create a more "hands on" approach than the traditional mouse and keyboard approach used by desktop applications.

All apps aren't created equal, however, and some are developed with vulnerabilities, or worse yet, developed to appear to be a useful app and are just malware or spyware. Today, the term for these types of apps is "riskware". When you download an app (or install it as an .apk), almost immediately there is a screen that pops up where you get to choose which permissions the app can

have on your phone. The best way to avoid this kind of data seepage is to:

1. Ensure the app you are installing on your device is the real McCoy.
2. Only allow the app to have the permissions it needs to be effective.

By keeping apps from having full run of your device, all you are doing is mitigating potential problems.

Network Spoofing and Unsecured Connections

With so much content available to the mobile user, and carrier-enforced data caps still prevalent, many people will want to access any Wi-Fi they can to save their data. While this is great...

Automation Helps Deliver Secure Networks and Infrastructure

If you do it manually, your business is spending countless hours on implementing patches and security updates. That's not even mentioning the many other tasks that pile up if your technicians are simply too busy to get to them. Wouldn't it be nice if these routine maintenances could be issued without the need for an on-site visit? Automation maintenance and management can certainly be worth the investment.

Remote Monitoring and Management, or RMM, can be used to take advantage of some of the greatest benefits out there for small business technology maintenance. Here are just a few of them.

Patching and Updates

Keeping your business' applications up-to-date is vital to the success of your organization. Unfortunately, it can be a time-consuming process that eats up too

much of your company's resources to be effective. Depending on the number of workstations, servers, and network components your business has, this process could range from a short amount of time to an incredibly long and drawn-out process. A dedicated monitoring and management service can help you apply patches without the provider being onsite to do the work. This means that they can be applied as they are released, removing the need to manually install updates every time they are issued. Furthermore, these patches can be applied en masse, building (and maintaining) a more agile network and infrastructure.

> *"Remote Monitoring and Management, or RMM, can be used to take advantage of some of the greatest benefits out there for small business technology maintenance."*

Network Security Management

You need to react to threats to your infrastructure, but you also need to prevent them from reaching your network in the first place. If you can detect attacks and deflect them immediately, you can prevent a considerable amount

of attacks. This is made simply by implementing remote security management. Offsite technology support makes this possible by alerting technicians in the event of any type of breach, giving them the tools they need to battle incoming security issues.

Save Time and Resources

When you take advantage of remote monitoring and management, your business gets immediate relief without waiting for the technician to arrive onsite to resolve the issue. Most issues can be resolved without the visit, so this ultimately winds up saving your business plenty of time and money. Plus, if you're not the one administering patches and updates, you will have resources available to work on other important initiatives.

Does your company want to take advantage of remote monitoring and maintenance? Reach out to Ashton Technology Solutions at 216-397-4080.

Ashton
TECHNOLOGY SOLUTIONS

A Physical Backup Has a Place in Your Overall Strategy

Physical data backup can be a key part of data backup and disaster recovery. Even if you utilize the cloud for your business continuity solution, there can be no discrediting the importance of having physical data backup. A simple physical data backup can be effective under the right circumstances.

Here are some of the most important factors to consider for any physical data backup system that your business uses.

Types of Physical Data Backup

Your business could already be using any number of physical data backup devices. Some of the most common include USB hard drives, solid state drives, thumb drives, and tape-based backups. These all have different uses depending on what their intended purpose is. For example, a thumb drive allows for great ease of portability for certain data. If you're only taking something on the go, perhaps a thumb drive is ideal. On the other hand, a hard drive or solid-state drive is ideal to store lots of large files, as they generally have a much higher capacity. These are typically designed to be used for portability purposes--not necessarily data backup.

Tape backup is the primary method of on-site physical backup. Essentially, it allows organizations to store copies of data on magnetic tapes and keep them somewhere on or off-site for restoration at a later date. Tape has fallen out of use in recent years, however, as it is simply less convenient than cloud-based business continuity solutions. Yet, this still shows that physical backup was (and still is) considered of major importance.

How to Effectively Use Physical Backup

The important thing to remember about physical backup solutions is that they are no longer the optimal method of data backup and disaster recovery for your organization. This is primarily due...

Read the Rest Online!
http://bit.ly/2wjlQYC

At Ashton Technology Solutions, we don't think of ourselves as computer guys, geeks or techies. Instead, we're problem solvers in the business of helping clients leverage technology for lasting business results. We just happen to have some serious technical skills as well. Of course we can talk geek with the best of them, but that's just the starting point for what we do, not the heart of it.

While we do take pride in delivering the most technically elegant solutions, at Ashton, we get the biggest satisfaction from integrating into our clients' processes, helping them look ahead, avoid trouble, and find better and more cost-effective methods of operating. In other words, we become partners in their growth. Ultimately, we earn our real enjoyment by watching our clients grow and prosper right along with us.

3 Pieces of Software that Read the Screen to the User

If we're all going to be honest, the ability to read is an underappreciated skill. However, many people need assistance with reading, often due to some visual impairment or learning disability. Preparing yourself for the day when someone in your office may need the assistance is a simple step in the right direction. For your consideration, we've compiled some of the most common screen reading software titles.

Job Access with Speech (JAWS)

JAWS has a history of being the most common screen reading application worldwide. In 2015, JAWS was the program of choice for 30.2% of frequent users, while infrequent users made up about 43.7%. Whether the user is browsing the web, reading content like articles and ebooks, reaching out to a team member through telecommunication, or is engaged in another activity, JAWS can simplify their process - even if that user is still using Windows Vista!

Windows Narrator

A standby on every version of Windows since Windows 2000, Windows Narrator...

Read the Rest Online!
http://bit.ly/2wmZO7u

Ashton Solutions

23625 Commerce Park
Suite 130
Beachwood, Ohio 44122
Voice: 216-397-4080

Visit us **online** at:
newsletter.ashtonsolutions.com

✉ newsletter@ashtonsolutions.com

f facebook.ashtonsolutions.com

in linkedin.ashtonsolutions.com

🐦 twitter.ashtonsolutions.com

g+ google.ashtonsolutions.com

🔲 blog.ashtonsolutions.com

THIS ISN'T WORKING RIGHT...
I HAVE A BACKUP, BUT I DON'T SEE...
BACK UP.
NO. BACK AWAY FROM THE COMPUTER. I'LL FIX IT.