Newsletter

Celebrating 30 years serving Central, N.C. *April 2020*

Top Security Risks and Solutions for Cloud Computing

Remember at the end of 2013 when most of us were getting ready for the Holidays, hackers were in the process of stealing around 70 million Target customer's information. This security breach was one of the worst to date, granting hackers the access to millions of customer's names, addresses, and phone numbers. However, Target was not the one completely at fault in this case. Instead, Fazio Mechanical Services a smaller HVAC company that worked for Target was the origin of the hack. By hacking this smaller company the cyber attackers discovered themselves to the secret ingredient, the sensitive credentials, that retrieved personal information from millions of shoppers.

The moral of this crisis is that small and medium sized businesses are the ones hackers are trying to lure in; though there is not much gain in the beginning, the end prize may just be as big as Target. We cannot chalk instances like Fazio Mechanical Services all up to ignorance, instead it is best to understand where the risks lie when it comes to using Cloud services and how a few changes in procedure can eliminate those risks. As we have learned, you never know if you could be next.

Data Breach

We all know that a data breach is the loss of crucial company information, but we may not know that the Cloud gives hackers multiple opportunities to attack the master computers holding this information.

For example, we tend to use local restaurants, hotels, and coffee shop's Wi-Fi or our own hotspots to do business work. This leaves our phones vulnerable because hackers are preying on us to open sensitive documents from our email or other applications that use the Cloud in order for them to steal the information. Also, some of our social media applications such as Skype, Twitter, and instant messaging apps use local hotspots without your knowledge. Typing out a client's personal information via the messenger app can leave you at fault for allowing confidential information to get in the wrong hands.

Upcoming Events

Webinar: Office 365: How to Fully Protect Your Data
April 2, 2020

Life in the Cloud: Security & Backups Panel Discussion
POSTPONED

Webinar: The Wireless Revolution
May 14, 2020

For more information on our upcoming events, please visit https://www.tcsusa.com/calendar/.

One last way a hacker can get information over your phone in a public area is using VOIP which allows them to listen in on conversations during a Skype or Facetime meeting.

However, there are some ways to prevent data breaches such as these over your personal or company's phone. You can make your information more difficult to access depending on your location.

This would mean more questions to pass before you can visit your client lists and calendar full of appointments and meetings, but it also means the hacker a few feet away from you will have a hard time getting every access question correct. You can also simply avoid unsecured networks such as those at your local coffee shop or restaurant; instead, you could choose to do any vital work activities at your job or at home.

Data Loss

Another Cloud security risk that no one likes to think about is data loss. What is worse is knowing that it can be an accident. We expect our data center support to help keep things running smoothly, but sometimes work mishaps occur. Remember the last time you thought you lost a crucial thumb drive, but in the end it was in your second briefcase at home.

Another example of data loss is through the use of a BYOB policy. Employers can be unaware that their employees' phones, iPads, and computers are jailbroken or rooted. This turns the device into a less secure version of its original. Also, employees' devices may not have the newest edition of a security application, use short passwords, and have many accepted permissions. However, the issue with solving BYOB matters is that "according to the Ponemon BYOC study, a majority [64%] of respondents say their companies can't confirm if their employees are using their own Cloud in the workplace."

Data loss through the use of the Cloud does occur, but there are a few ways your company can prevent this security risk. First, you may want to try working with a Cloud expert, either an IT analyst or a third party auditor to ensure your Cloud Provider Services are compliant. For further reading " Seven Questions to Ask Before Moving to That Application to the Cloud." It is best to know which devices and applications your staff is using, and possibly dismantle the BYOD policy if it is not an efficient system.

Shared Infrastructure

One of the risks that many Cloud users forget is that a database has multiple users on a single infrastructure. Like an apartment infestation, when one company is hacked, the other companies feel the pain.

Cyber criminals have an easier time hacking into everyone's data once they have the special credentials to access one company's information. Also, if a Cloud Provider is careless then this can hurt everyone using their infrastructure.

A shared infrastructure means that you should not only encrypt information during entry into the Cloud, but it must be encrypted in the Cloud.

Encryption should take place before uploading to the Cloud, and can then only be decrypted by those that own the correct credentials. Lastly and as always, to prevent any future risk due to this make sure your passwords are strong by using various characters, cases, and numbers.

As we recall Target's data breach, we must remember how it all started with a single medium sized business. Yet, anyone can prevent all of the risks that come part and parcel with Cloud computation by taking a few simple steps forward in a secure direction.

Why HIPAA Should Not Deter You From Storing Your PHI in the Cloud

Cloud-based Software-as-a-Service (SaaS) systems deliver high-value, cost-effective information services in the healthcare industry. However, many healthcare providers are not sure about how to leverage cloud computing technology while complying with HIPAA regulations for the privacy and security of protected health information (PHI). Perhaps, an understanding of and confidence in the ability of cloud healthcare solutions to satisfy industry standards and laws will see more hospitals trust the technology with the storage of sensitive patient information.

What are the Main Cloud Security & HIPAA Compliance Issues in Healthcare?

HIPAA privacy and security rules regulate PHI handling and storage, and noncompliance exposes healthcare providers to hefty fines. So, before moving their databases to the cloud, hospital CIOs want security guarantees that unauthorized third parties may not access, copy, or steal patient names, Social Security numbers, medical files, financial information, and other personal data.

The Perks That Come With Storing PHI in the Cloud

Once healthcare establishments address cloud security and HIPAA compliance concerns satisfactorily, they can start enjoying the benefits of storing PHI in the cloud (some may include additional fees), such as:

Quick data access: Hosting healthcare records in the cloud makes it quick to access them, which translates to high usability. For example, a hospital may have several cloud-hosted servers in various strategic locations close to where most of its customers are.

Locating a data center close to its users helps minimize latency and improve application performance, increasing the clinical value of the stored healthcare information.

Cost-Effectiveness: Cloud computing eliminates the need for healthcare providers to build and maintain expensive data centers and applications. Lower IT investment costs may then translate to more days cash on hand, which is great for a hospital's liquidity.

Safe backup/disaster recovery options: The cloud is ideal for implementing disaster recovery and business continuity options. Healthcare providers can have redundant IT systems hosted in the cloud for their quick deployment in case of primary data center failure. Such redundancies are very critical to the continuity of hospital operations. Likewise, cloud-based disaster recovery measures prevent the permanent loss of PHI in the event of natural disaster, malicious/accidental deletion, or theft.

How to Secure PHI in the Cloud as Per HIPAA Privacy and Security Rules

1. Anyone who handles sensitive patient data in a healthcare organization must be aware of HIPAA rules for data information protection. All personnel and parties involved in the creation, receipt, transmission, or maintenance of electronic PHI should undergo formal training to meet compliance standards. IT professionals in healthcare establishments should figure out their legal responsibilities as well as the obligations of their SaaS providers as per HIPAA rules. A secure cloud-based system for storing patient information should address the following:

- Encryption of data during transmission as well as storage
- Data ownership
- Portability of data
- Integration of information systems through APIs and open interfaces
- Protection of structured and unstructured data

2. It is also critical to conduct a compliance assessment to reveal any loopholes in native data protection strategies.

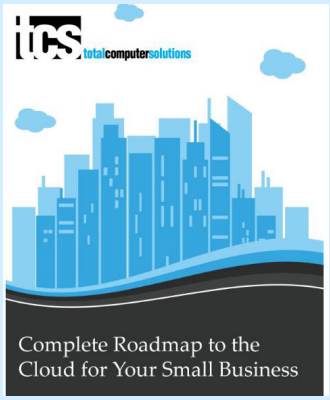
- How likely is it for a user to accidentally delete patient data?
- What is the possibility of data loss due to application integration mishaps?
- How safe are the hospital records from malicious insider-actions or hacking?

Addressing these concerns is critical to HIPAA compliance.

3. Likewise, a healthcare organization storing sensitive patient information in the cloud should have an HIPAA-compliant backup system. Be sure to test your SaaS data protection solution to ensure it can facilitate quick and accurate data recovery. The system should support automated and on-demand backups to inspire more confidence in its ability to prevent the permanent loss of critical patient data.

Compliance with HIPAA rules in the provision of healthcare services is achievable, and it need not deter hospitals from moving their patient data to the cloud.

FREE Guide: Complete Roadmap to the Cloud for Your Small Business



If your company has 5-100 users, the Cloud could be a reliable solution. The benefits of moving your business to the cloud include less on-site hardware, and software maintenance costs, lower capital expenditure costs, predictable IT spend, remote access to cloud data and applications. Throughout this guide, we will walk you through these benefits and provide suggestions for choosing whether it is right for you.

Get your FREE copy today!
Visit tcsusa.com/resources/e-books/

If you would like to receive our newsletter digitally, please email alimbers@tcsusa.com.

totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

Webinar: Office 365: How to Fully Protect Your Data

Join us for our upcoming webinar!

Date: Thursday, April 2nd
Time: 11:00 AM ET
Presenter: *Greg Kirkman, Analyst,Total Computer Solutions*
Registration: Visit www.tcsusa.com/calendar/ or call 336.804.8449

A staggering 60% of companies that lose data close within six months of the loss. Data loss can be a significant concern for Office 365 users because Microsoft's security and backup policies cannot defend you against malware or guarantee a thorough and rapid restore of lost data. Microsoft does what they can to safeguard their customers, but they do not specifically specialize in security or data backup and recovery. Therefore, the customer is responsible for keeping their organization's data safe in the cloud.

Data loss, and the concern that surrounds it, can be easily avoided by following and implementing security guidelines and policies as well as having a backup and recovery solution in place.

Key Topics for Discussion:

- What can you do to keep your email secure?
- Why you should use third party backups?
- How is your MSP critical to this process?

In this webinar, we will discuss ways to help keep your Office 365 account secure and minimize the risk of data loss.