Newsletter

Celebrating 29 years serving Central, N.C.! *November 2019*

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 led 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. therefore, we cannot chock 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.

Cloud Computing's Risks and Solutions

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. However, 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 easily. Also, some of our social media applications such as Skype, Twitter, and instant messaging apps use local hotspots without your knowledge. Therefore, 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. 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.

Continued on inside

Upcoming Events

Open House Celebration
November 8, 2019

Webinar: Preparing for Windows 7 End of Life
November 13, 2019

CIMP 2019 Conference
November 15 & 16, 2019

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

Continued...

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. But, it is worse knowing that it can be an accident. We expect our data center support to help keep things running smoothly, but sometimes work mishaps occur, which we all can relate to. 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, which 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. Also, 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.

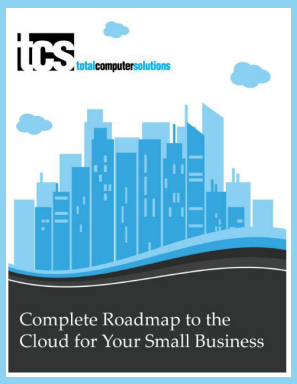
Shared Infrastructure

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 sitting lazily 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. For more information about Cloud computations risks, and prevention recommendations to eliminate those risks take Total Computer Solution's free Cloud consultation. TCS has plenty of experienced analysts to help sort out your fears about Cloud moving.

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/

Follow us on social media!

TCS along with The Guilford Merchants Association and Greensboro City Council District 5 member, Tammi Thurm, held a ribbon-cutting ceremony to celebrate the recent move of its headquarters. The event was held on Wednesday, October 16th at 5601 New Garden Village, Greensboro, NC 27410.

TCS clients and civic members attending the Cybersecurity Panel Discussion at the new Hyatt Place Greensboro/Downtown on Thursday, October 17th. The expert panelists discussed cybersecurity, including common risk scenarious and how to respond in the event of an attack.

totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue:

webinar

Preparing for Windows 7 End of Life

Join us for our upcoming webinar!

Date: Wednesday, November 13th
Time: 11:00 am ET
Cost: Free
Presenter: Michael Brown, Analyst, Total Computer Solutions
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449

Learning Objectives

- Understand what end of life means
- How not upgrading can have an impact on your business continuity
- Learn how to save on the costs of upgrading
- Create a plan for upgrading existing PCs to Windows 10