Newsletter

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

Why Your Business Is Not Prepared for a Disaster

Many business owners make a fundamental error when it comes to disaster recovery: they assume that their backups are working. Once those automated processes are set up, they merely assume that they are running smoothly, with few checks to ensure accuracy and capability. Then, the system goes down, or data is needed for recovery. That is when they discover that their backups are inadequate to their needs.

How Often Do You Back Up Your Data?

In general, we recommend that business owners back up their data every fifteen minutes. Unfortunately, some businesses still back up data only every thirty minutes or less--and some are still backing up manually at the end of the day. Consider the volume of data you go through every day: customer information, information about your products, and invoicing, to name a few. What happens if you lose that data? 93% of businesses who lost their data for just ten days had to file for bankruptcy within a year of the disaster--and half of them had to do it immediately. Can your business weather that kind of loss?

Are You Checking Your Backups?

Many businesses have great backup systems in place. They might even be backing up every fifteen minutes, which means they will lose significantly less productivity if for some reason they need to rely on those backups. There is just one problem: they don't know whether or not those backups are running smoothly. Instead of evaluating their backups regularly, they are just assuming that they are working properly--and that can lead to disaster if you do have a data loss.

Are Your Backups Tough Enough to Withstand Challenges?

When you plan for backups for your disaster recovery, are you taking into consideration all of the challenges that could impact your business? Consider:

Your physical devices could be broken or stolen. In many cases, physical damage to your devices--including both tablets and laptops--can render them completely unusable. Consider the havoc that could result from an overturned cup of water on your desk or a thief who breaks into your car. If you lose your physical devices, do you have backups that will allow you to keep running your business?

Your business could be inaccessible. A disaster sweeps through your area, leaving your physical business inaccessible.

Continued on inside

Upcoming Events

Disaster Recovery Lunch & Learn
May 9, 2019

5 Simple Steps to Improve Network Performance Webinar
May 15, 2019

Night at the Hoppers
May 17, 2019

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

Continued...

If your physical building is destroyed by fire, flood, or another natural disaster, do you have the means to keep your business running anyway? Insurance can cover a lot of things, but it will not replace your data.

Your data could be deleted. All too many businesses have felt the horror of an accidentally-deleted piece of data. Worse, a disgruntled employee might decide to cause problems by deleting that data deliberately. Do you have a system in place that will help protect against those types of challenges, or are you relying on automatic backups that could also register that you deleted a specific file? How long do your backups go back? Could you restore a file deleted weeks or even months ago?

Ransomware can strike anywhere, any time. Ransomware could be devastating to your business as it locks your files away until you pay a substantial ransom--and sometimes, even the hacker who infected you will not provide the key. Sometimes, a bad actor will infect you more than once if you pose as a good target. When you have reliable backups in place, on the other hand, ransomware is a minor inconvenience from which you can quickly recover.

Regular data backups and a smooth-running network are critical to your business's overall functionality. If you are struggling to keep your network running smoothly or you need a few extra tips, sign up for our webinar, 5 Simple Steps to Improve Network Performance. Need more help with your overall security? Contact us today to learn how we can help.

Inside Tallahassee's $500,000 Cyber Attack: Why Security Awareness Training is So Important

Recently, Tallahassee, FL, fell victim to a cyber attack that cost the city nearly half a million dollars.

This high-profile security breach serves as a model cautionary tale but is unfortunately just one of many costly cyber attacks that target companies, businesses, schools, and cities. Though $500,000 may seem excessive, the average cost of a cyber attack is greater than $1 million. Though hackers show no sign of slowing, understanding Tallahassee's attack can help companies and businesses prepare for costly breaches, starting with end-user security.

Tallahassee's Expensive Cybersecurity Attack

Fortunately, Tallahassee has already started to recover a portion of the $498,000 that was stolen.

Meanwhile, investigators have unpacked some of the details of the attack.

Believed to be orchestrated by a foreign party, the hackers targeted the city's third-party payroll vendor and diverted employees' direct deposit pay. Though it is unclear how the hackers managed to infiltrate the system, officials discovered that this was the city's second major breach in the past month. A month previously, the City Manager had unwittingly sent out a virus-containing phishing email to fellow employees.

Though officials do not believe the City Manager's initial phishing email was related to the $500,000 payroll attack, cybersecurity experts interviewed by USA Today were quick to state that hackers often use the most simple means to topple secure networks: email. These emails target the end-user in a business or company, quickly introducing viruses and collecting data.

The Cost of Simple Phishing Scams

One thing is clear from Tallahassee's cyber attack: phishing attacks are a simple, common, and effective social engineering method used by hackers worldwide. Hackers use these attacks to perform a variety of illegal acts:

- Install malware in a system
- Steal sensitive information and data
- Gather login credentials

Incredibly, phishing scams cost half a billion dollars yearly for American businesses by merely targeting unwary end-users. Employee negligence when it comes to cybersecurity constitutes the biggest cybersecurity risk in the U.S. In fact, a recent study indicated that 27% of employees would fail a phishing test.

Often, attacks target employees in deceptively simple ways. For example, hackers might send employees an "official-looking" email that asks them to update their login credentials, thereby poaching valuable security information. Or an email might ask an employee to open a Dropbox link that contains a security-compromising virus. Whatever the case, one simple mistake can quickly escalate into an expensive breach similar to Tallahassee's.

Preventing Cyber Attacks: Train End-Users in Security Awareness

The best way to prevent cyber attacks is through a comprehensive network security strategy that includes security awareness training.

Continued on next page

Trained security consultants can help prepare your employees for attacks in a variety of ways:

- Education & Information. If employees do not know what a phishing attack looks like, they will be way more vulnerable to clicking on malicious links or visiting dangerous websites. Therefore, proper security awareness training provides employees with generalized education and training on what phishing attacks look like, how to adequately report suspected scams, and how to recognize false domain names.

- Password Policies. Strong password policies ensure that employees are familiar with the oft-ignored basics. For example, employees must be coached to keep password info private, log off of unattended devices, and avoid updating password information through links sent in emails.

- Personal Devices. Incredibly, 2018 saw 25% of healthcare organizations suffering a breach through a mobile device. With more and more employees using personal technology like cell phones and mobile devices, training needs to cover the risks of using public Wi-Fi networks, leaving devices unlocked, and encrypting sensitive emails.

- Testing. To ensure that employees grasp their training information, a solid security awareness program includes frequent tests – such as imitation phishing emails – that gauge end-user comprehension of cybersecurity.

Tallahassee's massive breach is alarming but offers an educational opportunity for U.S. businesses. By bolstering network security at every level – especially for end-users – companies can stave off the daily onslaught of hacking attempts.

Total Computer Solutions provides businesses with the Cyber Security Awareness Training they need to keep employees educated, aware, and proactive about cyber attacks. For more information, please contact us today.

TCS Tech Tips | Search

Watch our new TCS Tech Tip videos! Visit tcsusa.com/resources/tcs-tech-tip/ to find tips and tricks to help keep you more productive.

Digital Newsletter

If you would like to receive our newsletter digitally, please visit tinyurl.com/ycqvv2r6.

TCS Spotlight: Angie Goodwin

Congratulations to our Service Coordinator, Angie for receiving her ConnectWise Manage Administrator Degree; demonstrating mastery of the admin features of ConnectWise Manage. Way to go Angie!

TCS Spotlight: Tim Hicks

Congratulations to our Network Analyst, Tim for receiving his StorageCraft Certified Engineer Certificate; demonstrating competence in design and implementation of disaster recovery solutions. Way to go!

webinar

5 Simple Steps to Improve Network Performance

Join us for our upcoming webinar!

Date: Wednesday, May 15, 2019
Time: 11:00 a.m. ET
Presenter: Barry Utesch, President, TCS
Cost: Free
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449.

Key Topics for Discussion Include:

- Replacing outdated hardware
- Consumer class vs. commerical and business class machines
- Infrastructure considersations
- Bandwidth and Internet connection
- OS and application updates

If you are interested in attending our upcoming webinar, please visit tcsusa.com/calendar/ or call us at 336.804.8449.

168 Thatcher Road
Greensboro, NC 27409

In this Issue:

Lunch & Learn: Disaster Recovery: Who Defines a Disaster and What Happens Next?

Join us for our upcoming lunch & learn!

Date: Thursday, May 9, 2019
Time: 11:45 am - 1:00 pm
Location: Undercurrent Restaurant, Greensboro, NC
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449
Cost: Free
Presenters: Mark Deal, StorageCraft Sales Engineer and Carl Bjerke, StorageCraft Enterprise Account Manager

Key Topics for Discussion:

- Facts about disaster recovery and what is required to recover successfully
- Prioritize systems and criteria to determine the importance of servers
- How to preemptively prepare for minimal downtime
- Important information to know other than hardware, software, and colocation