IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

Inside This Month's Newsletter

August 2016

This monthly publication provided courtesy of Howard Globus, Security Evangelist & Partner of **IT On Demand.**

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Betting The Farm Your Backups Are Safe?

It's only natural that when you hear of a disaster you think it couldn't happen to you.

That's why, even though we're told constantly that we should diligently maintain a working backup recovery system because all our company's data could be lost in an instant, we tend to brush off the advice.

Yet disasters do happen when you least expect them, and they can happen to anyone. So to illustrate the importance of staying on top of your data recovery system, here are three tales of "data gone wrong." After all, there's nothing quite like a good horror story to inspire action!

Toy Story 2: Gone!
One morning in 1998, the animators at Pixar Studios working on *Toy Story 2* noticed that Woody's hat started disappearing. Then his boots… Then all of Woody – gone! Other characters started disappearing too.

A rogue command in their system had started wiping out data. No problem, the team thought, as they pulled out the backups. Unfortunately, the backups were bad and only had data from 10 months ago.

Luckily, one of the project leaders who'd just had a baby had recently asked to have a copy of the film installed at her house. So they drove to her house and escorted her computer back to the studios "like an Egyptian Pharaoh." And as we now know, *Toy Story 2* was saved.

Moral: It's not enough to simply run backups. You need to periodically check to make sure the data is actually getting backed up and nothing is corrupted.

46,000 Insurance Customer Records: Lost!
In 2010, Zurich Insurance announced it had lost a backup tape containing confidential data from 46,000 customer records as it was being transferred from one site to another. To make matters worse, it was later revealed that it took a full year for their headquarters to learn that the tape was missing.

While there was no evidence that the data had fallen into the wrong

Continued on page 2

hands, it was not encrypted and therefore easily accessible by anyone in possession of the tape. The company was slapped with a £2.3 million fine from the British Financial Services Authority.

> “Everything had been tied into that one database. And no backup.”

Moral: If your backups are physical, make sure they’re transported and stored securely in a location away from your computer. And regardless of whether your backups are physical or in the cloud or both, make sure they are encrypted with high-level security.

Why MegaPetCo Closed Their Doors

The fast-growing set of chain stores MegaPetCo had refused to upgrade their IT system to one that could handle their needs. One day a systems developer accidentally programmed a query that wiped out their entire database. All of a sudden, operations ground to a halt; from sales to payroll to purchasing and reporting, everything had been tied into that one database. And no backup.

They tried to sue their ISP, but between recommendations to upgrade and failure to do so, the lawsuit was dropped. Three months later, MegaPetCo filed for bankruptcy.

Moral: Just because your data is in the cloud or hosted somewhere else do not assume it is being backed up. Even if it is you should still be backing up cloud data to your own network or make sure it is going to an account that you have access to in case something happens to your vendor that is hosting your data. And as we always recommend make a backup before any major changes including mass deletions.

Why Take A Chance That Your Backups Are Safe? Our FREE Data Recovery Audit Will Help You Know For Sure!

The effects of a data disaster run the gamut from minor annoyance to a death knell for the organization it happens to. We don’t want that for you. That’s why **until August 31st,** we’re offering our complete audit, normally valued at $297, **free*** to any company in the New York City area.

At no charge, our data security specialist will come on-site and audit your current data backup and security procedures and determine whether your current system can guarantee you a fast, safe and full recovery of your data.

Depending on what we find, we’ll either give you a clean bill of health or reveal gaps in your data backup system that could prove catastrophic. Then, if appropriate, we’ll provide you with an action plan for further securing your data with our **state-of-the-art computer hard drive backup and disaster recovery solutions.**

Call (212)235-0260 TODAY and let’s make sure your company isn’t betting the farm on a flawed recovery system.

**Offer valid for prospective clients with 10 or more computers and a minimum of 1 server.*

The Ultimate Small Business Guide To Setting Up A Work-From-Home System For Your Staff

WORK FROM HOME GAMEPLAN

“The Ultimate Small Business Guide To Setting Up A "Work From Home" System For Your Staff”

Secrets Every Business Owner Must Know Before Installing A 'Virtual Network' To Allow Employees To Work From Home, On The Road, Or From A Remote Office

You will learn:

- What telecommuting is and why so many small businesses are rapidly implementing work-from-home programs.
- The single most important thing you MUST have in place before starting any work-from-home or remote office initiative.
- How one company slashed its turnover rate from 33% to nearly 0%—and increased productivity by 18%—by implementing a work-from-home program.
- How to get a FREE “Home Office Action Pack” (a $99 value).

Claim Your FREE Copy Today at www.it-on-demand.com/remote-office/.

An Overview of Internet Security and Healthcare

The frequency of healthcare organizations featured in the news as security breaches and cyber attackers continue to strike only increases. The healthcare industry as a whole has traditionally been lax when it comes to internet security practices. With almost all information and medical data being electronically stored, it is more important now than ever that healthcare IT teams minimize the risk of a cyber-attack.

Healthcare organizations and businesses suffered 57 reported data breaches in 2015, a 68% increase from the 34 incidents reported in 2014. For this year, as of June 2016, there were already more than 18 reported IT incidents. The continual rise in incidents could be the result of more responsible reporting or it could be the nature of cyber security within the healthcare industry. Healthcare organizations have become a choice target because of the notoriously low percentage of budget money spent on internet security. It is estimated that financial businesses and organizations spend double what healthcare does on keeping their systems secure and minimizing cyber threats.

The attacks plaguing healthcare businesses are done using ransomware. Ransomware attacks are not sophisticated in nature and can be performed by almost anyone with an internet connection. There are also ransomware models for hire for the truly inept who want to try to make an easy buck. The easiest way to deliver damaging software is into unsuspecting employees' email inboxes. An employee will open the email, click on the link, and the damage is done.

A hacker needs just one employee to take the bait and click on the link or attachment and the entire network is compromised. It is up to the IT and internet security teams to train their organization's staff, secure their network as much as possible, and prepare for an almost inevitable attack. Cyber-attacks and security breaches can have devastating consequences and significant financial repercussions in the form of potential lawsuits, loss of funds due to the security breach, and any fines associated.

IT teams are facing a huge challenge in updating and revamping the way they protect healthcare organizations. One way to achieve this new level of protection is by switching to a multi-layer IT strategy. In addition to the usual software updates and upgrades, all employees with access to the internet must have extensive training on how to properly and safely navigate their network. User account access can be based on priority level and who needs to be able to access which programs. Blocks and password requirements can help keep information safe. Backups and a plan for how to handle an attack when it does happen are also key components that make up the entire security strategy.

The healthcare industry faces increased cyber-attacks and security breaches each year. As the number of attacks continue to grow, IT teams are faced with the challenge of revamping their security and protecting their organization. A different approach and new spending limits are the key to decreasing the risk of a cyber-attack.

Call us at **(212)235-0260** for assistance with your cybersecurity needs. Allow our security experts the opportunity to reduce the threat of a data breach so that your business, your staff and your clients are protected.

Fiat Chrysler Program to Pay Good Hackers to Find Security Flaws

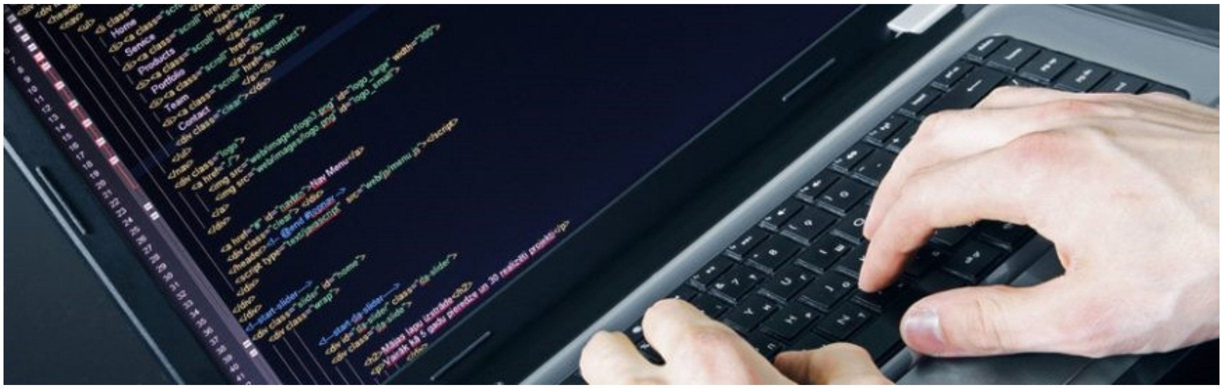
A year ago, hackers shocked the public and Fiat Chrysler Automobiles by demonstrating how they could take control of a moving Jeep. This demonstration raised concern and plenty of questions about vehicles safety and what would be done about it. Fiat Chrysler Automobiles recently announced that they would be utilizing organized hacking to find and repair security flaws in their software.

Enlisting the help of Bugcrowd, a San Francisco based company designed to manage organized hacking, Fiat Chrysler will pay hackers for uncovering cyber security flaws and reporting them. Many companies, including Tesla Motors Inc., participate in programs from Bugcrowd to help them identify and resolve security flaws. Hackers could earn up to $1,500 for uncovering an unidentified problem.

As cars become more advanced and connected to the internet with entertainment systems, navigation, and wifi capabilities, the threat for cyber attack increases as well. The increased concern is not misplaced. Cyber criminals could potentially gain access to consumer's cars, targeting them for monetary payouts. For example, ransomware could find a way in that would lock the car and prevent any functions from operating, demanding the owner pay to regain control of the vehicle.

Even with the company's own security team working to prevent cyber attacks, the new program will be used to encourage hackers to share what they may find. By having more people testing the security of the technology, potential vulnerabilities will be found before cyber attackers can exploit them. The goal is to stop attacks before they happen for the safety of the public and customers of the company.

The auto industry is slowly coming up to speed when compared with other industries. Programs like the ones run by Bugcrowd are increasingly common for companies in many different industries. Fiat Chrysler's initiative in creating a program to find security flaws is a step in the right direction for the auto industry.



Favorite Quote of the Month:

"To be yourself in a world that is constantly trying to make you something else is the greatest accomplishment."
--Ralph Waldo Emerson