IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

Attend Our FREE Cyber Security Webinar Coming Soon!

"5 Critical IT Security Protections EVERY Business Must Have In Place NOW To Avoid Cyber-Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

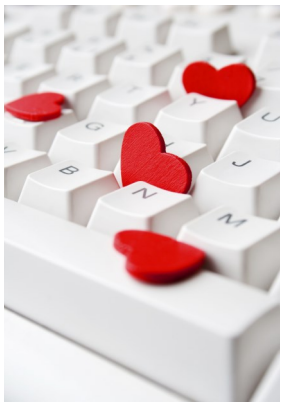
Details will be available soon at www.it-on-demand.com/Events

IT ONDEMAND
it-on-demand.com

February 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.



A Backup Plan You're Sure To Fall In Love With

In today's fast-paced, data-driven world, backups are mission critical to your company's survival and success.

Yet your data may be just one damaged drive, lost laptop, natural disaster, accidental deletion, malware attack, equipment failure, power spike or petty theft away from a profit-sucking, heartbreaking disaster.

So what measures must you take to keep your data safe, secure and where you need it, when you need it? While there's no one-size-fits-all-guns silver bullet, there are some general principles to be aware of.

Image-Based Backups

An image-based backup or "clone" serves like the spare tire for your car. If you get a flat, the spare will get you to a tire shop.

If the hard drive on any device in the network goes kablooey and its user is in a time crunch to complete a project, an image-based backup allows them to get right back to where they were. It saves all files, apps and settings that were on that device, exactly the way were at the time of the last backup. And generally, that means the user can get right back to work with no need to reconfigure everything all over again.

But, just as a spare tire isn't designed for long road trips, an image-based backup may not perform as well as the original drive. It may, for instance, take a little longer to access data from the server, slowing down user workflow.

An image-based backup will be useful only to the extent that it has backed up data recently. For servers, daily or even multiple backups per day are recommended.

Archive Backups

Archive backups don't replace image-based backups, but are an efficient way to reduce the size of these backups because they take less -frequently-used data off the main

Continued on page 2

computer or server.

You can't reboot from an archive, but if you've accidentally deleted a file, you can retrieve it from an archive. If any device on the network goes down, you can simply plug the external hard drive into another computer and regain access to the archived files.

"Should the absolute worst happen, the cloud backup image can be 'spun up'."

Cloud Backup

Backing up to the cloud can serve as an alternative to a rotating off-site backup and eliminates the human component of having to remember to rotate drives.

However, for complete protection, you'll want a cloud backup that makes a nightly copy of the image-based backup files. Should the absolute worst happen, the cloud backup image can be "spun up," allowing access to your applications and data using just about any computer or tablet.

Automated cloud backup systems offer a variety of feature sets. Some only back up files, while others back up entire image-based backups and can even spin them up. Select a system that's simple, continual, fast, secure, easy to restore from, inclusive of different devices and operating systems, cost-efficient and, most importantly, provides the kind of protection and redundancy you need for your operation to run even if things go south.

A Fail-Safe System

So, can you rest assured that your company's backup system is built to minimize downtime in the event of data loss or equipment failure?

If you're 100% certain you can answer yes, congratulations – you are one of the few! If not, NOW is the time to take action – rather than after you wish you had.

Not only is our ITOD Backup highly affordable, it continuously backs up your entire server – including open files – as frequently as every 15 minutes, so you'll never lose a whole day's work. Then, every night, it automatically backs up a snapshot of your entire server to an off-site military-grade data center where it's held safe and secure until you need it.

Don't put this off another minute! Contact us right now to claim your free Backup System Audit. Due to time constraints, we can only offer this to the first 5 *qualified businesses, so call now! Let us make sure your backup system never lets you down. We can fix broken computers but a broken heart is another thing entirely….

Call TODAY ((212) 235-0260!

**This offer available to qualified prospective clients with 10 or more computers and a minimum of 1 server in the New York City area.*

An *Ethical* Hacker?

In this world of cyber-attacks and growing cybercrimes, every businessman is a target for hackers. It's not just big businesses that are the focus of these cyber-attacks but also small and medium business that are often the victims. According to a recent report, one in five small and medium businesses has been targeted by hackers in the US. The total loss that the global economy has borne as a result of cybercrimes is estimated to be $575 billion.

In an environment like this, having a hacker on your side can protect you from a malicious attack or from becoming a victim of data breach. But it is crucial to remember that you don't just need a hacker, you need an ethical hacker.

There are two sides to hacking. On the one side sit black hat hackers who are the cybercriminals of the digital underworld. These are people who exploit individuals and attack business networks using malicious software. On the other side, there are the ethical hackers who are the good guys and whose aim is to protect businesses and governments from cyber-attacks of black hat hackers.

Continued on Page 3

An *Ethical* Hacker

(continued from page 2)

Ethical hackers are experts in computer and networking and their accountabilities are to identify cyber-threats to their company's computer systems and networks. They test various systems and find out weaknesses of each system using the same tools and techniques that are used by black hat hackers. They then prepare a document which contains actionable advice to fix all the vulnerabilities to improve the overall system.

Are you wondering where to find these good guys? You can simply hire an ethical hacker or can train any of your existing staff members. Hiring an ethical hacker can be a costly option; the average salary for a certified security professional in the US is $72,499 per year. But this amount is obviously less than the loss that you may have to bear as a result of malicious attacks. So whatever you decide, make sure to plan in advance to avoid delays and minimize losses.

Cyber Insurance & Financial Loss

In the world today, cyber security is becoming more and more important, as is cyber insurance. Cyber insurance is becoming as important as physical insurance – and probably even more so. However, there are a number of uncharted territories when it comes to cyber insurance, because it's still so new, compared to traditional insurance methods.

One example of this is in Texas, where a manufacturing firm in Houston is suing their provider of cyber insurance, claiming that they refused to cover a $480,000 loss following an e-mail scam. These email scams are becoming more and more common, and more and more dangerous.

At the heart of the issue were e-mails that claimed to be from Gean Stalcup, the CEO of Ameriforge Group Inc., which does business as AFGlobal Corp, to the firm's accounting director, Glen Wurm. Of course, the emails did not originate from the CEO, but rather from an imposter, but were convincing and led to the transfer of $480,000.

The insurance company, Federal Insurance Co., a division of Chubb Group, says that the claim was being denied because it didn't involve the forgery of a financial instrument, which was specifically required by the policy. They maintain that the email is in no way similar to the types of instruments in question, but this may be an antiquated way of thinking about financial instruments.

The case with AFGlobal Corp. is actually the second time this year that Federal Insurance/Chubb Corp have been taken to court over a financial loss as a result of electronic fraud taking place. The first case involved Medidata Solutions, Inc., and their suit was for $4.8 million, significantly more than the AFGlobal Corp. case.

In order to prevent these email scams and subsequent insurance issues and questions from taking place, the FBI is now urging businesses to adopt two-step, or two-factor authentication for their email services. They also suggest adding other communication channels to ensure that larger transactions are verified more securely, and of course to keep as much information private and away from social media as possible.

If you have any questions or you would like assistance in preventing email scams, please contact us at (212) 235-0260 or at sales@it-on-demand.com.

HOW HACKING THE INTERNET OF THINGS IS GETTING SCARY

As the calendar rolls on into 2016, more and more items are becoming connected to the Internet. And that means that for every item that is designed to make life easier through technology, there is an added risk that safety and security can be compromised. And let's just say that some of the examples you'll read about below are things that you wouldn't want to be left vulnerable to hackers.

Take cars, for example. Security researchers were able to attack a 2014 Jeep Cherokee through its on board Wi-Fi system and demonstrate that they could disable the transmission and brakes, which led to a safety recall of over 1.4 million vehicles. It was also proven that a Tesla Model S could be remotely started and driven off through hacking into the car's computer. Imagine paying that much money for a car and having someone drive off with it.

In another potentially dangerous situation, medical equipment that is Wi-Fi enabled can also be hacked. While in office, Dick Cheney's doctors had the Wi-Fi component disabled on his pacemaker, fearing that malicious hackers could cause him problems. Their fears were proven to be accurate when students later showed that they could hack similar components embedded into an iStan, a medical dummy used in research.

Hacks were not limited to these items, however, and affected everything from toys to guns. That's right, guns. Sniper rifles with Wi-Fi functionality through TrackingPoint, for example, were proven to be vulnerable. Everyone would certainly agree that guns are dangerous enough without the added problems associated with connectivity and security.

Clearly, there is a real requirement for companies to consider security a lot more heavily when building Wi-Fi connected devices, so that safety of customers and the general public can be ensured. The benefits of connectivity can be significant, so it would be much better to focus on those rather than the potential vulnerabilities.

For more information on security, please contact us at info@it-on-demand.com.

FREE Report: The Business Owner's Guide To IT Support Services And Fees from IT On Demand

You will learn:

- The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

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