This Issue:

Couple Jailed for Scamming More Than a Couple Dollars From the IRS

It all goes to show: don't mess with the IRS. The prison system has two new residents, after Anthony Alika, 42, and his wife Sonia, 27, were sentenced for filing fraudulent tax returns through the often-exploited "Get Transcript" site maintained by the Internal Revenue Service…

Read the Rest Online!
http://bit.ly/2bCr5UI

About Total Tech Care

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
totaltechcare.com

Outsourced IT is Specially Designed for Businesses that are Stretched Too Thin

Running a business is challenging, especially when it comes to juggling your assets and your IT budget. That's not even mentioning managing your workforce, or delegating tasks out to those who are qualified to perform them. While you're busy with all of these responsibilities, chances are that there will always be one task within your organization that's better handled by a professional: your IT management.

Some businesses have a hard time admitting that they don't have someone skilled enough to perform certain tasks. Plus, IT management and maintenance isn't something that you want an inexperienced worker handling. The truth about situations like this is that outsourcing is, in fact, a valid option, and one that shouldn't be dismissed - especially for small businesses. Sometimes small organizations don't have the time to deal with routine maintenance, while others have trouble attracting top talent. Both scenarios inevitably lead to technology that isn't cared for properly, and will eventually break down.

For this specific reason, outsourcing IT management and maintenance is one of the most valuable outsourced services that your business can implement. After all, you started your business for the purpose of providing a service you love, not to manage your technology solutions. If you want to focus on maximizing the quality of your services, you need someone watching your technology that can keep an eye on it 24/7. You just might find that your goals are all within arm's reach at long lost.

How a Single Data Breach Can Cost You Millions of Dollars

With all of the major data breaches making the news these days, it's not very surprising when you hear about a new one. However, what is surprising is just how much the average cost per breach has skyrocketed in recent years. The cost of data breaches is up 29 percent since 2013, which equates to roughly $4 million per data breach.

This sobering statistic is from a recent study by the Ponemon Institute and IBM Data. In it, 283 international companies that experienced a major data breach were examined. Here are some more findings from the study:

- The United States leads in terms of sheer overall cost of breaches by record value. The value per record is $223 on average. In total, the average cost of a data breach in the United States was roughly $7.01 million.
- Particular industries, like healthcare, education, and finance, have a higher value per record at $355, $246, and $221 respectively.
- 48 percent of all data breaches were the result of malicious intent, like hacking attacks and network infiltrations.
- Encryption and other security protocol decrease the costs of data breaches by up to $16/record.
- How quickly a company responded to the security breach had a positive impact on the

How a Single Data Breach Can Cost You Millions of Dollars

overall cost of the breach.

- There's a 26 percent chance that an enterprise will be hit by one or more data breaches of over 10,000 records within the next two years.

It's important to keep in mind that this study doesn't track the reputation fallout that a business experiences after news of their data breach goes public. This includes future customers choosing another business, as well as losing clientele. It's difficult to put a number to factors like these, but one thing's for sure; it will certainly be a major loss for any business that experiences a data breach. Reasons like these are why the average business that fails to recover their lost data after a breach will go out of business within one year of the incident.

Do you think that you've got what it takes to bounce back from a costly data breach? If you're unprepared and you don't have a proper data backup solution or your business continuity plan is inadequate, then you're in for a world of hurt.

Therefore, how much should you invest in a quality data backup solution? Before you make your decision, consider three more relevant points of interest from the study.

- **Cost per record from data theft due to malicious intent: $236.** This is data that's considered lost or stolen due to hacking attacks like ransomware or viruses. This category is virtually limitless with thousands of new strains of malware released on the Internet every single day.

- **Cost per record from data loss due to hardware failure: $213.** This is data that's lost due to system malfunction or hardware failure, like a server or workstation crashing unexpectedly. The good news; hardware failure is relatively easy to safeguard yourself against if you follow best practices and perform routine maintenances on all of your equipment.

- **Cost per record from data loss due to human error: $197.** This is data that's lost due to the actions of the user. It could be from intentional actions like sabotage by a disgruntled employee, but it's often accidental, like moving a file to the...

Read the Rest Online!
http://bit.ly/2bAQGx9

Every Business Can Improve Operations By Going Mobile

Computers have evolved from giant machines that take up an entire room, to compact devices that can fit in your pocket. In fact, today's smartphones are more powerful than computers built a decade ago, which is an impressive testament to the growth of computing. This mobility trend is a huge factor that every modern business must consider.

Your business needs to focus on mobility, and in doing so, you'll be able to take advantage of many benefits. Yet, this isn't to say that mobility doesn't come with its fair share of problems. As a business owner, it's your responsibility to determine whether or not you want to provide mobile devices to your staff. Just know: the benefits, when handled properly, can far outweigh the risks.

Mobile technology can be a powerful asset that can help your business bypass barriers associated with traditional office operations. Here are some of the prima-

ry reasons why your business needs to take mobile technology into account:

Improved Productivity
Since your team will have mobile devices, they can work and be productive anytime, anywhere. Your employees can check their email, organize their schedules, and communicate while out of the office. Mobile technology is valuable primarily because it gives your team the opportunity to work as they see fit, allowing them to get more work done, on or off the clock.

Workplace Versatility
Giving your team the choice of how and where to work can be empowering, and a mobile office provides the technology needed to accommodate this office design. Are there many places in the office where your team can set up shop for a few hours? This is helpful if your employees need a nice, quiet place to get something done, especially if your office is usually rife with chatter of all kinds. If your office environment is structured without a lot of room for collaboration, letting teams meet up in a conference

room or break area can empower employees to work together face-to-face.

Greater Efficiency
Improving mobility allows your business model to become more efficient, as you will also be designing your infrastructure with the intention of maximizing access to data and applications. This keeps your employees productive by guaranteeing that all critical assets will be available anytime, anywhere.

With all technology solutions that affect your network in some way, shape, or form, you need to make sure that it doesn't put your organization's data at risk. This is most important for mobile devices, which often do quite a bit of roaming. You don't want these devices to accidentally share information with the outside world or potentially threatening sources. Plus, if these devices are taking corporate data off the company network, and carrying them around...

Read the Rest Online!
http://bit.ly/2bARD8D

Outsourced IT is Specially Designed for Businesses that are Stretched Too Thin

One of the major benefits of managed IT services is the fact that your technology will be handled by a professional technician, rather than untrained employees. You don't want just anyone performing maintenance on your business's IT solutions.

Imagine what would happen if the person in charge of your IT were to mishandle or mismanage your technology - expensive downtime could ensue, and your budget could be burdened with frustrating repair costs and replacement fees. Of course, one of the most crippling parts of a hardware failure or

downtime event is the data that's lost when a server goes down. Unless you have support ready and on-hand to help you get through the incident as quickly as possible, an unexpected data loss incident could break your business badly enough that it can't recover.

When you outsource your IT to Total Tech Care, you can eliminate this uncertainty and ensure maximum uptime. Total Tech Care is ready to assist you with your technology at any time, and we make it our goal to minimize downtime and prevent technology difficulties altogether. Our managed IT services can be helpful even if you have an in-house

IT department. Chances are that they're bogged down with IT work, be it upgrading to better technology or applying routine maintenance. Our technicians can assist them and provide a second opinion when it's needed, as well as free up time by eliminating issues altogether.

Our technicians want to see you make the most of your business, and we'll use our expertise to limit the IT roadblocks you encounter so that you can focus on your goals. To learn more, give us a call at 866-348-2602.

Share this Article!
http://bit.ly/2bAPbzd

Why You Need to Have a Technology Replacement Plan

Computer hardware doesn't last forever. Sooner or later, you'll need to replace your equipment, or risk operations slowing to a crawl due to outdated equipment still in use. Do you have a timetable for replacing your equipment? Do you have a procedure in place to properly dispose of your old hardware? Every organization needs to think through the end-of-life and the afterlife of their computer hardware.

Plan Ahead to Replace Your Technology
Technology is no different than every other aspect of business in that it pays to have a plan. We call this an IT roadmap, which is a plan detailing what equipment needs to be replaced and at what time. A typical IT roadmap takes into account your company's technology needs over the next one, five, or even ten years.

The advantage to having an IT roadmap is that it's easy to come up with an IT budget so you can set aside money for the equipment you need, instead of running your equipment into the

ground and having to replace it when you least expect to.

Alternatively, you could put off replacing your old technology for as long as possible. Although, doing this won't save you money like you might think it would. Instead, the cost of having to make constant repairs, losing productivity due to downtime, and missing out on the performance-enhancing solutions of the latest technologies, will all eat into your budget and set your company back.

Be Sure to Wipe Your Old Hard Drives
If you're completely done with an old hard drive, then you'll want to be sure to wipe all of the data on the drive before disposing of it. Getting a hard drive wiped by a professional is your safest option, which is something Total Tech Care can handle for you. Also, it's important to remember that simply deleting your files won't cut it, seeing as your old files will still be able to be recovered.

Properly Dispose of Your Devices
A way to properly dispose of your old technology needs to be included in your plan. Electronic equipment is made up of components containing toxic chemicals that can leak into the environment.

Therefore, you'll want to properly handle and recycle your e-waste, a task which Total Tech Care is specially equipped to do. Additionally, be warned that if you simply throw your e-waste in the trash, you'll never know what will become of it. For example, your old hard drives could end up in the hands of hackers--which can lead to identity theft if the drive isn't properly wiped.

When it's time to think about new technology, you'll find that having a plan and a schedule to replace and refresh your company's technology will keep operations running smoothly and make these expenses more predictable.

Total Tech Care can assist you in coming up with an IT roadmap that prepares your business for all of your upcoming technology expenses for years to come, as well as properly disposing of your old equipment.

To get your very own IT roadmap customized to meet your company's needs, call us today at 866-348-2602.

Share this Article!
http://bit.ly/2bUT2sz

Study: 95% of All Cyber Attacks are Financially Motivated

Businesses need to take security into account and make it a priority. In fact, security is so important that Verizon has compiled a report of the various types of attacks and data breaches that occurred in the past year. This is Verizon's Data Breach Investigations Report, or DBIR, and it offers insights into how you can protect your business and secure your assets.

The DBIR has a method of outlining data breach types into nine separate categories. In particular, your business should focus on four of them. We'll provide you with a basic outline of what the threat entails, as well as how your organization can protect itself from them.

Crimeware
The DBIR reports that crimeware is one of the most common trends in the business environment, citing that 39 percent of all attacks in 2015 involved ransomware. The DBIR's definition of "crimeware" is quite large, and is used to refer to "any use of malware that doesn't fall into a more specific pattern." This lack of predictability makes crimeware rather dangerous, and only serves to show business owners just how many

different types of threats exist that fall into this category.

The DBIR recommends that all workstations and servers be patched and maintained at all times, and that organizations have backup and disaster recovery solutions put into place to prepare for the worst. Additionally, it's recommended that you monitor your systems for any changes to system configurations.

Web Application Attacks
E-commerce platforms are some of the most common targets, and it's simple to understand why. In the DBIR, 95 percent of all web application attacks had some sort of financial motivation. These attacks are caused by successful phishing attempts to steal credentials and infiltrate networks. Additionally, content management system data breaches have become quite common, with some aiming to infiltrate and repurpose sites as phishing centers.

The DBIR suggests using two-factor authentication, and to promptly update and patch software as needed.

Cyber Espionage
Some criminals will primarily target intellectual property. These cyber-espionage tactics will stick to your typical methods of network breaches and

utilize sophisticated means to meet their goals if simple tactics don't work. Therefore, many of these attempts to steal sensitive data can be undermined by basic protection, like firewalls and antivirus, but these solutions shouldn't be counted on to keep out more advanced threats.

Additionally, you need to take advantage of advanced security solutions, like remote monitoring and management, to ensure that your infrastructure's configurations aren't being tampered with, and implement a mobile device management solution to protect your organization's mobile data infrastructure.

Miscellaneous Errors
This category consists mostly of mistakes of all kinds that leads to compromised security. Verizon reports that around 40 percent of miscellaneous errors are caused by server issues, and about 26 percent are caused by simple employee mistakes, like sending a message filled with sensitive data to the wrong person.

The DBIR suggests that business owners or technology...

Read the Rest Online!
http://bit.ly/2bCpnTd
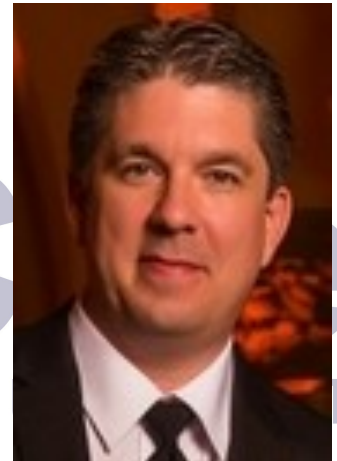
Robert St. Germain
CEO

Tech Fun Fact
NBC made more than 100 hours of 360-degree VR footage available to Samsung Gear VR users during the 2016 Olympics.

Total Tech Care

600 W Prospect RD
STE 2G
Oakland Park, Florida 33309
Voice: 866-348-2602

facebook.totaltechcare.com

twitter.com/totaltechcare

newsletter@totaltechcare.com

Visit us **online** at:
totaltechcare.com

WE ARE PUSHING TO GET THESE INSTALLED IN EVERY BUSINESS.

In case of IT EMERGENCY

BREAK GLASS FOR TECH