



This Issue:

Can a HIPAA Violation Result in Malpractice?

Why SMBs Need to Move Away from On-Premises Computing

How to Search the Web Without Typing

Don't Let Underutilized Servers Hold Your Business Back

Prepare for Employee Turnover with a Foolproof Exit Checklist

5 Signs Your Hard Drive is About to Fail

How to Search the Web Without Typing



How fast are you at finding the information you need using Google Search? In today's data-driven world, knowing how to effectively use Google is actually a marketable skill. Did you know that there are ways in Google Chrome to search for what you need that take less time...

Read the Rest Online!
<http://bit.ly/1N81rW0>



About Total Networks

Locally owned and operated since 1986, Total Networks is the only firm in Arizona to receive CompTIA's Security Trustmark validating the firm's adherence to best practices for information security. Services include IT support, security & compliance assessments, document management, backup & disaster recovery and IT planning/CIO services.

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

Can a HIPAA Violation Result in Malpractice?



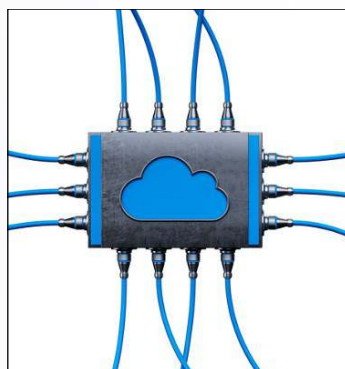
The answer increasingly appears to be yes. Government action and fines are clear consequences of failure to comply with HIPAA and Federal & State privacy laws, but private party action has also been successfully litigated using HIPAA, despite the fact that there are no direct allowances for private cause of action in the law.

In 2013, an Indiana jury awarded \$1.44 million to a customer as a result of a violation of the Health Insurance Portability and Accountability Act (HIPAA) by a Walgreens pharmacist. The pharmacist's husband had an affair with a woman, who was a customer of Walgreens, that resulted in a child. The woman (now ex-girlfriend) was seeking child support. The pharmacist suspected her husband's ex-girlfriend of giving her husband a sexually transmitted disease and accessed her confidential medical history. The husband then sent a text message to the ex-girlfriend referencing her confidential medical information in an attempt to blackmail her to stop seeking child support. The suit by the ex-girlfriend accused Walgreens of negligence in its supervision of the pharmacist.

The company argued that the pharmacist's illegal acts weren't authorized by the company and the pharmacist admitted that she was aware of the strict privacy policy and that she knew she was violating it. Walgreens still lost and the damages were split 80 percent company responsibility, 20 percent pharmacist responsibility.

(Continued on page 2)

Why SMBs Need to Move Away from On-Premises Computing



Most small and medium-sized businesses aren't new to IT. For the past 15 years or so, SMBs have been attempting to keep up with their larger competitors through the implementation of technology systems. They've instituted computing systems from servers to workstations to mobile devices, peripheral technologies like fax machines and copiers, "state of the art" networking technology, and all other sorts of tech, just trying to keep a leg up on their competition.

The problem for these businesses is that every cent they spend on managing physical technology won't necessarily produce much of a return on their substantial investments as they need to actively maintain the technology in order for it to work properly. This has left many companies hemorrhaging money by just trying to compete. If your business is still hosting all of its own IT infrastructure, it may be time for you to consider moving your IT out of your office.

While hosting your own IT has its benefits, for the small or medium-sized business it may bring more expense than it's worth. In moving your IT infrastructure to the cloud or to a collocated data center, you may see a dramatic cost savings, or at the very least a shift in way your organization pays for its crucial IT systems. The cloud, in particular, offers many SMBs a very attractive value proposition: Receive a scalable IT infrastructure, hosted in a secure data center, with proactive maintenance, billed monthly as an operational cost.

(Continued on page 3)

Can a HIPAA violation result in malpractice?

(Continued from page 1)

"I did not sue Walgreens for violating HIPAA, I sued Walgreens for negligence, but I used HIPAA to prove that Walgreens was negligent. Similarly, I did not sue the pharmacist for violating HIPAA, I sued her for professional malpractice, but I used HIPAA to prove that what she did fell below the commonly-accepted standard for privacy protection." – Neal F. Eggerson, Attorney

Privacy breaches are increasing and the laws around them have evolved substantially. There are detailed requirements mandated by the law which are being used not only to levy fines, but to support private party lawsuits. You and your clients may or may not be subject to HIPAA, but it would be in the best interest of every business to act as if you are. You may eventually be held ac-

countable to this standard. You are almost certainly subject to other privacy laws and lawsuits where HIPAA may be the yardstick against which your actions or inactions are measured. This is all separate and in addition to your ethical responsibilities.

Complying with the law here is much harder than most people assume. Please consider this recent quote from the FBI: "The biggest vulnerability was the perception that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise," FBI Memo, April 17, 2014.

Top 10 Security & Compliance Guidelines For Your Firm:

1. Assess risks in maintaining privacy and security, then update and/or establish policies and safeguards to

ensure that everybody who touches your data (including any subcontractors and their subcontractors) will keep information confidential and your environment secure.

2. Get assurances from employees and contractors in writing that they will follow adequate procedures. Please note, that simply getting a Business Associate Agreement (as required by HIPAA) is not sufficient – be sure vendors actually understand and meet the requirements.
3. Designate a single individual of appropriate authority who is ultimately responsible for your firm's security & privacy.
4. Ensure that your policies and procedures support the concept...



Read the Rest Online!
<http://bit.ly/1UJIQ11>

Don't Let Underutilized Servers Hold Your Business Back



How messy is your server room? When was the last time you took note of how many machines

you have, and what each of them are contributing to your business's goals? If either of these situations sound familiar, it might be time to take a closer look at your technology and examine how you can improve operations. One of the best ways you can do so is by eliminating unnecessary costs from unused and underutilized servers.

According to Processor magazine, a solid 30 percent of all powered-on servers aren't working to their maximum potential. In fact, support servers average only about a 12 to 18 percent utilization rate. This means that there are a ton of servers out there that are costing businesses money on unnecessary expenses. It's basically like wasted money, especially

when you consider that many businesses use several dedicated servers for email, file hosting, and more. The reasoning behind this is that the servers can function independently from one-another, but the reality of the situation is that servers use a ton of energy; energy that's wasted if not taken advantage of properly.

The Benefits

There are many benefits to consolidating your server infrastructure. Performing a close analysis of your organization's server infrastructure is imperative to cutting unnecessary costs and optimizing your bottom line. Here are some of the great ways your company can benefit from elimination of underutilized or unused servers.

Dramatic decrease in energy costs.

With less machines online at all times, you can save money on operational costs, maintenance, and energy. Servers eat up a ton of electricity, so it's natural that you do whatever you can to limit how much you use. Furthermore, maintenance is significantly less expen-

sive if you only have one machine that needs updating, rather than four.

Simplified computing infrastructure.

Instead of having all of your technology spread across multiple pieces of hardware, you only need a minimal number of machines operating at all times. This makes it much easier to maintain and manage all of your mission-critical technology from one central location.

More physical space for activities and other technology. Regardless of how many servers you're able to eliminate, you'll be saving valuable space that can be used for other, more productive things. For instance, you can use the freed space for storage. You'll finally be able to get rid of that fax machine that's been collecting dust on your desk.

If you're unsure how many of your servers are underutilized, or if you need help identifying where you can shave off some IT costs, Total Networks...



Read the Rest Online!
<http://bit.ly/1N80PzH>

Why SMBs Need to Move Away from On-Premises Computing

(Continued from page 1)

For some SMBs it may not make sense to move your entire IT infrastructure to the cloud. In fact, some organizations, just like the idea that they are in complete control of their IT, or more specifically, their data. If your organization needs to adhere to often-complicated IT regulations, or if you just want the freedom to have control over your company's IT management, you still don't have to host your computing infrastructure on your premises. By purchasing server space in a colocation facility, you can set up a private cloud platform that provides your business with all the benefits of cloud

computing (like cost savings) without having to relinquish complete control over your crucial IT systems.

The professional IT consultants at Total Networks can assess your situation and find a solution that works for your needs. We have a complete technical understanding of cloud computing systems, and how they fit into a SMB's IT strategy. Our technicians can also assist your company in the proliferation of new computing systems to provide your organization with powerful functions such as communications (like VoIP and email), productivity application deploy-

ment, and even cloud-based security solutions.

It's hard to ignore the benefits that moving all or some of your company's computing infrastructure to the cloud can bring. For an organization that is looking to free up capital, or simply to increase mobility, cloud computing can be of real benefit. Call us today at (602)412-5025 to learn how moving your IT out of your office can really benefit your company.



Share this Article!
<http://bit.ly/1N80v3X>

Prepare for Employee Turnover with a Foolproof Exit Checklist



One of the most dreaded situations in the modern office is the resignation of experi-

enced talent. It's always sad to say goodbye to a colleague and friend... under the right circumstances. What would happen if an angry employee left your company and used their privileges to wreck havoc on your IT?

If you've taken proper precautions to ensure your former employees can't sabotage your network and steal your data, you're golden. However, this simply isn't the case with a lot of companies, mainly because they don't count on their former coworkers backstabbing them. This isn't the entire issue at hand. Even if a former employee doesn't intentionally take data from your business upon resignation, they could get hacked in the future, leaving sensitive data exposed. The best way to avoid employees walking off with corporate data is to take proper precautions, starting before they walk out your door.

Perform an Exit Interview

Besides getting the opportunity to discuss why they're leaving the company, conducting an exit interview is a good time to iron out details that shouldn't be left unchecked. This is a good time to talk about what accounts the exiting employee has access to, what devices they've borrowed from the company, important documents they might possess, and how to get in touch with them after they leave.

Take Back Any Company-Provided Devices

Once you've identified that your employee is indeed leaving the organization, you need to collect the devices they've borrowed from the company, like laptops, mobile devices, and storage devices like USBs or hard drives. This helps to ensure that you don't let corporate data slip through the cracks. Collecting these devices ensures that you're the one in control of your data, which mitigates the chance of the data being compromised, both voluntarily and involuntarily.

Promptly Change Email Passwords and Remote Access Accounts

For obvious reasons, you need to revoke access to their email accounts. This helps to prevent them from accessing infor-

mation that they shouldn't have access to following their departure from your company.

Change All Relevant Passwords

You never know just how many passwords an employee might walk out of your company with, especially if they're saved in their personal mobile device's browser cache or they use a password manager. This is why it's important to make sure that all passwords are changed. If an employee were to get hacked, or decide that they don't agree with their dismissal from your organization, it could put your data at risk of being compromised.

Wipe Mobile Devices

If your network can dish out security policies to mobile devices that gain access to company email, you will want to make sure you remotely wipe your accounts. This is something you would have needed to set up prior, but it prevents the user from walking away with their email in their pocket. Even if your former employee isn't a threat, if the device is lost or stolen it could...



Read the Rest Online!
<http://bit.ly/1N81bGp>

5 Signs Your Hard Drive is About to Fail



We all know the fleeting moment of fear as a computer slows to a grinding halt, taking forever to perform the most basic of tasks. At the same time, we also know the relief of when you find out there's nothing wrong with your PC. Still, what if that relief never comes? What if you're dealing with one of the most dangerous computer issues of all: a hard drive crash?

The risks of a hard drive crash are similar to any other type of hardware failure. If your drive is used for storing data, it can lead to data loss. If you're not using a quality backup and disaster recovery solution, you can bet that it'll be difficult, if not impossible, to restore your infrastructure to its former glory.

Frequent Computer Crashes

If there's anything you've learned from reading our newsletter, it should be that computer crashes are never a good sign of anything. Ever. The reason it crashes is because it's incapable of locating or accessing important files that are crucial to the operation of the system, and it's a

clear sign that something is not right with your machine.

Disappearing Data

Another sign that your hard drive is failing is that data isn't where it's supposed to be. You'll probably notice this when you try to access a mission-critical application, but the software can't load because a file is missing or some other complication. Unless someone is behind the scenes messing with the location of data, your hard drive is probably just about done.

Out-of-the-Ordinary Noises

You know there's something wrong when you hear strange grinding noises coming from your hard drive, but really, if anything at all sounds out of the ordinary, you probably have a big problem on your hands. If you start hearing noises coming from your hard drive that aren't normal, you should shut down your PC and contact a professional for further consultation. These typically sound like a clicking noise coming from inside your PC. The last thing you want is your hard drive crashing on you while you're in the middle of an important project.

Your Computer Doesn't Recognize the Drive
If your PC doesn't

acknowledge the hard drive, it's a clear sign that there's something wrong. You can test whether this is an issue with the hard drive by testing it in another PC, but you should do so only if there's a professional on-hand to guide you through the process.

Painfully Slow Processing Speed

If it takes your PC ages to open a basic folder or file, this means that it's having trouble locating and accessing it. Basically, if there's ever a problem opening files, you can assume that there's something wrong with the hard drive.

The idea behind these tips is to identify problems with your technology before they cause irreparable damage to your systems and, more importantly, your business. Unexpected problems can cause downtime, which is one expense your organization can't afford to deal with. By taking these proactive approaches, you can make sure you spot a problem before it harms your business's productivity.

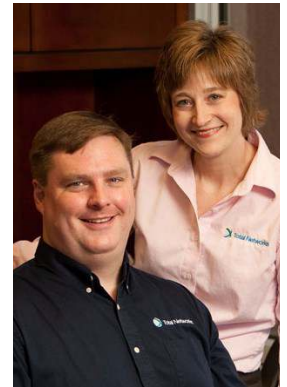
What Total Networks offers is a more comprehensive and...



Read the Rest Online!
<http://bit.ly/1N809KJ>

We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

If you would like to receive an electronic version of our newsletter please email skinsey@totalnetworks.com



Dave and Stephanie
Kinsey
Owners



Bill Fox
VP, Customer Service

Total Networks

4201 North 24th Street
Suite 230
Phoenix, AZ 85016
Voice: 602-412-5025

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



info@totalnetworks.com



[facebook.totalnetworks.com](https://facebook.com/totalnetworks.com)



[linkedin.totalnetworks.com](https://linkedin.com/company/totalnetworks.com)



[twitter.totalnetworks.com](https://twitter.com/totalnetworks.com)

