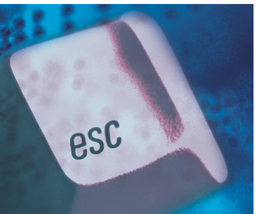
MAY 2015

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"



The Smarter Path

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

- Willie Kerns, SmartPath Technologies

What's Inside:

(270)238-8997

Memorial Day 2015

The "National Moment of Remembrance" resolution was passed on Dec 2000 which asks that at 3 p.m. local time, for all Americans "To voluntarily and informally observe in their own way a Moment of remembrance and respect, pausing from whatever they are doing for a moment of silence or listening to 'Taps."

Why Do I Need To Be Concerned about Security?

All antivirus does not come with any kind of guarantee. You should view antivirus software as a flu shot. Even though you take the flu shot, you have a chance to get the flu, and the doctor doesn't guarantee you won't. Your risk is greatly reduced, but it's still there. Same with antivirus software - It's unlikely you'll get infected, but it does happen. Out of close to 5000 computers under management, all with antivirus software, you will have 15-20 virus PC's per year.

One risk that business have is that they may need to be mitigated is their firewall. The firewall (sometimes known as a router) is the box that stands between the public internet and your private network. It keeps the bad guys out, and it does this through various methods - one of which is inspecting all traffic coming into the network from the internet to make sure it was requested by a computer inside. Firewall technology has come a LONG way in the past five years since you've been hearing more and more about things like the Sony hack, the Target hack, etc. Most new firewalls now come with a subscription, much like your antivirus software, and that subscription keeps the firewall's intelligence up to date against the latest threats being developed. Newer firewalls also contain a level of antivirus protection so that all traffic coming in from the internet gets inspected for viruses before it's allowed through to your computer. In combination with antivirus software on the computers, this added layer of antivirus and antimalware protection provides the equivalent to a double dose of the flu shot. Newer firewalls have a host of other features too, including tracking and reporting by user, as well as blocking of websites (like workplace violence, gambling, and other sites known to cause cyber threats).

The other key in mitigating cyber threats in 2015 is a big part of what we proactively manage for our ITWorks clients—it's making sure that every computer, server, phone, and tablet that is in use or contains company data (including e-mail on phones/tablets) is updated and patched daily. Hacking groups who want your data are constantly finding ways to exploit Windows, Office, Adobe, iPhones, Droids, etc. When they figure out a new way to attack computers and devices, software vendors will typically immediately release an update, or patch for the software. You see this in the form of Windows update that show up to be installed down by the clock, as well as Java, Adobe updates that typically also show up by the clock or when you open Acrobat Reader, Macromedia Flash updates that sometimes display on websites, and notifications of software updates on phones and tablets. It's very very important that all updates get installed as soon as they are released—for our managed ITWorks clients, we run updates on all machines daily automatically. A huge amount of hacks in 2014 came as a result of having unpatched/up-updated Adobe Reader. It's so much more vital now than it used to be to keep all systems updated on a VERY regular consistent schedule. It can be a little hairy handling these on your own because there are a number of fraudulent messages that can pop up that say you need updates that are really designed to infect you, and it's also hairy trying to handle making sure s happen on EVERYONE's computer.

Your insurance company may offer a cyber-threat rider of additional policy. We advise all clients to seriously consider adding this coverage. The average cost of getting a virus for an unmanaged client (meaning a client who isn't part of our ITWorks monthly managed services) in 2014 ended up being $2323.51. This includes time to clean/sanitize the PC, the cost of labor for not being able to work while infected including payroll burden, about 10 other factors. It's expensive to have problems. Incidents of data theft, especially of payroll data, add up a lot higher a lot faster. If that data is lost— say because you don't use online backup and backup to a USB hard drive, and that hard drive gets stolen of lost, you are required by law to pay for credit monitoring for all employees, pay for the cost of cleaning up any identity theft, pay for legal expenses for those employees, etc. That's one situation where using online backup provides a bit more of a safeguard than taking data offsite manually.

Call Us For Your Cyber Security Audit Today!

The Lighter Side…

The First Computer Bug Was Actually A Moth?

- The first actual computer "bug" was a dead moth stuck in a Harvard Mark II computer in 1947.
- Big banks don't process checks and debit card charges to your account in the order they're received, but instead use a computer program that selects the biggest amounts first and charges them against your account, emptying your account faster and resulting in more overdraft fees (profit).
- In September 1956, IBM launched the 305 RAMAC, the first "SUPER" computer with a hard disk drive (HDD). The HDD weighed over a ton and stored 5 MB of data.
- A computer as powerful as the human brain would be able to perform about 38 thousand trillion operations per second and hold about 3,584 terabytes of memory.
- The first entirely computer-generated movie sequence in cinema history was the Genesis Device demonstration video in *Star Trek II: The Wrath of Khan*. The studio that made the scene would later become Pixar.
- CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."
- MIT has developed computer software that can identify and distinguish a real smile from a smile of frustration.

"Hey, no problem! I've always felt that a little sales resistance is a healthy thing!"

Not Just For Medical Offices

"Business Associates are on the hook for HIPAA violations."

A prospective client asked for our help after receiving a HIPAA audit letter from the Office of Civil Rights (OCR). OCR sent the client the letter after one of the client's business associates experienced a HIPAA related breach. I won't give any additional information on the client, the business associate or details of the security incident. The only additional information is that the prospective client was a covered entity. **Note: the breach was NOT caused by the covered entity but by one of their business associates.** As you can see any business that deals with medical records can be subject to OCR audits. Whether you are a medical office, lawyers office for a medical office, CPA for a medical office, business supply office for a medical office, you can be affected by a breach to any one of these business. Even SmartPath Technologies has to abide by the rules of HIPAA.

Regardless of who caused the breach, OCR was looking directly at the covered entity. The sum of the information requested is clearly looking to see if the covered entity was complying with HIPAA regulations and more specifically the HIPAA Security Rule. 20 days is not a lot of time to produce this information. If the covered entity did not already have the Book of Evidence it would have been very difficult to create and compile the information in the requested timeframe.

When we perform a risk assessment for a client we always make it clear that it is critical to not only perform or implement security safeguards but you MUST have documentation that you can produce that shows you are performing or have implemented the safeguard.

Many covered entities don't feel the risk of an audit is real. They point to the lack of HIPAA enforcement and have a false sense of security. This case shows that CEs and BAs need to not focus on random audits but understand that they can be audited if one of their subcontractors (in the case of a CE or BA) or one of their clients (in the case of BA) have a security breach. And not being able to produce the above requested items by OCR may lead to OCR finding the organization in willful neglect of HIPAA regulations.

Breaches can be very costly for a medical organization. Penalties have ranged from $ 50,000 to $ 4.8 million. Notification costs, legal fees, and lost revenue add up fast. HIPAA has been used as a Standard of Care in malpractice suits and in 2012 a jury awarded $ 1.4 million for malpractice when a patient's information was released without authorization.

Shiny New Gadget of the Month

SaneBox

Have you ever felt overwhelmed or even drowning with the number of emails in your inbox?

Then SaneBox could be your answer. This month's gadget is a cloud-based software application that helps you manage your email. SaneBox analyzes your email behavior on all your devices. Then, based on which emails you let slide and which ones you open right away, SaneBox creates rules about sorting your email for you. The result? Your inbox only has emails you need to attend to now. All other emails go to your SaneLater folder. You can drag and drop emails from that folder to your inbox, and from then on, those emails will display in your inbox.

SaneBox keeps you focused on high-priority emails. There's nothing to download. There are additional productivity features to manage tasks, your calendar, and your attachments. And the SaneBlackhole is the fastest way to unsubscribe from emails. See www.sanebox.com.

The Benefits of Creating a "Book of Evidence"

Creating a Book of Evidence on an organization's compliance with HIPAA privacy, security and breach rule is not difficult, only takes a couple of weeks, and helps an organization not be overwhelmed if it's selected by the HHS Office of Civil Rights for a random HIPAA Audit.

A good example of what should be in a Book of Evidence (BOE):

A BOE will show proof of updating the risk analysis with introduction of business changes or new information systems; an incident response system that is quick, effective and a repeatable process; that all employees have received timely HIPAA training with their scores available; that appropriate authentication controls are in place; and can even shoe the receipts for security technology buys such as encrypted hard drives.

At SmartPath Technologies we have been thinking about a Book of Evidence for years. Our HIPAA Compliance Portal can be your Book of Evidence. If you were to get audited by OCR, you can give them a user id to access your HIPAA Compliance Portal. All of your "evidence" of HIPAA compliance is in one place.

1. **HIPAA Security Policies and Procedures**

All your HIPAA privacy and security policies are stored in our Compliance Portal. All employees have access to the Compliance Portal and access to your policies and procedures. You can even upload OHSA policies, your employee handbook and HR policies and procedures that employees can access online.

2. **HIPAA Risk Assessment, Business Associate Agreements, Disaster Recovery Procedures**

The Compliance Portal contains your Risk Assessment reports, tracks Business Associates and allows you to upload Business Associate Agreements, Disaster Recovery Plans and also allows you to upload other contracts or documents. Only administrators have access to this section. Employees do not have access to this sensitive information

3. **HIPAA Security Training**

All training is done online via our Compliance Portal. The administrator training report is accessible only to the administrator(s). The reports shows each of your employees, when they took the HIPAA security training and what grade they received on their HIPAA compliance quiz. There is no better way to prove you have provided HIPAA security training to your employees! Employees also have access to our HIPAA Security Tips and Reminders which helps show that you are in compliance with the requirement to provide periodic security reminders to employees.

4. **HIPAA Security Incidents, Server Room Access, Track ePHI Removed and Received**

The Compliance Portal allows you to track HIPAA security incidents and what your response was to each of those incidents. You can also track who has accessed the server room, and ePHI that has left your organization (i.e. USB drives) and any ePHI that has been received by your organization (i.e. DVD drives with x-rays or ultrasound images given to you by patients).

As you can see, the HIPAA Secure Now! Compliance Portal can be your "Book of Evidence" in the event OCR audits your organization.

Happy Mothers Day
Happy Mothers Day
to all the Mothers out there
It's definitely not always the easiest job
!but it is the most rewarding

SmartPath
TECHNOLOGIES
Business Computer and Network Specialists

78 Ash St
Calvert City, KY 42029
(270) 238-8997

Ever flip a switch and wish you could be HIPAA Compliant?

Create a culture of compliance.

SmartPath Technologies' SmartHIPAA program provides a way for any medical office, practitioner, or covered entity to achieve HIPAA compliance very quickly and without making you pull what hair you have left out of your head. Our SmartHIPAA program certifies your entire staff is trained, your policies and procedures are created or edited, and that your office meets the Meaningful Use Core Objectives. HIPAA compliance can happen in between 15-90 days. It's easy – it's totally done-for-you AND has a $100k financial guarantee if you incur fines from a HIPAA violation or data breach.

Join us on May 21st, 2015 for a totally FREE webinar that will quickly and easily – no tech talk – explain the law that is HIPAA, the Office of Civil Rights (OCR)'s role in levying HIPAA fines and conducting random audits, what's needed for YOUR practice to comply, how breaches happen and what they can cost, how to prevent those breaches, and what's required to meet the requirement for meaningful use.

If you have ever wished you could flip a switch and become HIPAA compliant, great news – you CAN! One provider or an entire hospital can all become compliant – guaranteed.

Register today at www.smartpathtech.com/smarthipaa-webinar.

PS: Did you know if your business works within any medical offices, that YOU are required to be HIPAA compliant to or face fines in the event of a data breach. Most people don't – but if you ever are in physical proximity to paper records or work within the practices' software programs, you have to be certified as HIPAA compliant, too!