TECHNOLOGY TIMES

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

Breaches Come To Those Who Wait

Breaches have come to many organizations this year, from Target, to Michaels, to Neiman Marcus. But this year of breath-taking data breaches climaxed with the largest one of all, when Home Depot announced that it had breached 56 million credit card numbers on September 8. As details of the breach have begun to emerge, it is clear that the company moved too slowly to tighten security, and it allegedly cut corners on security measures that could have detected the breach much earlier.

A New York Times story based on interviews with former Home Depot employees details a "record of missteps." Security managers raised alarms at the company as far back as 2008, but the company continued to use outdated software and inadequate security policies for years. The company did not take definitive action until April 2014, when it finally began to encrypt credit card data stored on its systems, and encryption was not rolled out across all stores until early September. But hackers had already planted malicious software on Home Depot's networks months before. By the time Home Depot secured its network, millions of credit card records had already been stolen.

It's like putting in a bank vault just as the robbers ride off with all your gold. Six long years passed while Home Depot executives dithered, and the company's luck finally ran out.

Breaches are rarely caused by technological failures. They are almost always caused by cultural failures. *That is, the people in charge fail to take security seriously until it's too late.*

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

- Rick Johnston, Information Management Systems

October 2014

Fargo, ND

Inside This Issue...

THAT? THAT'S A STORE, HON. IN THE OLDEN DAYS PEOPLE WOULD BUY THINGS IN STORES INSTEAD OF ONLINE.

In the year 2030.

Former employees allege that Home Depot was not performing the network scans required by the credit card industry. Every organization that takes credit or debit cards is subject to the Payment Card Industry Data Security Standard (PCI DSS), and PCI DSS requires merchants like Home Depot to perform network scans at least once a quarter. Such scans can detect unusual activity, such as data transmissions to strange servers. But Home Depot apparently relied on a loophole in the PCI DSS requirements, which offer an exception for store networks that are separate from the larger corporate network.

This attitude toward compliance is backwards. Building strong security is not a matter of checking a box, or satisfying some regulation. Rather, the point is to prevent breaches. If the rules may allow you to avoid implementing a security measure for some technical reason, will cutting that corner leave you exposed to breaches? The real danger is always the breach. Home Depot may have narrowly satisfied industry requirements, but the breach will still mean several billion dollars of losses for the company.

Meanwhile, thousands of breaches occur each month, in organizations that are too small to grab headlines. PCI DSS compliance seems to be following the same trajectory as HIPAA. That is, the largest companies have been implementing compliance programs, but smaller organizations may not have implemented any real network security at all.

If you mention PCI DSS to most healthcare providers, you'll get nothing but a blank stare in response. They simply do not know that anyone who takes payment cards must follow PCI DSS. Fortunately, PCI DSS mirrors HIPAA in many response, so compliance with one goes a long way toward compliance with the other. But how many healthcare organizations have proper policies on credit card security?

I've never met a provider who got into medicine because of their passion for data security. But the breach will come to you anyway. When security managers went to Home Depot executives with their concerns, they were allegedly told, "We sell hammers." But they collected millions of credit card records to sell those hammers, and they failed to protect that data. Now, Home Depot will have to sell many more hammers to pay for the breach their indifference caused, and it will be years before they regain the trust of customers.

This article was written by Brian Johnson with 4Medapproved

October is National Cyber Security Month. Contact us at 701-364-2718 or info@imsnetworking.com, to create your custom Cyber Security plan for $199 ($400 value!). Please read our insert "**Ten Cyber Security Tips for Small Businesses**".

If you are on our Managed Services Contract you do not need to worry! You are completely protected against Cyber Security Threats.

* If you are not on our Managed Services Contract please look on the backside of the "**Ten Cyber Security Tips for Small Businesses**" insert to select a plan that fits your needs.

Shiny New Gadget Of The Month:

Neo Grab

It's amazing how quickly our technology evolves. When the GPS devices for cars first came out, could we imagine that our phones would quickly take over that job? More and more, we see people using their phones to navigate in the car, but holding on to the phone while driving can be dangerous. The result has been a series of phone-holding apparatuses that cling to the car in the same manner our GPS's did.

Finally there is one that is not only functional, but also beautiful, and it battles one of the biggest problems with car phone holders. The NEO GRAB allows you to mount and remove your phone one-handed, and it works for you in ways unimaginable, not only in the car, but also in the kitchen, office, bathroom, bedroom, garage, at work, etc. With its extreme suction cup, the NEO GRAB is easy to attach to any smooth, non-porous surface, like glass, drywall, plastic, wood and metal.

The NEO GRAB fits devices with LCD screens up to 6 inches and can be used for smartphones, mini-tablets and even your GPS device. Needless to say, this is the ideal accessory for any smartphone user.

It comes in 5 colors and can be purchased for $34.99 from www.SkyMall.com.

Don't Make These 3 Mistakes With Your Next Office Move

Moving is always a pain in the rump, but it doesn't have to be a horrific, expensive experience. The No. 1 lament from someone who's experienced a "bad" move is "I didn't know I needed to…" followed closely by "I completely forgot that…" In other words, *it's what you don't do that makes the move a disaster*. To make your move easy and effortless, here are the 3 most common mistakes you want to avoid:

Mistake #1 — Trying To Save Money By Using Your Employees To Move Your Computer Network

Don't ask your staff to disconnect, move and reconnect computers, phones and other devices just to save a few bucks. You'll frustrate them and end up with phones ringing at the wrong extension, lost cables and PCs that get dropped. You don't want to let your movers do this job either; they may be great at moving furniture, but a network is a lot more sophisticated and sensitive. *Be smart and hire an IT pro to pack and move your network.*

Mistake #2 — Not Hiring The RIGHT IT Firm To Move Your Network

While we're on the topic, make sure you know what to look for when outsourcing the move. A few things to look for would include references from other clients, proof of insurance (get them to fax you a copy), a service-level guarantee limiting the amount of time you are down and a professional, organized approach to quoting the move. A real pro will insist on visiting your current location as well as your new location to conduct a detailed site survey. NEVER hire anyone who wants to quote moving your network over the phone.

Mistake #3 — Not Giving Your Phone, Internet And Cable Vendors Enough Advance Notice

80% of unexpected communications blackouts and cost overruns on network moves are caused by failure to properly plan voice, data and electrical installation *in advance*. Just because the prior tenant had computers and telephones is no guarantee that the cabling is suitable for *your* phones and *your* computer network. Allow at least 6 weeks for Internet and telephone connections to be installed. Advance planning will help you avoid emergency rush fees or Band-Aid fixes to make things work.

Call us before your next office move and get an Office Move Checklist, Site Survey and Network Plan for only $99!

---

*Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY!***

Overtype in Word 2013

Chances are high that you spend a good amount of time editing or compiling Microsoft Word documents. Regardless of what you are editing, there will come a time when you are working on a file and the words are replaced as you type new ones. This could cause some problems, especially if you are unsure how to turn this feature off.

Words two editing styles

Every version of Word used in businesses these days has the same two editing styles or modes:

1. **Insert mode:** This is the default editing mode where words are inserted where the blinking cursor is placed. All text that comes to the right of the cursor will be moved to the right with newly typed text coming before it
2. **Overtype mode:** This mode replaces text to the right of the blinking cursor. So when you type new text any existing text to the immediate right will be replaced with new letters

While the vast majority of users prefer to use insert mode, overtype mode can be useful when editing documents and replacing words, or rewording paragraphs and keeping track of what needs to be written.

Turning overtype on and off

On some older versions of Word, and on some computers, overtype mode is already enabled, and simply hitting Insert on the number pad of your keyboard will turn it on. You will know overtype is active by looking at the status bar at the bottom of your document. The words OVR should be visible in bold letters.

If you don't see a status bar, try clicking on File> Preferences > View. Once in the View window, scroll down to the Windows section and tick Status Bar. Finally press Ok and the bar should pop up at the bottom of the window.

Managing overtype

If you find that overtype cannot be activated, or have received a document where it is already activated and can't figure out how to turn it off, you can manage overtype by:

1. Right clicking on the status bar at the bottom of the document
2. Clicking on Overtype to add it to the status bar
3. Clicking on OVR in the status bar to turn it on or off

You can also activate or deactivate overtype by:

1. Clicking on File followed by Options
2. Selecting Advanced
3. Scrolling down to Editing options
4. Ticking or unticking User overtype mode

If you untick User overtype mode you will disable the feature, meaning you won't be able to hit Insert to switch between the two editing modes.

This entry was posted in Cloud Office 365, General Articles C and tagged 2014Aug26_Office 365_C, Microsoft word editing feature, Microsoft Word editing styles, Microsoft Word overtype, Microsoft Word turn overtype off, Microsoft Word turn overtype on, QS_3. http://www.techadvisory.org/2014/08/overtype-in-word-2013/

The Lighter Side:
Halloween Graveyard Story from Vienna

Chris Cross, a tourist in Vienna, is going past Vienna's Zentralfriedhof churchyard on October 31st. Suddenly he hears some music. No one is around, so he starts searching for the source. Chris finally locates the origin and finds it is coming from a grave with a headstone that reads: Ludwig van Beethoven, 1770-1827. Then he realizes that the music is the Ninth Symphony and it is being played backward! Puzzled, he leaves the graveyard and persuades Tim Burr, a friend, to return with him.

By the time they arrive back at the grave, the music has changed. This time it is the Seventh Symphony, but like the previous piece, it is being played backward. Curious, the men agree to consult a music scholar. When they return with the expert, the Fifth Symphony is playing, again backward. The expert notices that the symphonies are being played in the reverse order in which they were composed, the 9th, then the 7th, then the 5th. By the next day, the word has spread and a throng has gathered around the grave. They are all listening to the Second Symphony being played backward.

Just then the graveyard's caretaker ambles up to the group. Someone in the crowd asks him if he has an explanation for the music.

"Oh, it's nothing to worry about," says the caretaker. "He's just decomposing!"