TECHNOLOGY TIMES

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

By Computer Networks of Roanoke, Inc.

Serving Roanoke and surrounding areas since 2006

Volume 8, Issue 12 December 2015

"As a business owner, 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!"

Hank Wagner, Owner/Founder
Computer Networks of Roanoke

IT Guru, Published Author, and Trusted Advisor to Medical Practice Administrators and Business Owners

Loaf of Bread

Some of you might not know me from a loaf of bread, so I am going to take a couple of minutes to bring you up to speed:

1994-1996	**Medic Computer Systems** Medic Software Trainer
1996-1998	**Misys Healthcare (purchased Medic)** Medic/Misys Field Engineer
1998-2005	**Misys Health Care Field Engineer** Branch Manager Adv. Implementation Ambassador
2005 -2015	**Computer Networks of Roanoke, Inc.** Co-owner Healthcare Information Technology Computer Support HIPAA Risk Analyses Disaster Recovery

See Loaf Page 2

INSIDE THIS ISSUE

3 Ways To Instantly Open Up Your Computer Network To A Cyber Attack

Welcome to the brave new world of cyber-warfare.

Gone are the days when software patches were just for nifty little feature add-ons or updates.

Today, a software update notice could mean your whole computer network is suddenly at risk. Dangers include data theft, crippling malware attacks and mischief you may not discover for months, or even years…

As with graffiti on your garage door, if you don't pay attention and clamp down on bad behavior, your problems have likely just begun…

And, like those who hire a professional security firm to keep thieves out of the warehouse, thousands of CEOs and business owners are now waking up to the fact that it's absolutely imperative to hire a pro when it comes to securing your data network.

Here's why you need a professional handling this:

#1: Not patching fast enough - speed is of the essence.
"If you didn't update to version 7.32 within seven hours, you should assume you've been hacked." That's what software maker Drupal told millions of its customers around the world last year. It's just one example of what can happen if you don't respond with lightning speed.

See Cyber Attack on Page 3

Loaf continued from Page 1

So, if you do the math, I have been in Healthcare Information Technology for the past 18 years, 11 of them as Owner of my own firm.

If you take a peek around at some of the other IT firms in our area, you will see that they do not specialize in Healthcare IT, that their Owners/Founders do not have a background in Healthcare IT, and consequently do not always understand the challenges presented in Healthcare.

Specializing in a particular vertical market is the same thing that many of your Physicians have done. Your Doctors have picked a particular field of study and become an expert in that field. So have we.

Looking further into those other IT companies who are "playing" in this space, those firms are your Business Associates (BAs) under HIPAA because they are exposed to Protected Health Information (PHI) when they are on your network or because they store your backup data offsite.

Being the BA of a Medical Practice carries some pretty important duties, the first of which is that **all BAs must be HIPAA compliant**. That means that they are required by Federal Law to have completed a Security Risk Analysis (SRA) just as you are; they are required to develop Polices and Procedures for dealing with PHI, just as you are; and that they are required to train their staff on HIPAA, just as you are.

- Has your Information Technology firm completed the necessary steps to become HIPAA compliant?
- If so, can they offer proof of that compliance?
- If not, why are they in Healthcare IT?

This is a serious concern. The Office for Civil Rights (OCR) plans to do more audits this year. And they have made it known that they are going to ask you for a list of your Business Associates (BAs) when they audit you and then OCR is going to audit the BAs as well. ☸

Hank Wagner
757-333-3299 x232
hank.wagner@computernetworksinc.com

Ransomware On The Rise

This is some really BAD stuff and it is spreading.

Cryptowall is a Trojan Horse/Ransomware that encrypts files on the compromised computer. It then requires the user to pay a hefty ransom to have the files decrypted. The threat typically arrives on the affected computer through **spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware.**

The only way to guarantee recovery is to have a Backup and Disaster Recovery solution in place that backs up every hour and then ships your files offsite.

RULE #1
Do not open any email attachment unless you are expecting it and unless you know the sender! The people in your organization are going to be the weakest link.

Here is an email that I had to send today to one of our clients:

Dear XXXXX:
To protect your business,, we have installed a high end firewall, with:
- ***ICSA-certified gateway anti-virus and anti-spyware protection***

Combine network-based anti-malware with a cloud database of over 12 million malware signatures for deep security protection against advanced modern threats.
- ***Cutting-edge IPS technology***

Protect against worms, Trojans, software vulnerabilities and other intrusions by scanning all network traffic for malicious or anomalous patterns, thereby increasing network reliability and performance.
- ***Application intelligence and control***

Help administrators control and manage both business and non-business related applications with granular, application-specific policies providing application classification and policy enforcement.
- ***Content filtering***

Address safety, security and productivity concerns with controls to enforce Internet use policies and block access to harmful and unproductive web content.

*There are **no** products on the market that can protect you from a hacker that writes malicious code this morning and sends it out via spam emails this afternoon. These trojans, viruses, and malware are called "zero-day" viruses because today is day zero of their life. The antivirus and security Vendors know nothing about them, so there are no defenses against them until they are reported to the antivirus Vendors.*

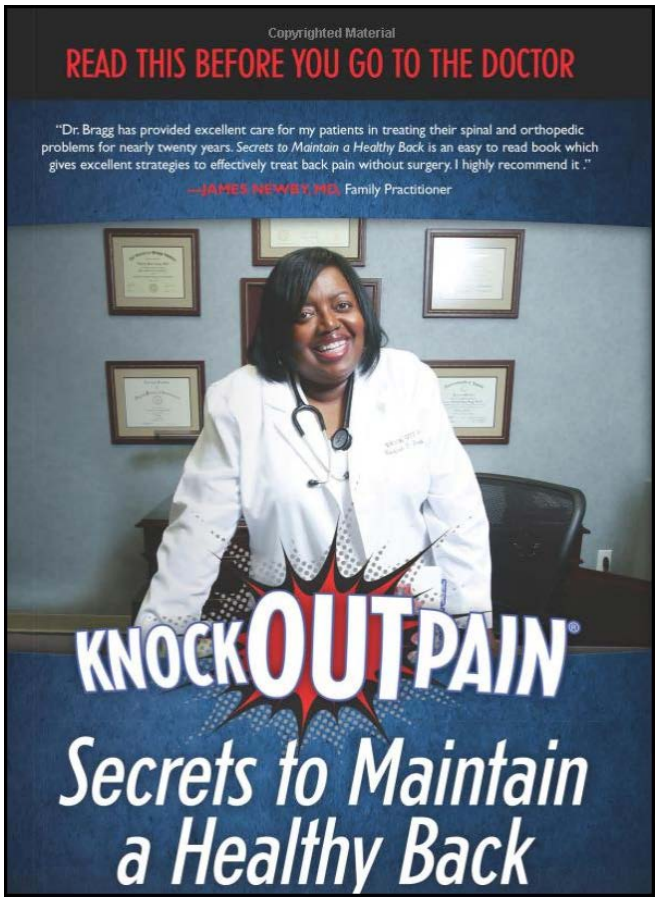
You became a victim when one of your Physician/Owners checked his personal email on a Corporate device, in violation of your HIPAA Policies and Procedures, then clicked on an attachment that he did not know what it was, thereby infecting your network with a "zero-day" Cryptowall.

Additionally, I sent you an educational newsletter two weeks prior to this event that was very clear in how to identify and explain to staff the importance of not engaging in this exact, risky behavior when checking emails. I am at a loss as to what other steps you would like us to take other than:

- *install the best equipment for the job*
- *monitor the equipment for intrusions*
- *educate your staff on what not to do*

By way of example, if you open your door at 2:00am this morning and a robber is standing there, you invite him in, and he in fact robs you, how would one defend against that? ☸

Congratulations Dr. Bragg



We would like to take a minute to congratulate Dr. Winnifred Bragg on publishing her new book about treatment of back pain. 80% of us will have back pain at some point in our life by age 55. Back pain often comes at inopportune times. It destroys vacations, work, outings, holidays and special occasions.

Dr. Bragg has treated thousands of patients with back pain over the past 20 years. She has written this book to educate people about the symptoms and causes of low back pain and to offer her proven strategies for pain relief.

You can pick up a copy from the folks at Amazon: http://www.amazon.com/KnockOutPain%C2%AE-Secrets-Maintain-Healthy-Back/dp/0997008202/ref=sr_1_1 ☸

See Cyber Attack on Page 3

Once a security breach has been identified, hackers rush in. On "Day Zero," cyber-crooks around the world go after at-risk targets. You've got to be quick to patch the gap, or else you risk a system compromise.

Unless you have the time, knowledge, experience and skill set to respond instantly, you are far better off leaving this to a professional IT firm you can trust.

#2: Thinking you are too small - it's not just the big boys they're after.
Sure, the top news stories are about the attacks on companies like Target, Home Depot and Sony…

Yet your business is just as vulnerable, if not more so.
Chances are, you simply do not have the resources that giant corporations have to manage a data disaster. The statistics bearing this out are shocking: more than 60% of small businesses close their doors following a serious data breach.

The threat is not confined to giant corporations. Small and medium businesses are being attacked every day, and, unfortunately, your business is no exception.

#3: Not hiring a good IT firm- dealing with data breaches requires specialized knowledge, skill and experience.
Here are just a few of the things a competent data guardian must be able to do to effectively protect your systems:

Review documentation and monitor forums. Sometimes your software vendor doesn't tell the whole story. It's critical to check online forums and other communities to see if anyone else is having issues with the new patch before jumping in with both feet.

Know when to apply a patch immediately and when to wait. Typically, somewhere around 95% of patches work hassle-free. The trick is to spot the 5% that don't — *before* installing them. ☸

Hank Wagner
757-333-3299 x232
hank.wagner@computernetworksinc.com

The Lighter Side:

Joe was at the country club for his weekly round of golf. He began his round with an eagle on the first hole and a birdie on the second.

On the third hole he had just scored his first ever hole-in-one when his cell phone rang... It was the doctor notifying him that his wife had just been in an accident and was in critical condition and in ICU.

The man told the doctor to inform his wife where he was and that he'd be there as soon as possible. As he hung up he realized he was leaving what was shaping up to be his best ever round of golf.

He decided to get in a couple of more holes before heading to the hospital. He ended up playing all eighteen, finishing his round shooting a personal best 61, shattering the club record by five strokes and beating his previous best game by more than 10. He was jubilant....

Then he remembered his wife. Feeling guilty he dashed to the hospital. He saw the doctor in the corridor and asked about his wife's condition.

The doctor glared at him and shouted, "You went ahead and finished your round of golf didn't you! I hope you're proud of yourself!"

"While you were out for the past four hours enjoying yourself at the country club your wife has been languishing in the ICU! It's just as well you went ahead and finished that round because it will be more than likely your last! For the rest of her life she will require round the clock care and you will be her care giver! She will need IV's; you will have to change her colostomy bag every 3 hours; she will have to be spoon fed 3 times a day and don't forget the hygiene care."

The man broke down and sobbed.

The doctor chuckled and said, "I'm just screwing with you. She's passed away.

What'd you shoot?" ❁

No Explanation Needed

By Steven Nardone

- **$6 billion:** The cost associated with cyber attacks, attributed specifically to healthcare.
- **94 percent** of healthcare organizations have indicated they've had some type of a breach.
- Healthcare sustains about **two and half times the cost** for each record that is lost.
- Healthcare information is about **10 times** more valuable than any other data on the black market: "There's tremendous incentive for breaches to take place."
- **68 percent** of breaches that occurred have been in healthcare.
- **175.5 million** records have been lost.
- **317 million** new pieces of malware last year.
- **1 million** new threats every single day.
- **$4.5 billion** was lost in 2014.

Happy Holidays to all

We want to thank all of our Clients for their continuing support and commitment over that past year. We appreciate your faith and trust in us and we want you to know that we take the protection of your business personally and seriously.

For those of you who are not Clients yet, fell free to give us a shout to talk about how we can help create a problem-free network at your office. ❁