TECHNOLOGY TIMES

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

By Computer Networks of Roanoke, Inc.

Serving Roanoke, Rocky Mount, Salem, Lynchburg, Danville and Martinsville since 2006

Volume 8, Issue 2 **February 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, Former Medic/Misys/Allscripts Engineer and Trusted Advisor to Medical Practice Administrators

Server 2003 and Exchange 2003 To Die In 2015

See Server 2003/Exchange 2003 Page 2

INSIDE THIS ISSUE

1	Die In 2015
1	BUDR
2	Predictable Results
3	Meaningful Use News
3	Security Quick Hits
4	The Lighter Side

BACKUP AND DISASTER RECOVERY (BUDR)

Is your business protected from data loss? That's a pretty simple question. The answer ought to be pretty simple, too. Yes or no, right?

Well, maybe it is or maybe it's not. I guess it really depends on your definition of "protected".

If you consider "protected" as:

- having a daily **tape** backup
- being OK with waiting a couple of days to have your server repaired, or in the event of something catastrophic, waiting to have it replaced
- being OK waiting another day or so after that in order to load your data back on the server from those tapes
- taking the tapes offsite, so that you have one from a day or two ago from which to restore
- being OK with losing a day or two of data that your staff will have to recreate once the tape is restored
- not minding the business owner jumping up and down because you don't have the computers for a couple of days while all this is happening

-then you are protected. (Umm, you have been testing those tapes by periodically restoring the backups, right?)

On the other hand, if this is NOT what you had in mind about recovery from a disaster, then we probably ought to chat about our affordable, recover and go back to work within an hour, Disaster Recovery solution.

We put a small server at your office, backup your equipment to our equipment hourly, move your latest backup offsite nightly, have the ability to go back 1 hour in time and mount a copy of your server so that you can return to work ASAP.

Interested in hearing more? It does not cost you a dime to talk. Call us…757-333-3299 x232. ❖

Server 2003/Exchange 2003 continued from Page 1

What does end of support mean for you? After July 14, Microsoft will no longer issue security updates for any version of **Windows Server 2003**. If you are still running Windows Server 2003, you need to take steps now to plan and execute a migration strategy to protect your infrastructure. By migrating to Windows Server 2012 R2, Microsoft Azure or Office 365, you can achieve concrete benefits, including improved performance, reduced maintenance requirements, and increased agility and speed of response to the business.

Support for **Microsoft Exchange Server 2003** will soon be coming to an end. Are you ready? Each product that Microsoft releases has a lifecycle that determines how long we maintain and support the product. Exchange 2003 mainstream support is over. And, Exchange 2003 extended support ends on April 8th, 2014. In the meantime, don't panic. It's time to start planning your upgrade to the latest version of Exchange. ❖

Call us today at: 757-333-3299
Or, you can email us at:

hank.wagner@computernetworksinc.com

Predictable Results For a Predictable Fee

We do it all…HIPAA Risk Analysis, Backup and Disaster Recovery (required for HIPAA Compliance), Network Administration, Help Desk, Hardware Sales/Service, Hardware Refreshes/Installs, Consulting.

We are looking for a select number of new clients in the healthcare, legal, accounting and professional services markets. If you are dissatisfied with the level of service you are getting from your current Information Technology Vendor, pick up the phone, call me, Hank Wagner, at 757-333-3299 x232, or email me: hank.wagner@computernetworksinc.com and let's chat a bit about your needs. ❖

Meaningful Use Changes Coming

Healthcare IT News

It's official. The federal government has announced its willingness to ease up on meaningful use reporting requirements for the EHR Incentive Programs.
In efforts to "reduce the reporting burden" for eligible providers and hospitals, the Centers for Medicare & Medicaid Services has proposed a new rulemaking, expected spring 2015, that could shorten the 2015 MU reporting period to 90 days – something that many CIOs and health IT organizations have been strongly pushing for in recent months.
In addition to a 90-day reporting period, CMS also is considering the following changes to the Meaningful Use Program:
• Realigning hospital reporting periods to the calendar year to allow eligible hospitals more time to incorporate 2014 Edition software into their workflows and to better align with other quality programs
• Modifying other aspects of the programs to match long-term goals, reduce complexity and lessen providers' reporting burden.
The new rule "would be intended to be responsive to provider concerns about software implementation, information exchange readiness, and other related concerns in 2015," wrote Patrick Conway, MD, chief medical officer at CMS, in a Jan. 29 blog post announcing the agency's decision. "It would also be intended to propose changes reflective of developments in the industry and progress toward program goals achieved since the program began in 2011." ❖

Security Quick Hits

By the SANS Institute

--BMW Fixes Software Flaw that Affected 2.2 Million Cars (February 2, 2015)

BMW has remotely fixed a vulnerability in software used in some of its cars that could have been exploited to open the vehicles' doors using a mobile phone. The software, ConnectedDrive, uses an on-board SIM card and manages door locks, air conditioning, and traffic updates, but not brakes or steering. The patch encrypts data from the car with HTTPS.

--Adobe Will Patch Third Flash Vulnerability in Two Weeks (February 2, 2015)
Adobe has released an advisory about yet another flaw in Flash Player.
This is the third flaw discovered in Flash in less than three weeks.

--Apple iOS Updated to Version 8.1.3 (February 2, 2015)
Apple has released an update for its mobile device operating system. iOS 8.1.3 fixes 33 security issues.

--Verizon to Let Cookies Crumble (January 30 & February 1, 2015)
Verizon says it will let its customers opt out of having their online activity on smartphones and tablets tracked with so-called "unkillable" tracking identifier, also known as super cookies. Verizon began injecting unique identifying headers (UIDH) into all HTTP requests made to sites over its network. These cookies survived cookie deletions from browsers because they are inserted by carriers.

--ZeroAccess Botnet Operating Again (January 29 & 30, 2015)
The ZeroAccess botnet, which was taken down in a cooperative effort between Microsoft and international law enforcement more than a year ago, appears to be active once again. The peer-to-peer botnet, also known as Sirefef, is being used in click fraud schemes. It has infected approximately 55,000 computers, far fewer that the nearly two million computers that had been infected prior to the December 2013 takedown. ❖

All This Postage Is Expensive

I have been writing and mailing this newsletter going on 8 years now. Our mailing list is growing, but, some of you reading this are not doing business with us. I am OK with that, because we are not the right firm for everyone. However, it is getting more costly to print and mail this newsletter, in color, every month.
So, over the next few months we will be calling those of you who are not customers to give you a chance to receive the newsletter via email, so that we can continue to provide you with this information at a reduced cost to us. Please be so kind as to take this call, so that we do not drop you from our list. ❖

Call us today at: 757-333-3299 x232
Or, you can email us at:
hank.wagner@computernetworksinc.com

Ready to hire a new IT firm? Give us a call. It doesn't cost anything to talk. 757-333-3299 x232.

Trend Micro Security Predictions for 2015 and Beyond

1 | More cybercriminals will turn to darknets and exclusive-access forums to share and sell crimeware.
2 | Increased cyber activity will translate to better, bigger, and more successful hacking tools and attempts.
3 | Exploit kits will target Android, as mobile vulnerabilities play a bigger role in device infection.
4 | Targeted attacks will become as prevalent as Cyber-crime.
5 | New mobile payment methods will introduce new threats.
6 | We will see more attempts to exploit vulnerabilities in open source apps.
7 | Technological diversity will save IoE/IoT devices from mass attacks but the same won't be true for the data they process.
8 | More severe online banking and other financially motivated threats will surface. ❖

The Lighter Side:

13 ADULT TRUTHS

1. Sometimes I'll look down at my watch 3 consecutive times; and still not know what time it is.

2. Nothing sucks more than that moment during an argument when you realize you're wrong.

3. I totally take back all those times I didn't want to nap when I was younger.

4. There is great need for a sarcasm font.

5. How the hell are you supposed to fold a fitted sheet?

6. Was learning cursive really necessary?

7. Map Quest really needs to start their directions on # 5. I'm pretty sure I know how to get out of my neighborhood.

8. Obituaries would be a lot more interesting if they told you how the person died.

9. I can't remember the last time I wasn't at least kind-of tired.

10. Bad decisions make good stories.

11. You never know when it will strike, but there comes a moment at work when you know that you just aren't going to do anything productive for the rest of the day.

12. Can we all just agree to ignore whatever comes after Blu-Ray? I don't want to have to restart my collection...again.

13. I'm always slightly terrified when I exit out of a Word document and it asks me if I want to save any changes to my ten-page technical report that I swear I did not make any changes to.

People, Wake Up And Smell the Coffee

Businesses need to pull their head out of the sand and take a look around. If you have not developed a **culture of security** at your business, then you are already behind the power curve. If you employees are running rampant around the Internet using YOUR computer network, you are putting YOUR business at risk for data loss, intrusion or being compromised by hackers. This stuff is real. And, just like you lock your car every night, and lock your home's doors every night, you need to insure that your computer network is locked.

Folks, it is past time to begin thinking about cybercriminals and thieves and how they might steal your customer information. How would YOUR customers react if you called them up and told them that they were the victim of identity theft because you didn't buy a good enough firewall, or because you didn't update your antivirus, or because you didn't see fit to encrypt your emails with that contained their personal information. Think Sony Pictures, Target, Home Depot, PF Chang, Michael's Arts and Crafts…just on a smaller scale. Do you want to be next?

And I do not buy the "We are too small of a target" argument. Cyber attacks on small businesses continue to rise. And small businesses are vulnerable targets. That's because small businesses are the path of least resistance for cyber criminals, according to a recent report by Internet security provider Symantec.

Symantec reports that companies with fewer than 250 employees were the focus of 31 percent of all cyber attacks in 2012. That's a dramatic jump from 18 percent in 2011.

If you think your business is too small to be an attractive target for cyber criminals or you don't have anything worth stealing, think again: The 2012 Data Breach Investigations Study by Verizon shows that in 855 data breaches they examined, 71 percent occurred in businesses with fewer than 100 employees. Verizon's 2013 Report shows attacks on small business increased in record numbers as well.

You have to start protecting the computer part of your business just like the physical part of your business. Put up multiple layers of defense, then keep a low profile. Most criminals will move on to an easier, less hardened target if they encounter formidable defenses. ❖

Call or email us if you want to chat.
Hank Wagner 757-333-3299 x232
hank.wagner@computernetworksinc.com