



BUSINESS TECHNOLOGY QUARTERLY

Brought to you by *The Technology Group, LLC*

(860) 524-4400 www.TheTechnologyGroup.com

\$19 Billion for Healthcare IT as Part of Stimulus Act

By Mark Torello



Congress is expected to approve \$17 billion dollars for incentives plus \$2 billion to jump start healthcare IT adoption as part of the Stimulus package. Provisions in the bill include funding for health information technology initiatives such as electronic medical health records (EMR) by providers that serve Medicare and Medicaid patients. It would provide bonus payments from \$44,000 to \$64,000 for physicians and up to \$11 million for hospitals that use electronic health records.

The bill supports Medicare and Medicaid incentive

(Continued on page 6)

What's New in QuickBooks® 2009?

By Linda Swanson

QuickBooks' new Company Snapshot, available in the 2009 versions of QuickBooks Pro, Premier, and Enterprise, offers a real-time view of company information such as income and expense trends, account balances, customers who owe money, vendors to pay, and reminders all on one screen. A transaction can even be entered from the snapshot screen by clicking

(Continued on page 3)

**Technology Group, LLC
Earns Microsoft Gold
Certification**



Full story on page 6

Reduce IT Costs – 10 Money Saving Tips!

By Ian Apruzzese

Everywhere you turn, the news about the economy is bad, really bad. The demand to reduce costs has never been higher. Growth in these economic times is going to be hard to come by, but by applying some simple cost cutting measures, you can keep your IT operations running and be poised to reap the benefits on the upswing of our economic downturn.

1. Assemble a cost cutting team

Assemble a group to identify ways to reduce spending. Choose your best thinkers to assist in this project. Put a focus on cooperative collaboration and avoid laying blame toward past wasteful activities. The goal here is to create a budget-focused think tank.

2. Outsourcing IT

Partnering with a technology service firm can give you access to specialized skills and best practices, while reducing IT project and support costs. Organizations that have a quality technology partner can

(Continued on page 2)

INSIDE

For Non-Profits Only: MIP Hosted Solution

pg. 3

Security News

pg. 4

In-House News

pg. 6

Server Room Best Practices

pg. 6

Autoplay: Security Threat

pg. 7

CCPA Seminar for Non-Profits

pg. 8

Cost Cutting

(Continued from page 1)

have better control over their IT budgets by having predictable maintenance and project costs. It is possible to realize savings of 50% or more by utilizing outsourced IT professionals, rather than attempting to hire and train in house.

3. Go green

Reducing your organization's carbon foot print can have a real impact on the bottom line. With current energy efficient processors, LCD displays, and energy-smart power protection, you can see a significant reduction in energy use from the server level to the desktop. Power usage can be reduced as much as 40%, simply by removing old CRT monitors and replacing them with energy efficient LCD displays.

4. Virtualization

By refreshing existing servers and deploying them in a virtual environment hosted on a single quad core server, energy consumption can be reduced by 80%. And, this can be accomplished while improving performance, reducing server footprint, and increasing system uptime. The ROI on virtualization can be as short as 18 months.

5. Reduce network/telecom costs

Renegotiate your data network and telecom contracts. This can be a delicate process, but persistent negotiation can be

successful in reducing these recurrent costs. Vendors are keenly aware of our economic woes, and are acting to retain customers. Be aware that, in most cases, you will need to extend a current contract, but the extension can be worthwhile. If you are nearing the end of a current contract, shop around, there could be better deals out there.

6. Standardize and document to improve efficiency

Standardization of hardware and software throughout the organization reduces complexity, training and support costs. These benefits are augmented with accurate documentation of network systems and software applications. This process can reduce IT support costs and improve systems management by creating a blueprint for the network, infrastructure, and software. Standardization and documentation also reduce the impact of employee turnover and training for new IT workers.

7. Resist "future proofing" the network

The urge to spend extra dollars to ensure that the network architecture does not have to be redone for your next major rollout can be strong. When looking at replacing aging equipment or implementing necessary new hardware, look for solutions that fit immediate needs, rather than spending extra IT dollars on hardware or software for "future" projects that might not be funded for 12-24 months or more.

8. Use more of your existing technology


Are you sure that you're getting the most out of your current IT investments? If not, it would be wise to contract with a technology integrator that can assess your network and provide guidance on how you can get more out of your existing IT investments.

9. Don't throw away your old equipment - sell it on eBay

You can't just toss environmentally harmful IT equipment in the dumpster and computer disposal services charge as much as \$100 per unit. EBay them! Selling hardware on eBay comes with its own set of hassles, but making \$20 per monitor sure beats paying a recycler hundreds of dollars to haul them away!

10. Don't stop saving

Continual improvement and cost reductions will have a significant impact on your bottom line. The savings are out there for the taking. Leave no stone unturned. This recession... depression... economic slow down... or whatever you want to call it, will come to an end. The question is: What will your business look like at the other end of the tunnel? Be smart, spend smarter, and you'll be able to emerge on the other side, ready to hit the ground running.

For help evaluating your IT infrastructure for cost savings opportunities, contact The Technology Group, LLC. 

Quickbooks

(Continued from page 1)

on “pay bills” or “receive payments.”

INTUIT STATEMENT WRITER

The Intuit Statement Writer, available with Premier 2009 and Enterprise, is an easy to learn tool used to generate custom financial reports. This replaces the Financial Statement Designer in previous versions. Templates (balance sheet, income statement, and budget-to-actual) are available to customize as needed. Intuit Statement Writer works with Excel 2003 and above. You have all the functionality of Excel, such as formatting, charting, and formulas. Any accounts can be rolled-up without modifying the QuickBooks chart of account structure. In a matter of minutes you can create reports to meet your needs.

MULTI-CURRENCY TRACKING

QuickBooks Pro 2009, Premier 2009 and Enterprise 9.0 now support all global currencies, making it easier for you track foreign sales, purchases, banking, and credit card transactions. Setup is easy – just click the currency you wish to use from a list and make it active. You can download the latest exchange rate quickly and easily.

LISTS IMPROVEMENTS

The search feature in lists, previously only available with Enterprise, is now available in Pro and Premier. Simply type the search criteria in the “find” box and click on the looking glass. To search within a specific field, such as City or State, click the looking glass first, enter the search criteria, and then select the search field.

For Non-Profits Only MIP Hosted Solution

Sage MIP chose nGenX in December, 2008 to be the hosted solution for MIP Fund Accounting. nGenX is a leading nationwide provider of on-demand software solutions with headquarters in Overland Park, Kansas. The company hosts and manages more than 400 line-of-business applications in a virtual on-demand environment from its SAS 70, Type II certified data centers. All on-demand services from nGenX include data backup, disaster recovery, remote access and 24-hour customer support. nGenX also offers managed server and relocation services.

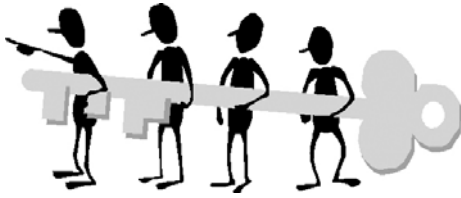
Managed Hosting for Sage MIP software through nGenX includes the following:

- **Storage for applications** and data in a SAS-70, type II certified data center
- **Coordination with Sage MIP** for updates and support
- **Migration of user data** to nGenX servers, or deployment of software in their data center
- **Professional monitoring and maintenance**
- Daily, weekly, monthly and annual data **back ups**
- **End user technical support**, 24 x 7 x 365
- **Remote access** for home and traveling users
- **Virus protection** (on the nGenX network)

Contact The Technology Group to explore MIP Hosted Solutions.



As Certified QuickBooks Professional Advisors, The Technology Group, LLC can provide installation, configuration and implementation assistance.



SECURITY NEWS

(Courtesy of the Sans Institute unless otherwise noted)

Five Sentenced in Connection with Attempted Cyber Bank Theft

Five men have been sentenced to between three and eight years in jail for their roles in a scheme in which they attempted to steal GBP 229 million (US \$324 million) from the London branch of Japan's Sumitomo Mitsui Bank. Hugh Rodley, the apparent mastermind of the plot, received an eight-year sentence. Kevin O'Donoghue, a bank guard who allowed members of the cyber crime gang in after hours, received four years and four months; Jan Van Osselaer and Gilles Poelvoorde, who entered the building and planted devices to steal information, were sentenced to three-and-a-half and four years, respectively; and David Nash received a three-year sentence. After harvesting information from the bank computers, members of the group returned and attempted to make transfers of various sums to accounts set up in Spain, Turkey, Dubai and other countries around the world. The transfers failed because the would-be thieves filled out transfer forms incorrectly.

Judge Orders Man to Decrypt Drive

A federal judge has ruled that a man suspected of having child pornography on an encrypted drive on his laptop computer is not protected by the Fifth Amendment. US District Judge William Sessions ruled that Sebastien Boucher surrendered those rights when he

allowed his laptop to be searched the first time, and ordered Boucher to provide the court with an unencrypted version of the drive in question. The ruling reverses an earlier decision in which a judge ruled that Boucher was protected from incriminating himself under the Fifth Amendment. The original request from the US department of Justice had been to make Boucher surrender his encryption passwords; the appeal asked only that he decrypt the drive in view of the grand jury. Boucher's laptop was searched in December 2006 while crossing the border into the US from Canada. Agents claim to have seen the offending content, and then shut down the computer. When they tried to access the images after Boucher's arrest, they were unable to because of his PGP program.

Surveys Find Employees Stealing Data to Help Economic Prospects

A Cyber-Ark Software survey of 600 office workers in London, New York and Amsterdam found that theft of proprietary information is on the rise; many of the thieves are insiders concerned about losing their jobs. A study from Symark found that 40 percent of companies do not know whether employees' user accounts remain active after the employee no longer works for the company. According to UK Director of Cyber-Ark Mark Fullbrook, cyber criminals feel they are reaping benefits from the current economic crisis. Reductions in budgets have led to increased outsourcing and decreased focus on security.

Sensitive Presidential Helicopter Info Leaked Through P2P Program

A Maryland defense contractor appears to have leaked information through a peer-to-peer (P2P) file sharing program about the helicopter currently used by US President Barack Obama. The

information, including "blueprints and an avionics package for Marine One" were detected at an IP address in Tehran by a company that monitors P2P networks. There is speculation that an employee at the company downloaded the P2P program without understanding how it could compromise the security of information on the company's network.

Koobface Variant Spreading Through Social Networking Sites

A variant of the Koobface worm has been spreading through social networking communities such as Facebook and MySpace. The malware spreads by sending messages that appear to come from friends, asking them to click on a link to watch a video. When the users reach the malicious website, they receive a message that they need to install an Adobe Flash plug-in to view the clip properly. If they agree to install the plug-in, a Trojan horse program is installed on the computer instead, giving attackers control over the machine. This Koobface variant also sends out invitations to watch the bogus clip to contacts through the social networking account. In addition, two rogue Facebook applications have been attempting to steal user data.

Telecoms face possible fines for Failure to Prove Adequate Customer Data Protection

The US Federal Communications Commission (FCC) could fine more than 600 telephone companies and voice over Internet protocol (VoIP) providers for failing to provide adequate proof that they are taking steps to safeguard customer data. The FCC requires the companies to submit annual certification that they have employed measures to guard customer data against exposure through pretexting; they must also prove that they have kept records

of all instances in which they have provided customer data to a third party and of all customer complaints about information disclosure. Last year, 600 such operators either filed no reports or filed noncompliant reports. The proposed fines range from \$10,000 for filing noncompliant forms, to \$20,000 for not filing at all.

Adobe Reader Security Hole Leaves Systems Open for Outsider Control

(Source: Adobe Systems Inc.)

A critical vulnerability has been identified in Adobe Reader 9 and Acrobat 9 and earlier versions. This vulnerability would cause the application to crash and could potentially allow an attacker to take control of the affected system. There are reports that this issue is being exploited. Adobe recommends users of Adobe Reader and Acrobat 9 update to Adobe Reader 9.1 and Acrobat 9.1. Adobe expected to have updates available for Adobe Reader 7 and 8, and Acrobat 7 and 8 by March 18. In addition, Adobe planned to make available Adobe Reader 9.1 for Unix by March 25.

Microsoft Fixes Critical Windows Kernel Flaw

Microsoft released three security bulletins to address eight vulnerabilities in Windows. The most serious, MS09-006, fixes a critical flaw in Windows kernel that could be exploited to allow remote code execution. The other two bulletins address spoofing vulnerabilities and are rated important. The critical bulletin is the first to address a flaw in Microsoft's Windows 7 beta. In addition to the security bulletins, Microsoft issued an updated version of its Malicious Software Removal Tool that now includes definitions for the Koobface worm.

Sprint Notifies Customers of Account Data Compromise

Sprint has notified several thousand customers that their account information was sold or shared without their permission. The breach occurred several months ago when a Sprint employee accessed the account

information and appears to have given the information to a third party. The data included names, addresses, wireless phone numbers, account numbers and answers to security questions. Affected customers were urged to contact customer service and change their personal identification numbers and security questions.

Experts Establish Baseline Standard of Due Care for Cybersecurity—The Top Twenty Most Critical Controls

Washington DC, (February 23, 2009) A consortium of federal agencies and private organizations released Version 1.0 of the Consensus Audit Guidelines that define the most critical security controls to protect federal and contractor information and information systems. The draft may be found at <http://www.sans.org/cag/>. The public review period ran through March 23, 2009. The CAG initiative is part of a larger effort housed at the Center for Strategic and International Studies in Washington DC to advance key recommendations from the CSIS Commission report on Cybersecurity for the 44th Presidency.

Cyber attack and defense experts from the federal agencies most involved in cybersecurity pooled their knowledge of the attack techniques being used against the government and the defense industrial base to determine the twenty key actions (called security "controls") that organizations must take if they hope to block or mitigate known attacks and attacks that can be reasonably expected in the near term. They tested their proposal for protecting federal systems to determine whether they would also stop or mitigate attacks known to be used against financial institutions and found the Top Twenty Controls are essentially identical across government, the defense industrial base, financial institutions and retailers.

For each of the 20 controls, the experts identified specific attacks that the control stops or mitigates, illuminated best practices in automating the control (for 15 controls that can be automated) and defined tests that can determine whether each control is effectively implemented. The resulting document is called the Consensus Audit Guidelines and, once fully vetted, is expected to become the standard for measuring computer security in organizations that are likely to be under attack. The CAG project is led by John Gilligan who served as CIO for both the US Air Force and the US Department of Energy and served on the Obama transition team focusing on IT within the Department of Defense and the Intelligence Community.

Broad adoption of the CAG may lead to agreement on standards for security automation and government-wide procurement of tools that work. The Federal government spends more than \$70 billion on information technology each year.

The detailed Consensus Audit Guidelines are posted at www.sans.org/cag along with control descriptions, examples of attacks they stop or mitigate, how to automate them, and how to test them.

\$19 Billion

(Continued from page 1)

payments for critical access hospitals, federally qualified health centers, rural health clinics, children's hospitals and others. It phases in Medicare payment penalties for providers not using electronic health records starting in 2014.

Microsoft CEO Steve Ballmer asked Congress to pass the bill quickly. "We believe information technology can help create a connected health system that delivers predictive, preventive and personalized care - a system that will improve the health of Americans and help control healthcare spending," he said.

"Government support for rapid adoption of information technology is essential and measurable outcomes are needed to help the Administration and Congress achieve the goals of increased access, lower healthcare costs and improved quality of care."



"We believe information technology can help create a connected health system..."

In-House News



The Technology Group, LLC Earns Microsoft Gold Certification

The Technology Group, LLC (TTG) is now a Microsoft® Gold Certified Partner. These business partners represent the highest level of competence and expertise with Microsoft technologies, and have the closest working relationship with Microsoft.

At this level, TTG will have access to resources and support including a technical services coordinator, access to the Partner Knowledge Base, priority listing in Microsoft directories, and other top-level benefits.



TTG managing director, Mark Torello, commented, "Microsoft is everywhere in the enterprise space and there's always something new coming from them. Having this prestigious designation provides us with priority access to applications and technical support that we can pass along directly to our clients."

The Technology Group, LLC Earns Cisco Select Certification

The Technology Group, LLC (TTG) has earned the Cisco Select Certification from Cisco Systems, Inc. The TTG team has demonstrated that they are qualified to sell, install and support Cisco solutions. Cisco Systems is the worldwide leader in networking for the Internet.

Welcome New Clients!

The Technology Group, LLC would like welcome the following new client additions:

- **Read to Grow**
- **North Central Area Agency on Aging**
- **Connecticut Historical Society**
- **CF Oil**

Best Practices for Your Server Room

By James Amenta

Here are some helpful tips and "Best Practices" that can help prolong the life of your systems and improve the stability of your network. How yours is set up can affect your entire operation - for better or for worse.

Cleanliness - Clutter around your systems can create trip hazards for employees, and make it difficult to access the servers when needed. Clutter can also hide problems. A

cable that has come unplugged can be difficult to spot when hidden behind a mess.

Wires dangling from the ceiling, across the floor, or along the wall substantially increase the likelihood of being pulled out of the hardware to which they are attached. This can not only cause damage to the wire or connector, but to the equipment as well. Neatly bundled and organized cabling can avoid expensive repairs, prevent the loss of productivity due to downtime, and make troubleshooting easier when there is a problem.

Server Location

We all know that space can be a challenge. In many cases, servers are in small closets with other equipment around them.

Access Space – there should always be sufficient space around a server so that a technician can work on the unit from any side without having to move other items in the room.

Environmental controls – Server rooms should be kept cool with low relative humidity. Determine the BTU output of all hardware in a server room, and ensure there is proper air conditioning to meet the needs of the equipment. When you have one or two small servers, the heat created may not be

much. However, when you add many servers, routers, switches, firewalls, etc., in a rack mount enclosure, heat can build up quickly. Excess heat will cause computer hardware to shut down or fail. Such failures can cost a business in lost productivity, repairs and lost data.

Power Reliability

Every piece of hardware in a data center should be connected to an Uninterruptible Power Supply (UPS) that is correctly sized for the power demands placed on it. As new equipment is added, UPS needs should be evaluated to ensure units are not over taxed. Each computer connected to a UPS should also have the necessary software and cable installed to allow it to detect UPS status and perform a systematic shutdown if power gets low. This prevents the operating system from corruption, which can cause a machine to no longer function properly.

If your needs cannot allow for unplanned outages, a generator should be implemented; for the entire building or just for the server room.

Security

The first rule is physical security. You can have the best firewall in the world, but if your server is in an area where unauthorized personnel can walk into the room and have

access, it is exposed. Servers should be placed in a secure location. The more people in the workplace, the more important it is to secure your systems. The server should never be in a location where visitors can see it.

Keep in mind that each situation is unique, and many environments have challenges that make these conditions very difficult to achieve. If you are concerned that your environment needs improvement, The Technology Group for an assessment.

Security Tip

Disable Autoplay

By David Modzelewski



You may have noticed that if you put a CD or USB drive into a Windows PC it will automatically run the application located on the media. This happens because of a Windows feature named Autoplay. While convenient, this is also represents a significant security risk that just so happens to be enabled by default.

Unfortunately, Autoplay is extremely easy target for malware developers. Even simple Autoplay attacks can result in data theft, system downtime, and unnecessary repair costs.

Disable Autoplay and reduce your risk.

**Connecticut Community
Providers Association (CCPA)
Breakfast Seminar**

**Increasing Your Accountability
and Transparency**

Financial management and accountability are critical for non-profit organizations. Most non-profits, however, find that commercial accounting systems do not meet their special tracking and reporting requirements.

Join us for an informative meeting to learn how Sage MIP Fund Accounting proves itself as a dynamic, versatile powerhouse for non-profits.

When: April 22, 2009

Time: 9:00 am to 11:00 am

Where: CCPA

35 Cold Springs Road
Suite 522

Rocky Hill, CT 06067

RSVP: Kendra Maigarie

kmaigaire@ccpa-inc.org

860-257-7909

**The Technology Group, LLC
is proud to be allied with:**

sage
software

Authorized Partner

CISCO SYSTEMS
RESELLER

ISACA

Microsoft
GOLD CERTIFIED

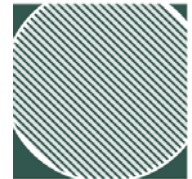
Partner

DELL™
RESELLER

CERTIFIED
QuickBooks
ProAdvisor

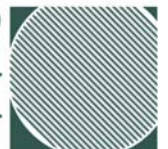
BUSINESS TECHNOLOGY QUARTERLY

SPRING 2009 EDITION OF



147 Charter Oak Avenue
Hartford, Connecticut
06106-5100

**The
Technology
Group, LLC**



PR SRT STD
U.S. POSTAGE
PAID
Hartford, CT
Permit #2639