

# BUSINESS TECHNOLOGY QUARTERLY

Brought to you by **The Technology Group, LLC**

(860) 524-4400 [www.TheTechnologyGroup.com](http://www.TheTechnologyGroup.com)

## No More Paper!



By Eric Stoltz

A "Paperless office" is when a company scans their paper files into a computer-based storage system that can increase the speed of document retrieval and processing, and eliminate the need for bulky on-site file cabinets. When a paperless office solution is implemented it adds value to your company both from a physical standpoint - through gained floor space - as well as a productivity standpoint with an expedited file retrieval process.

### Space and Time Savings

Technology has evolved to the point of affordable digital storage for any size office. A single server can hold millions

*(Continued on page 4)*

## Remote Access



By Ian Cranston

The ability to access your business information from any location is an indispensable tool in today's competitive environment. With a properly installed system, you can securely access all of your business's data and software from almost any PC connected to the Internet.

*(Continued on page 3)*

### Join Us!

## SAGE MIP FUND ACCOUNTING USER GROUP!

If you are interested in participating in our User Group, please email Camille Livsey [clivsey@ttgct.com](mailto:clivsey@ttgct.com), with USER GROUP in the subject line.

**Next Meeting: Oct 5, Bloomfield**

## Just for Non-Profits

### Optimizing your Raiser's Edge version 7 Software

By Camille Livsey

If your organization has invested in Raiser's Edge software are you are maximizing its strengths? If your organization doesn't budget time and money for training, whether self-taught or purchased, you might be under-utilizing the software.

Whether a converted version 6 user, or purchaser of version 7, could you answer yes to any of the following questions?

- Are you embarrassed when constituents receive duplicate mailings?
- Do you sometimes mail solicitations to a constituent who is deceased?
- Are too many mailings returned due to a bad address?

Strengths of ver. 7 that prevent problems listed above include "Head of Household" processing and checkboxes for constituents that are inactive, deceased and/or have no valid address. In previous versions, RE users used attributes or constituent codes to identify these

*(Continued on page 3)*

## INSIDE

Web Monitoring	pg. 2
Incident Handling	pg. 3
In-House News	pg. 3
Secure that Laptop Easily	pg. 4
Top 8 Reasons to use Whole Disk Encryption on Laptops	pg. 5
Security Center	pg. 6
Upcoming Sage MIP and Sage FR50 Seminars	pg. 6
It's Just Quickbooks	pg. 7

## Web Monitoring

By Jeff Gerace



No matter how much effort your organization puts into written and verbal policies, you are almost guaranteed to fall victim to some sort of web abuse. The CEO reading the on-line version of the New York Times may not be gross abuse, but if this became the habit of all employees this could turn into a problem that reduces efficiencies and would fall under the category of web abuse. Most organizations allow a reasonable amount of personal internet use, as long as their employees exercise good judgment. But when you have a business with more than one or two employees, the odds of a few of them abusing the use of the web are great.

To curb this abuse and maintain business efficiency, companies implement monitoring solutions. There are also other reasons to consider implementing a web monitoring solution; regulations such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley and Payment Card Industry (PCI) data security standards that some organizations fall under,

**“...you are almost guaranteed to fall victim to some sort of web abuse.”**

which require archiving and historical reporting of email and internet use. With the explosion of streaming audio and instant messaging (IM), precious bandwidth can be wasted on non-essential use while legitimate use is hampered due to taxed resources. It is important to remember that as useful (and necessary) the internet is, it is also a vast, unregulated entity that can and will cause damage to your organization if left unchecked.

Most organizations do not have the time, nor desire to look over the shoulder of every employee to see where they are going on the internet. There are some easy ways to let technology do this for you. In the world of web monitoring, there are really two choices; hardware and software based.

**Hardware based** refers to a dedicated device that is purchased as a “stand-alone” unit. It comes pre-configured with an operating system and all of the required components to begin monitoring web traffic almost immediately. The advantage to these devices is the convenience of a fully functional device that does not require any additional hardware to perform its job. These units are generally

very compact and easily fit into existing racks and server closets. The downside of these devices is the cost. They run on average 50-60% more expensive than their software based counterparts, this is due to the built-in hardware platform.

**Software based** internet filtering is purchased as a download or on a CD/DVD. The purchaser is responsible for providing a server for the software to run on, which is an important consideration when budgeting for cost and maintenance. Sizing of the server is dependent on number of users and the specific software choice. There are a large number of providers of software based internet monitoring software that provide excellent applications that consistently rate well, however there are also many are not very reliable, and do not have proven results.

**The final result:** After implementing a web monitoring solution, regular reports can be run outlining top web sites, top users, most time spent online, etc. Reputable monitoring software has reporting features built in making it convenient and easy to run. These reports are what management should be reviewing for trends and abuse. Coupled with sound policies, business efficiency can be restored and kept at an optimum level.

## Optimizing Raiser's Edge

(Continued from page 1)

constituents. If you are still using the old attributes or constituent codes you are creating one more step when creating a mailing list. Fortunately, with RE 7 global changes and table clean up can be used to change the old attributes and constituent codes to the stronger check box alternatives.

Business Rules new with RE7 are often overlooked and can solve many problems such as dealing with deceased constituents. This is a powerful tool and if used correctly prevents mailing to deceased and prompts the user to change the addressee/salutation. RE7 even allows you to define "User defined" business rules such as identifying board members, major donors, etc. when the record is opened.

Back to "Table Clean-up". Most nonprofit organizations see a lot of changeover with development personnel. As a result, there can be many attributes and constituent codes used by previous personnel that are no longer valid. RE7 allows you to easily clean up and delete old codes or attributes.

One of the strongest features of RE7 is the "Required Fields" function. This tool can be used to prevent a garbage database. Not only can you require certain fields but you can also hide fields.

Use the powers of RE7 to clean up your database and require fields to maintain a database you can trust.

## Incident Handling



By Greg Rothauer, MCSA

An Incident Handling Plan is a documented procedure that a company follows when confronted with the misuse of their computer systems. Examples of incidents include Hacker attacks, virus infestations and Trojan Horse programs that take over PC's or steal sensitive information.

An Incident Handling Plan is crucial because of one inescapable truth: An incident of some type will happen to you.

### What do you do?

Do you unplug servers from the network, reformat and restore from backup? Can you do that in the middle of the workday or do you wait until after hours? Should you call Law Enforcement? If you do call, do you know whom to call? Do you want to (or have to) notify customers, clients or patients of the possibility of identity or information theft? **Most importantly, who makes those decisions?**

An Incident Handling Plan is your roadmap, providing the answers to these questions while they're still hypothetical and you're not in "crisis mode". When you're embroiled in an "incident" is not the best time to be making rational, well thought through decisions or to be scrambling for phone numbers as everyone will be stressed out and reactive. The hope is that you will never need to use an incident plan, but having it during a crisis is crucial.

## Remote Access

(Continued from page 1)

Most businesses that utilize a server can provide secure remote access to email, files and programs without any additional computer hardware. Setting up remote access allows you to negate the impact of snowstorms, emergencies or illness on critical business applications.

Remote access uses software included with Windows XP (and is available for Windows 2000 free of charge), and a remote computer (a computer at another location) connected to your server via the Internet. Once your username and password are validated, a virtual desktop is displayed on your computer with access to your company email, shared drives and programs.

## In-House News



The Technology Group, LLC welcomes **Jill St. Sauveur** to our team as an Administrative Assistant and **Ian Apruzzese** as a Sr. Network Engineer.

We welcome the following new client additions:

- **The Open Hearth**
- **Hontek Corporation**
- **Also-Cornerstone, Inc**
- **Easter Seals**
- **Goodspeed Musicals**
- **Village for Families & Children**
- **Rhode Island Historical Society**

## Paperless Office

*(Continued from page 1)*

of files when scanned into digital format, reducing or possibly eliminating the need for the large, metal file cabinet. The extra floor space can open up a cramped office allowing for additional staff and workspace.

Once the files are scanned into digital format, the speed for finding and processing a file is drastically reduced. You no longer need to leave your desk to search for a folder – just open up an application on your computer and search with a few key terms to find the data. Paperless office users no longer have to wait for a folder that is already in use since digital files can be shared among multiple computers.

Quality control is also a benefit of going paperless. Once a file is scanned into the system, it can be set as unchangeable. No longer do you need to worry about lost pages in a folder, or possible data changes made by employees. Once the original is scanned into the server, the paperwork is saved as a picture that can be reviewed for processing and only approved users have the option to modify the digital media.

### Choices

There are many choices to be

made before setting up your paperless office. The two major areas are software and hardware. Selecting the appropriate software package is the first step. There are many different packages for scanning and retrieving your documents, so you will want to choose one that best fits your organization's needs. Once you have a software vendor selected, you can begin determining what hardware will be needed to make it function optimally. Server size, PC requirements, scanner speed, and network speed will be factors with your paperless office. You will need to build a system large enough to hold all your documents to be retrieved digitally, plus leave enough room for future growth. Your local area network should be fast enough to support large file transfers to all users. All computers should be fast enough to open the images promptly, with screens large enough to view the images.

A paperless office solution can be a great asset to any office, large or small, as long as it is researched and implemented properly.

If you are interested in setting up a paperless office and learning more about how it can benefit your organization, please contact The Technology Group at 860-524-4400.



## Secure that Laptop easily...A guilt free approach



Mark R. Torello, CPA, CFE, CISA

OK....yet another article focused on guilting you into spending more time and money on security....scaring you with stolen data horror stories....threatening your hard earned reputation with the possibility of a newspaper article showing your company in a careless light. Not this article! If you have not done anything by now...well, you either don't care or don't get it. Either way, you have stopped reading this article by now.

This article is for those that do care and are looking for some straight forward advice in securing their laptops and confidential data easily.

Before we lay out the options....I want to dispel some common misconceptions. If you access a server for all your confidential documents or programs, you may think that there is nothing on your laptop to worry about. This may not be the case, as software such as Microsoft's Word and Excel

develop temporary files of documents you work on and store them locally (on your laptop or PC) for crash-restore purposes, etc. If you only use a password on your laptop without encrypting the contents, you only put the smallest hurdle in front of the technophile gone bad. To protect temporary files, swap files and printer spools, you need to encrypt the entire drive. When you do this, the entire file system is encrypted, including the Operating System (OS). Because of this, drive-encryption software must load before the OS.

Now for the options.....

**Winmagic SecureDoc 3.1**

Network Computer Magazine Gave Winmagic SecureDoc 3.1 its Editors choice award. SecureDoc encrypts drives with DES, 3DES and AES. It also lets you encrypt floppy disks with the same encryption key or a key shared among a few people. You can protect and hide data from multiple departments within your organization. Disks can be encrypted and shared among a group, which is a common activity, or reserved for the lone user. In addition, you can store the encryption key on the floppy disk instead of the hard drive, thus

requiring the floppy in addition to user name/password and acting as a token. Another feature supported is locking down the removable drives.

*SecureDoc 3.1 Disk Encryption Software, \$159 (individual license).*

**PGP Whole Disk Encryption**

PGP products are generally considered the "Gold Standard" for security and encryption. PGP lets you create any number of virtual disks, encrypted containers that the operating system treats as if each were another drive partition. This comes in handy if you want to encrypt some files on an external drive but not the entire drive. The program also lets you create an encrypted PGP Zip file that you can send to others -- and your recipients don't need a copy of the program to open the files within. PGP's package also includes a secure data-shredding tool for making any deleted file unrecoverable. PGP allows for central management which is most appropriate for business networks.

PGP Whole Disk Encryption 9.5  
\$119 per licensed user

Contact The Technology Group LLC for assistance with laptop security.



**TOP 8 Reasons to Use "Whole disk Encryption" on company laptops**

By Mark R. Torello

**1. Protects Data When Laptop Lost**

No matter who finds the laptop, the data on the hard drive is protected.

**2. Protects Data When Laptop Stolen**

If unfortunately your laptop is stolen then the data on the laptop is protected.

**3. Better than Mountable Encrypted Volumes for Normal Users**

Mountable encrypted volumes turns an encrypted file to a drive letter, like a "F" drive. The user has to remember to run the encryption software and mount the volume before they can save their data. "Automounting" does not provide protection if some one can boot your operating system.

**4. Better than Encrypted File System (EFS)**

Encrypted File System (EFS) is included with Windows 2000 and Windows XP Professional. It allows you to encrypt selected files, but does not let you encrypt operating system files. It is good for securing data but as the operating system stores configuration and temporary files in many places EFS is not as effective as full disk encryption, but better than nothing.

**5. Help Meet With Regulatory Concerns**

If the laptop is lost or stolen, or if the laptop has private customer

*(Continued on page 6)*

**"...consider full disk encryption to protect your corporate data."**

## TOP 8 Reasons...

(Continued from page 5)

data on it then the loss of the data must be reported and customers notified. This can be a huge embarrassment for any company.

### 6. Transparent to User

Unlike EFS and Volume Mounted encryption, the only evidence that full disk encryption is active is the password request when the computer boots.

During heavy disk operations there is only a 5% performance hit while reading and writing to the encrypted drive.

### 7. Beyond Username and Password of the Operating System

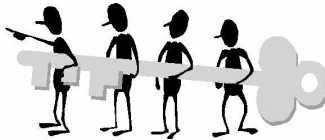
Many people think the username and password protects the data on the laptop. This is not the case. Without full disk encryption if someone has physical access to your laptop, it is not your data anymore.

### 8. Protects Against Rip and Attack

Not only laptops need full disk encryption. There may be desktops in your organization that contain sensitive information if stolen would not be good. Attackers could take out the hard drive, make a copy and put it back before anyone knows.

### Conclusion

For portable data and confidential data in high risk locations consider full disk encryption to protection your corporate data.



## SECURITY CENTER

### Security News

(Courtesy of the Sans Institute)

#### DoD Report: China Bolstering Cyber Warfare Capabilities

(May 28 & 29, 2007)

China "has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks," according to a recent report from the US Defense Department (DoD). In previous years, the Pentagon's annual report to Congress on China's military power has indicated that China was focusing on defensive measures, so a shift to offensive tactics merits attention.

#### Energy Dept. Lost More Than 1,400 Laptops Over Six Years

(May 25 & 29, 2007)

The US Energy Department (DOE) has acknowledged that it has lost 1,427 laptop computers since 2001. According to DOE, none of the missing laptops contained classified data. Nine had encryption software installed. No employees have been disciplined as a result of the laptops' disappearances. New DOE policies include annual inventories of laptops, desktop computers and Blackberries, and require offices to report missing equipment to headquarters within 24 hours.

#### Spear Phishing Attack Spoofs Better Business Bureau

(May 29 & 30, 2007)

More than 1,400 US corporate executives fell prey to a phishing attack that appeared to be from the Better Business Bureau (BBB). Executives received email messages that claimed complaints had been filed with the BBB about their companies. When they clicked on the provided link to view the complaint, a post logger was installed on their computers which sends all information sent through Internet Explorer (IE) to the attackers. The email messages are targeted to specific executives; their names and the names of their companies are correctly spelled to allay suspicions of fraud. The BBB has issued a fraud alert regarding the attack.

#### iTunes Now Selling DRM-Free Music

(May 30, 2007)

On May 30, iTunes online music store began selling songs from the EMI music label without digital rights management (DRM). All EMI songs previously sold by iTunes are now available in DRM-free format; users who have purchased DRM-protected music can upgrade to the unprotected versions for 30 cents a song or US \$3 an album. DRM-protected versions will still be available at a lower price. Music without DRM is playable on a broader range of portable players.

#### Cisco Warns of Cryptographic Library Vulnerability

(May 25, 2007)

Cisco has issued an advisory warning of a vulnerability in a third-party cryptographic library

used by several different Cisco products. The flaw could be exploited when parsing a malformed Abstract Syntax Notation One (ASN.1) object. Repeated exploitation of the flaw could result in a denial-of-service (DoS) condition. Affected products include Cisco IOS, Cisco IOS XR, Cisco PIX and ASA Security Appliances, Cisco Firewall Module and Cisco Unified CallManager. Cisco has released a patch to address the vulnerabilities; there are no workarounds.

### **Substitute Teacher to Get New Trial in Pop-Up Case**

(June 7, 2007)

The guilty verdict against Connecticut substitute teacher Julie Amero has been set aside. Judge Hillary B. Strackbein granted the defense's request for a new trial. The jury had returned a guilty verdict against Amero on January 5, 2007 for risk of injury to a minor. The prosecution argued that Amero had willfully surfed pornographic websites, resulting in middle school students in the classroom viewing adult images. Amero has maintained that the computer in the classroom was inundated with pornographic pop-ups; whenever she closed one, more would appear in its place. Researchers conducted a forensic examination of the computer that contradicted the prosecution's version of events. The State of Connecticut then ordered new testing of the computer; the findings agreed with those of the researchers. The PC on which the offensive pop-ups appeared did not have a firewall or security software. Evidence indicates the computer became infected after a user visited a hairstyle

website. In setting aside the verdict, the judge dismissed as erroneous testimony from a police detective that Amero had deliberately surfed to a pornographic site; jurors may have based their decisions on that erroneous testimony. No new trial date has been set.

### **Teens Arrested in School District Intrusion**

(June 5, 2007)

Two recent graduates of A.J. Moore Academy, a high school in the Waco (Texas) Independent School District (WISD), have been arrested and charged with breaking into the district's computer system. Both teens were charged with breaching a computer system and were freed on a US \$1,000 bond. The young men allegedly gained access to sensitive student information, including addresses, parents' names and Social Security numbers. One of the teens maintains he did not download any data; however, an affidavit alleges he downloaded a file containing the personal information of 15,000 WISD students.

### **Credit Union Bills TJX \$590,000**

(June 6, 2007)

A Brockton, Massachusetts credit union has billed TJX Companies US \$590,000. HarborOne Credit Union says it incurred US \$90,000 in costs associated with notifying customers and blocking and reissuing cards compromised in the TJX security breach. The credit union estimates it suffered an additional US \$500,000 in damage to its reputation. HarborOne sent the invoice instead of filing a formal lawsuit in an attempt to allow TJX to do the right thing. ■

## **UPCOMING SAGE MIP AND SAGE FR50 SEMINARS**

Join The Technology Group, LLC Wednesday, September 19, 2007 at the CSCPA in Rocky Hill for breakfast & a free demonstration of Sage MIP Fund Accounting & Sage Fundraising 50

**8:30 – 10:00 am: Sage MIP Fund Accounting Software,**

winner of the 2005 Campbell Award for User Satisfaction

**10:00 am – Noon: Sage Fundraising 50**

Register today by calling Camille Livsey at (860) 524-4465 or reach her via email at [clivsey@technologygroupllc.com](mailto:clivsey@technologygroupllc.com)



## **It's Just QuickBooks**

By Camille Livsey

How many companies and organizations dash into Staples, purchase QuickBooks and think they are all set with accounting software? Maybe the auditor says, "its just QuickBooks".

Unfortunately, QuickBooks (QB) does not come with accounting/bookkeeping training.

Implementing QB means suddenly what was in Excel or Word is now in software that requires accounting decisions to be made. Simple decisions such as determining an asset vs. a liability or reporting on cash vs.

(Continued on page 8)

### It's Just Quickbooks

*(Continued from page 7)*

accrual can be difficult for users who previously just put cash in a cash column, sales in a sales column, etc.

Without training, deposits can hang in "Undeposited Funds" for years. Bank reconciliation might have many items outstanding that really are duplicates due to data entry. Throw QB "Point of

Sale" into the mix, and errors can be doubled, or worse!

QuickBooks is a terrific solution for many companies and organizations aware that purchasing the software does not guarantee user knowledge of general accounting principles. In some cases, without assistance with implementation and/or training, the entity would be better off with Excel.

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

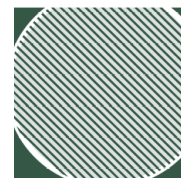


Authorized Partner



BUSINESS TECHNOLOGY QUARTERLY

SUMMER 2007 EDITION OF



at Whittlesey & Hadley, P.C.  
147 Charter Oak Avenue  
Hartford, Connecticut  
06106-5100

The Technology Group, LLC



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