



BUSINESS TECHNOLOGY QUARTERLY

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

(860) 524-4400 www.TechnologyGroupLLC.com

Your Greatest Security Vulnerability – Your Employees



By Greg Rothausser, MCSA

A recent experiment conducted in London highlights the need for companies to train employees in basic computer and network security.

A security firm handed out CDs to London commuters that were labeled: "Valentine's Day Promotion." They were clearly marked with a warning that running unauthorized software may violate their employers computer use policy.

Needless to say, the CD was not a Valentine's Day promotion. It was a program that, when executed, informed the security firm conducting the experiment

(Continued on page 5)

Web Site Held Hostage!

by Mark R. Torello,
CPA, CFE, CISA



The following is a true story of a hostage situation. The facts are real but names have been changed to protect the company from suffering additional publicity damage.

Don't let this happen to you:

You go to your web site at www.example.com only to find a picture of a tractor and the phrase "Under Construction." In disbelief, you hit the refresh button -

(Continued on page 3)

—NEWS BRIEFS—

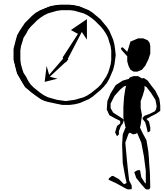
Changes in Quickbooks 2006 Cause Frustration. Page 5

Security Breaches Underscore Need for Strict Policies. Page 6

Wireless Internet Brings Benefits and Risks. Page 7

Just for Non-Profits

When Should You Invest in Nonprofit Accounting Software?



By Camille Livsey

Investing time and money in a new accounting software system is an important undertaking. If your organization has experienced growth (or downsizing), or if you have been awarded new grants that require additional, complex reports it might be time to consider a new accounting system.

Do any of the following apply to your organization?

- Are you spending large amounts of time trying to generate financial statements in spreadsheets or word processing applications?
- Is your budget maintained within your accounting system or on separate spreadsheets?

(Continued on page 2)

INSIDE

Why Automatic Updates should be "Turned Off" on your PC!	pg. 4
Quickbooks 2006 – The Frustration Begins!	pg. 5
Security Center	pg. 6
Is WiFi (Wireless Internet) Right for My Business? Part 1	pg. 7
In-House News	pg. 7
Additional MIP Seminar being Planned for New Haven	pg. 8

Nonprofit Accounting Software

(Continued from page 1)

- Are you having difficulty tracking donor-imposed restrictions on contributions?
- Would increased security or internal access controls help reduce data entry errors?
- Do you spend time manually reconciling your fund balances or maintain separate databases in order to meet FASB 117 reporting requirements?
- Is preparing the 990 a time-consuming process? Are you paying your auditors to prepare the 990 for you?
- Do you and your staff spend entire days pulling special reports for upcoming board or finance committee meetings?
- Do you have difficulty managing specific grants with reporting periods other than your organization's fiscal year?

If you answered "yes" to some of these questions, it is likely that choosing a nonprofit accounting software would be helpful and cost-effective.

Because accounting is a

mission critical part of any organization, you should list and prioritize your requirements. Evaluate the size of your organization, the complexity of the accounting required, the type and number of reports needed, any necessary interfacing requirements and the anticipated future needs of your organization.

Implementation of the right nonprofit accounting system will save you time, money and stress.

Accounting Software written specifically for nonprofit organizations addresses

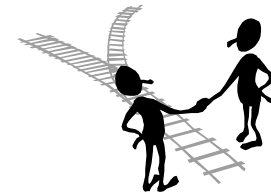
unique challenges that other accounting systems do not:

- Accounting records for a particular funding source, department, grant, program or function are separately maintained and reported;
- The unique reports required by grantors and donors are easily managed; even when they span a period that differs from the fiscal year;
- Funds can be recorded as encumbered;
- The budget (which is a formal part of the organization's books and may be a legal document) is easily managed;
- FASB 117 reporting is built in for reporting purposes;

- 990 information is immediately and directly obtainable;
- Security can be set for the individual user, complete with audit trail.
- Specific, required reports and financial statements are readily accessible – no need to export to other programs.

Converting to a new accounting program requires a considerable commitment. After evaluating your accounting needs, remember to consider hardware requirements, implementation, conversion and training costs.

While the task of assessing your needs and exploring options seems daunting, the implementation of the *right* nonprofit accounting system will save you time, money and stress. The busier your organization is, the more you can benefit from the right tools.



Contact Camille Livsey at 860-524-4465 with any questions about nonprofit accounting software

sage
software
Authorized Partner

Web Site Held Hostage

(Continued from page 1)

only to find a very unflattering picture of yourself followed by profanities and misquotes.

You can no longer send or receive email messages, inquiries or orders.

Your clients then receive a vulgarity laden message (seemingly from you) discharging them as clients.

Sound like a bad dream? It is the nightmare a local firm is living right now.

"Example.com" had an employee who developed and maintained their web site. Although he was with the company for almost 8 years, toward the end his work ethic plummeted. It was time for the firm and the employee to part ways.

The parting complete, the company breathed a sigh of relief and went back to business. Imagine the reaction when a client referred to the website said **"I see no directions, just a very funny picture of you at a Holiday party."**

What happened? **Sabotage.**

Without management knowledge or approval, the terminated employee had registered the company's domain name in his own name, with his personal email address.

Your domain name is as important to your identity as your firm's name, phone number, and address.

What did he do? He posted damaging statements about the company in place of their web site, sent derogatory emails to clients under the guise of the CEO and hijacked email accounts - ensuring

that clients received no response to orders placed over the Internet.

How could this happen? The employee had been allowed to register the company's domain name without oversight. **Your domain name is as important to your corporate identity as your firm's name, phone number, and address.** These are the keys to the company. Unfortunately, most firms and executives do not understand this simple, but powerful, distinction.

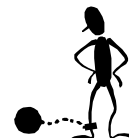
Could it have been prevented? Yes. First, any firm must make it a policy to **have their domain name owned by the firm and not by an individual.** When registering a domain name, the **"Primary or Administrative Contact" must be an officer of the company—with the officer's email address.**

The domain "Registrant" is the most important piece of information provided, as the "registered owner" is likely to win out in any legal battle. **The "admin email address" is also extremely important, as it is often used to validate changes to the domain.** Your outside systems consultant may be listed as the "technical contact."

Before parting ways with an IT employee, verify that their contact information is no longer on the domain registration. When parting ways with **any** employee, change all passwords associated with servers, firewalls and other office systems. It is in a company's best interest to consult an outside systems analyst for advice before parting ways with any IT personnel, to plan for a smooth exodus and avoid any system damage.

Who owns YOUR domain name? You can go to **technologygroupllc.com/services/whois.html** to find out.

How does the story end? You can find out in the next issue of *Business Technology Quarterly*. The resolution involves a \$20,000 ransom demand, the police, lawyers and a Forensic IT professional.



Why Automatic Updates Should be Turned “Off” on your PC!

By Mark R. Torello, CPA, CFE, CISA
and Ian Cranston, MCSE, CCNA

**Automatic updates sound like a great idea, right?
Not Always...
They can even cost you money!**

Windows Automatic Updates is a free and useful tool created by Microsoft to simplify the download and installation of “patches.” It was developed in response to the vulnerability of systems to worms and viruses – vulnerability that sent IT employees scrambling to clean and patch their systems and restore networks that were down for days.

The intent of the automatic processes was to offer users efficient and simple tools to “patch” the softwares’ weaknesses and keep systems up-to-date as additional vulnerabilities were discovered. The assumption was simple; if a user was prompted with a message that asked “would you like to update?” the user would answer, “yes,” hampering the spread of worms.

These automatic updates, while frequently helpful, can also be dangerous. Frequently the testing of the “patches” is not extensive, and accounting, billing,

ticketing or contact management systems can be adversely affected. While most home PCs and PCs that are used mainly for simple Microsoft and email functions benefit from these upgrades, businesses have other considerations.

Patches and updates should only be deployed after careful evaluation. The evaluation should include:

- **Compatibility research** (Check with mission critical software vendors)
- **Applicability review** (Do I need this update?)
- **Testing**

Compatibility Research: Before loading any updates, check that your mission critical software vendors have tested the functionality of their software with the update. Check the Internet for known conflicts. An IT professional will be very proficient with this type of Internet research. An IT professional will also have a first hand knowledge of many conflicts; on servers as well as workstations.

Applicability Review: Many updates that show up through Microsoft’s automatic update service are for specific programs like ACCESS. Some are as large as 50 MB! If you don’t use ACCESS, you don’t need to patch it.

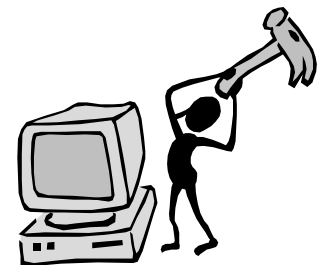
Testing: The best practice for deploying updates is testing the update first on a test computer running all the software in operation.

When your computers have “automatic update” turned on, updates download and install themselves whether you need them or not. Automatic updates do not afford you the opportunity to Research, Review, and Test (as discussed above).

How Do You Decide Which Patches SHOULD be Installed?

Rely on your technology support department or firm to deploy the updates they have determined as safe and required.

We recommend that systems be reviewed on a quarterly basis for such updates. This can coincide with any preventative maintenance that is performed. Your IT professional will have experience with patches and their compatibility with other software, thereby saving you time, trouble and money.



Contact The Technology Group, LLC with questions about running automatic updates or compatibility.

Quickbooks 2006 – The Frustration Begins!

By Greg Rothauer, MCSA



Most of us have at least heard of Intuit's popular bookkeeping line of software, Quickbooks. The ease by which Quickbooks allows small to medium businesses to manage their ledgers and payroll processing makes the software extremely popular with businesses and with their accountants and auditors as well.

Any transfer of financial data should be secure and protected – you should not transfer data until you have a security system in place!

Quickbooks' workbook file (.qbw file) has traditionally been stored on a file server for safe keeping. A user wishing to open that file would simply need permission and the proper version of Quickbooks to open it. This allowed businesses and their outside accountants to easily transfer financial data back and forth.

With the latest release of Quickbooks 2006, however, Intuit changed the way Quickbooks accesses the qbw file. There are several steps that must have been followed in anticipation of receiving and accessing the data on the file server:

- Quickbooks 2006 must have been installed on the computer **and** on the file server;
- Quickbooks 2006 must have run on the file server at least once (to start a hidden process that allows access to the file);
- The file stored must be set in "multi-user mode"

Confused? You are not alone. To clarify: Joe works for ACCOUNTANTS-R-US, and his client WE-DO-BUSINESS has been faithfully keeping track of their 2006 fiscal data within their upgraded Quickbooks 2006 software. They send their data to Joe for his review.

Joe receives the data and saves it onto the ACCOUNTANTS-R-US file server. Wishing to quickly verify that he received the correct information, Joe attempts to open the file – and receives an error. The file is not set in "multi-user" mode.

This scenario will be repeated in Accounting firms all over the country as 2006 fiscal information is shared with Quickbooks 2006. It is easily prevented with awareness and the proper set-up. If you have questions about "multi-user mode" or Quickbooks 2006 software, please call Camille Livsey at 860-524-4450.

Employees

(Continued from page 1)

who it was that inserted the CD and ran the program.

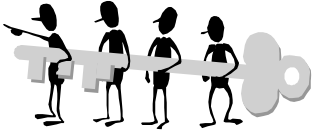
The results were alarming. Employees from banks, insurers and other businesses that handle personal, confidential information were among those who ran the CD.

By putting the CD into their PCs and running the application without bringing it to their IT department first, companies' firewalls and other security features were completely circumvented. Many businesses have policies against running applications that are not sanctioned by, and provided by, the company. However, this experiment proved that information security is not foremost in people's mind.

Employees need to be reminded of the employers vulnerabilities – and their role in preventing the dissemination of personal, confidential information. Periodic training sessions will help to create a "culture of security."

This time, the program on the CD was harmless, but it could just as easily have been a virus or worm that damaged or disseminated data.





SECURITY CENTER

This column is dedicated to IT security and protection of information assets

FBI Investigating Intrusions at Indiana Clinic

February 11, 2006

The FBI is investigating unauthorized changes made to a MySQL database that underlies an electronic medical record system at an Indiana-based orthopedics clinic. Orthopedics Northeast (ONE) noticed significant performance slowdowns in January.

The changes were apparently made by an intruder who gained initial access to the system through a back door in WebChart software from Medical Informatics Engineering (MIE). On one occasion, the intruder appended characters to a database query, causing it to crash. On another occasion, the intruder deleted a print-server directory.

Analysis demonstrated the intruder accessed the WebChart system through a proxy server at a hospital; ONE is connected to the hospital via a virtual private network (VPN).

Security Breach Prompts Cancellation of Bank of America Debit Cards

February 14, 2006

In response to a data security breach at an unnamed California office supply store, Bank of America (BofA) and Washington Mutual have canceled an undisclosed number of debit cards. A BofA spokesperson said there is no evidence of customer account compromise. An investigation is underway.

Affected BofA customers received letters informing them their debit cards were canceled and encouraging them to be vigilant about scrutinizing their statements for unauthorized transactions.

Lack of Security Brought Charges by FTC on CardSystems Solutions

February 23, 2006

CardSystems Solutions settled charges of failing to protect sensitive customer data by the Federal Trade Commission (FTC) following a security breach that resulted in more than 260,000 cases of identity fraud.

The company had been retaining data from the magnetic strips of credit and debit cards and keeping it without adequate security.

The company, which was bought by Pay By Touch in December, will "implement a

comprehensive security program and obtain independent audits every other year for 20 years." as part of its settlement with the FTC.

Forty million accounts were determined to have been vulnerable.

Accounting firm, Deloitte & Touche, Lost Disk Containing Client's Employee Data.

February 23, 2006

A McAfee spokesperson said that an external auditing firm lost a CD containing the unencrypted names, Social Security numbers and McAfee stock holdings of an unspecified number of current and former employees. Deloitte & Touche acknowledged that an employee left the unlabelled CD in the seat pocket on an airplane. The affected employees have been notified

Accounting firms use laptops, CD burners, and thumb drives now more than ever. Auditors take these devices on the road with their client's sensitive data on them. Many times these devices are left in vehicles unattended. The more diligent accounting firms have policies for keeping client data secure, such as utilizing encryption, and keeping data devices physically secure. The speed at which high capacity storage devices have come

to market has made it difficult for firms to address the security issues that come with them.

Credit Unions Hit by Debit Card Fraud Might be Linked to OfficeMax

March 10, 2006

Investigators say that debit card fraud affecting members of credit unions in Leominster and Fitchburg, Massachusetts may have been linked to a security breach related to OfficeMax; all affected customers had used Visa debit cards at OfficeMax.

Fraudulent account withdrawals have been made in Spain, Turkey, Greece, Switzerland, the UK, as well as in the US and Canada, suggesting that the information is being sold on the Internet.

The thieves used cloned debit cards constructed with the use of stolen PIN numbers, either from OfficeMax or from a transaction processor.

An OfficeMax spokesperson said there is no evidence of a security breach of their network.

Information courtesy of the SANS Institute unless otherwise noted.

Visit TechnologyGroupLLC.com for up-to-the-minute Security Updates

Is WiFi (Wireless Internet) Right for My Business? (Part 1)

By: Christopher Newton

The past few years have seen WiFi usage rise exponentially. This is primarily due to their simple, low-cost installation.

Wireless Internet enables businesses to provide their clients and guests access to the Internet while visiting.

However businesses that use WiFi need to keep in mind that they are "opening a door" to their systems and information, and they need to address their potential vulnerability when incorporating this technology.

To address this challenge, organizations should first decide what type of WiFi access they would like to provide (and over the next few newsletters we will discuss the types of access and their associated vulnerabilities).

Basic – I want to provide a means of Internet access.

Providing basic access is as easy as taking a trip to the local Wal-Mart to purchase and install a Linksys Access Point on your network. Once that is done, however, you have made your files more accessible – not only to

employees, clients and guests, but to the random hacker in the parking lot that is looking to hijack your information.

To address this threat while ensuring basic Internet access to those you wish to have it, you have two primary choices. Set-up a

separate, low-cost DSL line to be used only for guest and client access or segmenting your network appropriately. By utilizing the proper hardware devices (like routers and managed switches) you avoid

subjecting your network and confidential files to a serious (and often overlooked) vulnerability.

Please contact the Technology Group with any questions regarding WiFi and how to properly implement it within your organization.

...businesses that use WiFi need to keep in mind that they are "opening a door"...



In-House News

We are delighted to announce the addition of Ian Cranston MCSE, CCNA as a network engineer. Ian's specialties include wide and local area network engineering with Cisco and Microsoft products.

**Additional MIP Seminar
Planned**

Due to the popularity of our February MIP seminar, we are planning another in the New Haven area. Check our website for more information as it becomes available.

The session will cover Sage MIP Fund Accounting Software and Fundraising 50.

These software tools make your reporting and financial statements run more smoothly, and assist you in collecting more contributions and matching funds from donors than ever before!

www.TechnologyGroupLLC.com

860-524-4400

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



BUSINESS TECHNOLOGY QUARTERLY

SPRING 2006 EDITION OF



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



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