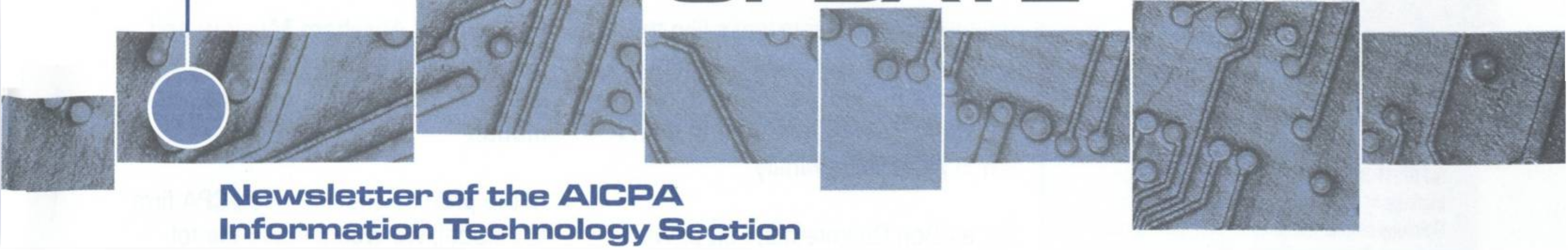
InfoTech Update, Volume 15, Number 6, November/December 2006

American Institute of Certified Public Accountants. Information Technology Section

InfoTech UPDATE

NOVEMBER/DECEMBER 2006
VOL. 15, NO. 6



Newsletter of the AICPA
Information Technology Section

What's Inside

Disaster Recovery Survival Equation: BC > DR + L

By Michael S. Kridel, CPA.CITP, CFC*

Regulated by the State of Florida

Michael S. Kridel, CPA*.CITP, CFC, is a partner with Daszkal Bolton LLP in Boca Raton, Fla., with responsibility for the firm's litigation services and consulting practice, as well as internal human resource and information technology systems.

When last we visited, I was staring down the gun of another hurricane season, facing weather experts' predictions of another large number of potentially devastating storms; perhaps not as many as in 2005, but an attention-getting prognostication nonetheless. As I write this, the experts have, in fact, said the revised prediction was one more "named" storm this season.

Thanks in a large part to an unpredictable El Niño, the gulf coast – and Florida in particular where I live – are through a nearly uneventful season, having only been brushed by one major storm system. Shutters went up only once (a good thing considering the cost of doing this at our office), no more than a day and a half of work was interrupted, and we're none the worse for wear.

Except ... to borrow a quote from Pogo, that venerable observer of human nature, "I have met the enemy and he is us."

Short Memories of Disaster

This season of respite, candidly, is rapidly erasing most everyone's memories of the past two years. With tourism attempting to reclaim New Orleans and hundreds of thousands of snowbirds migrating to Florida for the winter, we are a society that easily forgets – and forgives. Unfortunately, this complacency, coupled with misdirected risk management paradigms, will become major barriers to *preventive* measures and the adoption of disaster recovery strategies – many of which we, as accounting professionals – can help facilitate for our clients, employers and the public.

Moreover, for many firms who chose (before and after Katrina and other disasters) to roll the dice and adopt nominal "ultimate disaster scenario" solutions,

Continued on page 2

InfoTech UPDATE

November/December 2006, Volume 15, No. 6. Publication and editorial office: AICPA, 201 Plaza Three, Harborside Financial Center, Jersey City, NJ 07311-3881. Copyright © 2006, American Institute of Certified Public Accountants, Inc. Opinions of authors and the AICPA staff are their own and do not necessarily reflect policies of the Institute or the Information Technology Section. Any hardware or software products mentioned do not in any way represent an endorsement by the Institute or Section.

If you wish to change your e-mail address or update your member profile, please send an e-mail to service@aicpa.org.

For questions about your subscription to InfoTech Update or other questions about your IT Membership Section benefits, please contact the AICPA at infotech@aicpa.org or leave us a voice mail message at 201-938-3828, option 3.

Disaster Recovery Survival Equation

continued from page 1

rolling the dice *again* looks like the most likely path of least resistance. I, for one, am no more willing to relax my charge to protect our firm than I am to protect my family.

So, as Don Quixote did, I tilt at windmills.

During my learning curve, I have come to realize that in the months of fretting since June 1 – the official start of hurricane season – I have really been working toward the concept of business continuity (BC), which is to disaster recovery (DR) what calculus is to algebra. BC planning allows an entity to minimize reliance on luck (L), because the continuity of business is the real objective – and continuity is the ultimate goal of risk management.

We can look at BC issues without going into the diverse universe of risk management, with areas encompassing succession planning, every kind of insurance concern, employee turnover and competitive strategies. Moreover, BC is a year-round issue and addresses every kind of threat to entity survival, whether it is a sudden earthquake or terrorist attack, or the slow, methodical onslaught of a hurricane or pandemic. Interestingly, academics teach us that each of the foregoing examples is a *predictable* certainty, perhaps not as to *"when,"* but clearly as to *"if."*

The CPA Business Continuity Plan

The elements of BC are fairly simple and have their foundation firmly rooted in what could be called "natural laws." We could look to the work of Abraham Maslow and his classic Hierarchy of Needs as the base on which to build the BC model.

In the professional services/CPA firm BC model, we would make the following changes, working from the most basic need (Physiological) to the (nearly) most advanced need (Self-Actualization):

- **Physiological:** Safeguarding physical assets, such as information technology systems and client files.
- **Safety:** Assuring the well-being of our most important assets, personnel.
- **Love/Belonging:** Maintaining a sense of community even after disaster strikes and striving to avoid disconnects.
- **Esteem:** Providing each person the opportunity to help or be helped without having to ask, and providing them with positive feedback and increasing opportunities to participate.
- **Self-Actualization:** Developing clearly defined plans addressing contingencies and providing systematic solutions, as well as strategies to assure execution of business continuity tasks.
- **Contribution:** The true zenith of the model.

In my model, Self-Actualization is almost the most-advanced need because Contribution is paramount. Maslow's widow said that when her

Continued on page 3

Disaster Recovery Survival Equation

continued from page 2

husband was nearing death, he claimed his model was flawed; he had missed something that was even more important than self-actualization – and that "something" was *contribution*.

In our CPA environment, "contribution" is the opportunity for all personnel to play active roles in the BC process, whether it is preparing for the disaster or assisting with the recovery. This process flows and grows from satisfying the subordinate five needs in the model and is central to the definition of humanity.

Psychology aside, BC is merely a means of perpetuating three core elements essential to the success of any business: 1) systems and procedures, 2) communication and 3) personal support. The first two, systems and procedures, and communications, are commonly referred to as *infrastructure*, while the third, personal support, is the *people* factor. Because many types of BC planning are beyond the scope of this article, our focus will remain with disaster recovery planning, which incorporates these three pieces.

Daszkal Bolton came up with nine steps to the BC plan. As you're reading through this, I encourage you to measure your own firm's or company's similar plan – in whatever format it might take.

Step One: **Qualify and quantify the various components of the plan.** Someone much smarter than me said, "If it's not in writing, it doesn't exist. If it's not been tested, it has no value." This is the disaster recovery professional's mantra, so we have been documenting each step in the planning process.

Step Two: **Clearly define those areas essential to operation of the firm**; specifically, functional areas considered to be vital (IT), fundamental (time and billing), basic (client communications) and preferable (the working environment). We researched available resources to provide us with baseline definitions of what might fit within each of these categories and then vetted key personnel in an effort to determine their perceived priorities and willingness to conform to a plan.

This process was extremely challenging because an effective disaster recovery plan requires that the number of decision makers be severely limited. The experience of others has proved that group thinking and consensus is counterproductive to effective decision making under stress. In addition, the skill sets that make someone successful do not necessarily translate to the disaster recovery process. Most larger companies have designated a specific individual, such as a Risk Management Officer who is charged with developing and maintaining continuity and recovery teams, plans and, most important, has the authority to execute.

Step Three: **Explore available recovery alternatives.** Because we know that "data is the Prince to King Cash," and technology drives our abilities to work and respond to client needs, we were primarily concerned with that side of the recovery model. We met with, and solicited proposals from, numerous local and geographically remote-hosted and co-location solution providers; disaster conditions hard asset vendors; and hot, warm and cold site companies. We also explored lead/lag concerns with our traditional vendors.

> **"Psychology aside, BC is merely a means of perpetuating three core elements essential to the success of any business: 1) systems and procedures, 2) communication and 3) personal support."**

Step Four: **Review various forms of insurance coverage.** Much to our chagrin, we discovered that our business interruption policy had become extremely narrow. So much so, that the only coverage we had, should we be unable to work during an extended power interruption, would apply only if the interruption could be traced to

Continued on page 4

Disaster Recovery Survival Equation

continued from page 3

something on our own property (downed power lines or disabled power plants were excluded). We also discovered that, even if we could find a policy or rider that would mitigated these circumstances, the costs were prohibitive.

Step Five: **Look at less comprehensive forms of redundancy and data replication**, such as a Storage Area Networks (SAN), as well as offsite online backups and electronic vaulting. We had just replaced our primary server room's universal power supply cases (UPC) with a couple of monsters, but we only scratched the surface of data continuity protection.

Step Six: **Document what would be required to execute a bare metal restore.** This was particularly important because one of the alternative, though less preferable solutions we examined, involved contracting with a vendor to provide a complete working environment, including hardware and connectivity. This, in turn, also drove us to examine how our original application media and licenses were stored, both physically and geographically.

Step Seven: **Examine interruption issues.** Because we have three offices, with the shortest radius between two of these at about 13 miles, we looked at interruption issues to one, two or three offices, and our ability to respond to these interruptions. As unfortunate as it may have seemed at the time, we did gain quite of bit of experience over the summer with one particular office losing connectivity for days at a time due to telephone company equipment failures. As a result, we found that our remote systems could handle numerous remote users working from home through our Citrix (four server) farm.

Step Eight: **Examine circumstantial risks of interruption**, whether it was from internal or external sources, along with our ability to mitigate each of them. As part of this, we classified interruptions into timeline-driven categories: one day or less, one to three days and anything longer (disaster category), and began to map the response processes to each. A critical part of this process was to determine what would be an acceptable recovery period, the point we could maintain core operational processes (typically called Recovery Time Objective, or RTO), and data loss gap, the length of time for which we were prepared to lose data and in-process work (Recovery Point Objective, or RPO).

Step Nine: **Compile steps one through eight into an organized format** so we could present alternative solutions to our Executive Committee for review and decision. This document consists of numerous sections, each of which is designed to address the three core elements of successful businesses described earlier: systems and procedures, communication and personal support. The planning process is one thing; gaining buy-in and funding is another. It requires making a strong business case and demonstrating ROI, a difficult matter when you have a non-threatening hurricane season.

The Jury is Still Out

Just as Don Quixote continually tried defending himself and his lady from the Great Inquisitor, we have not finished the BC exercise and I am not yet satisfied with our written plan or short-term decision. I am, however, pleased that we have started the process. We have learned significant and valuable lessons from this exercise, and it is just a matter of time until we get it right. My concern: Which clock runs faster? Our ability to make better decisions and fund a solid solution *or* will the threat arrive first?

I do not gamble, except on myself. The L in the BC equation has no value for me, so BC is more than DR. Companies and firms need to learn that luck has its place, but not in assuring your future. BC is the ultimate form of insurance, one on which you need only rely on yourself and the people you trust. Perhaps, then, the correct equation should be: BC = S (Survival). But I was never any good at math, so I'll put on my armor, hoist my lance and keep tilting at this windmill.

Contact Michael Kridel at *mkridel@daszkalbolton.com.*

BEST OF THE BEST: AICPA TOP TECHNOLOGIES 2006

#2 - Assurance and Compliance Applications

By Dan Schroeder, CPA.CITP, CISA

Dan Schroeder, CPA.CITP, CISA, is director of the Business Process & Technology Management practice with Amper, Politziner & Mattia, P.C. Dan manages IT and Corporate Governance initiatives with clients in several industries, including Financial Services, Healthcare, Pharmaceuticals and Consumer Product Goods. He also serves on the AICPA's IT Executive Committee.

Assurance and Compliance Applications: "Collaboration and compliance tools that enable various stakeholders to monitor, document, assess, test and report on compliance with specified controls."

New this year to the 2006 Top Technologies List, this topic's emergence reflects a powerful movement by accounting technology professionals to apply process management principles and technology to drive significant improvements to the activities associated with executing and documenting Sections 302 and 404 of the Sarbanes-Oxley Act of 2002.

Early approaches to SOX compliance were frequently inefficient, expensive and disruptive. SOX filers quickly recognized that to make compliance efficient and sustainable, they needed to institutionalize the management of SOX control functions. Moreover, public registrants and organizations also have come to recognize that while SOX is critically important, it is just one element of an effective approach to corporate governance. In effect, SOX is intertwined with an organization's broader enterprise risk management (ERM) considerations, including:

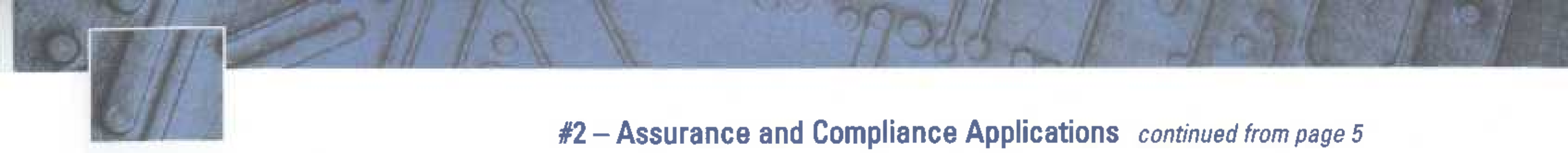
- operations risk management;
- compliance with industry regulations, such as HIPAA (Health Insurance Portability and Accountability Act of 1996), GLBA (Gramm-Leach-Bliley Financial Services Modernization Act of 1999), and FFIEC (the Federal Financial Institutions Examination Council); and
- information technology governance.

Accordingly, SEC registrants are increasingly approaching SOX compliance as an element of a broader initiative to institutionalize ERM. In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released *Enterprise Risk Management – Integrated Framework*. COSO defines ERM as "*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

Developers of compliance-related software have been quick to respond to the need to streamline the SOX compliance process and also extend the functionality to encompass ERM. Here are some common enabling characteristics of ERM compliance software that are emerging:

> **"Early approaches to SOX compliance were frequently inefficient, expensive and disruptive."**

Continued on page 6



#2 – Assurance and Compliance Applications

continued from page 5

Key Enabling Characteristics	**Description/Examples**
Common platform	ERM software is emerging as a comprehensive repository for the definition of risks, controls definitions, testing activities, test results and mitigation activities. Risk definitions and associated controls encompass financial reporting, operations management, and statutory and industry specific requirements (e.g., FFIEC, HIPAA, GLBA, SOX, etc.) ERM solutions are becoming a standard part of the corporate network, much like ERP, with defined responsibilities and associated access privileges.
Organizational and process structure	ERM software enables the complete mapping of organization structure (including operating divisions, regions, departments and cost centers) and association of business processes to those organizational elements.
Roles and responsibilities	Controls and compliance involves ownership and accountability. ERM software enables companies to deploy compliance requirements throughout the company. For example, SOX Section 302 requires quarterly and annual certification statements from CEOs and CFOs. An effectively designed and deployed ERM solution would enable the CEO to monitor the status of all controls throughout the organization at any time. Moreover, this allows the organization to have sub-certification where a business unit heads, and process owners submit, their certifications to the next level up in the company.
Continuous monitoring of risks and controls	ERM software enables companies to test controls throughout the year, following an organized approach that reflects risk and frequency on control activity. ERM software often integrates with ERP (and other) applications to automatically monitor activities using predefined rules and reporting parameters (e.g., automatically identify disbursements over $xxx for testing.)
Deployment of ownership and accountability for effectiveness of controls	SOX filers are seeking to minimize their dependency on consulting firms for development of controls and conducting management's assessment. They are working aggressively to lower audit fees that spiked when audit firms increased their burden as a result of SOX responsibilities. Example: Sub-certification linkage for 302 reporting to business unit management and functional process owners.
Embedded workflow	Deployment of workflow into ERM means the automated assignment of testing and validation requirements to individuals and roles, coupled with predefined and automated routines for notifications, alerts and exception reporting.
Integration to corporate messaging system(s)	An important underlying function for workflow and automated reporting is the ability to integrate to corporate messaging systems such as Microsoft Outlook, so reminders, exception notices and other reports can be automatically sent to auditors, valuators, process owners and executives.
Integration to corporate document or content management systems (DMS)	SOX filers and others enacting aspects of corporate governance are increasingly deploying formal change control over policies and procedures, and formal retention over compliance controls. Integration of ERM to DMS systems helps to ensure that policies and procedures are linked to process definitions, control test requirements and test results. DMS can also serve as a repository for test results and supporting workpapers to fulfill both internal and regulatory requirements.

Continued on page 7

#2 – Assurance and Compliance Applications *continued from page 6*

The COSO 2004 ERM Integrated Framework outlined six concepts that are fundamental to the deployment of ERM:

1. ERM is a process, ongoing and flowing through an entity.
2. ERM is effected by people at every level of an organization.
3. ERM is applied in strategy setting.
4. ERM is applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk.
5. ERM is designed to identify potential events that, if they occur, will affect the entity and manage risk within its risk appetite.
6. ERM is a method to provide reasonable assurance to an entity's management and board of directors (relative to design and effectiveness of risk management activities).

The implications of effectively deploying SOX and ERM compliance are complicated and represent significant challenges in terms of being cost effective. Through the use of advanced process and technology concepts outlined in the table above, companies are increasingly finding it feasible and beneficial to deploy SOX and broader ERM compliance programs.

Contact Dan Schroeder at *dschroeder @amper.com.*

BEST OF THE BEST: AICPA TOP TECHNOLOGIES 2006

#5 - Privacy Management

By Ken Askelson, CPA.CITP, CIA

Ken Askelson, CPA.CITP, CIA, is senior IT Audit manager for JC Penney in Plano, Texas, and vice chair of the AICPA/CICA Privacy Task Force.

If a breach of personal information occurred in your organization, are you equipped to effectively handle damage control for your clients and customers?

Ranked at #5 on the Top Technologies list for 2006 – and a completely new entry to the list itself – "Privacy Management" encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information. As more information and processes are converted to digital format, personal information must be protected from unauthorized users and from unauthorized usage by those with access to the data.

A key aspect of privacy management includes complying with local, state, national, and international privacy laws and regulations. It is important for the organization to identify and understand which laws and regulations are applicable to them in the jurisdictions they are doing business. For example, federal legislation mandates the protection and privacy of personal information for customers, clients and/or patients in the medical industry. The Health Insurance Portability and Accountability Act (HIPAA) includes a security rule that requires certain information security practices to be followed or addressed by covered entities. In the financial services industry, the Gramm-Leach-Bliley Act (GLBA) includes standards for safeguarding customer information required for covered entities.

While state legislation requires the protection of personal information, the law is often ambiguous on what *type* of protection is necessary. California leads the way with its Assembly Bill 1950 (AB 1950) and California State Bill 1386 (SB 1386) – legislation that requires organizations to follow certain privacy practices to protect this information, as well as notify customers within a reasonable period of time if their data is compromised.

Continued on page 8

#5 – Privacy Management

continued from page 7

As a CPA, how does this concern for privacy and federal/state legislation translate to you and the organization(s) you serve? What kind of assistance/services can you provide?

Numerous surveys have shown that customers are more likely to use and purchase services from organizations that have good privacy policies and practices and do what they say in their privacy notices. Still, other research continues to indicate that consumers have widespread distrust of many organizational business practices, including how companies collect, use and retain personal information. In the online community, for example, a Consumer WebWatch telephone survey of 1,500 U.S. Internet Users featured on Privacy & American Business reported that less than one third (29 percent) of participants trusted Web sites that sell products or services.

The accounting community ranked "Privacy Management" as a top technology for a good reason: Good privacy is good business, and good privacy practices are a key component of corporate governance and accountability.

As business systems and processes become increasingly complex and sophisticated, organizations are collecting more and more personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorized access and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments and the public in general.

Customers expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, *all* businesses need to effectively address privacy as a risk management issue. Specific risks of having inadequate privacy policies and procedures include:

- damage to the organization's reputation, brand or business relationships,
- legal liability and industry or regulatory sanctions,
- charges of deceptive business practices,
- customer or employee distrust,
- denial of consent by individuals to have their personal information used for business purposes,
- lost business and consequential reduction in revenue and market share, and
- disruption of international business operations.

In the last several years, the AICPA and the Canadian Institute of Chartered Accountants developed **Generally Accepted Privacy Principles** (GAPP). Formerly known as the Privacy Framework, GAPP is a guide to help CPAs and the organization(s) they serve to identify and apply a core set of standards through which good privacy practices could be developed, measured and assessed.

GAPP is designed to assist management in creating an effective privacy program that addresses privacy risks and business opportunities, and are founded on key concepts from significant domestic and international privacy laws, regulations, and guidelines, as well as solid business practices.

By using GAPP, organizations can proactively address the significant challenges they face in establishing and managing their privacy programs and risks from a business perspective. The use of GAPP also facilitates management of privacy risk on a multi-jurisdictional basis.

A CPA can find a number of resources in the primary GAPP document, as well as companion documents, articles and much more at *www.aicpa.org/privacy*.

Contact Ken Askelson at *kaskelso@jcpenney.com.* ●

INFOTECH UPDATE PROFILE

Natalie Hoffmann, CPA.CITP

Natalie B. Hoffmann, CPA.CITP, is a partner in Information Services for Honkamp Krueger & Co., in Dubuque, Iowa, a regional CPA firm of 175+ employees with six offices in Iowa and one in Wisconsin. The firm offers a full range of services, as well as payroll processing with HKPay, its own custom-developed proprietary software. Natalie has been with the firm for 18 years, and was previously with Andersen. She is a staunch proponent of the CITP credential, both as a member of the CITP Credential Committee and with her assistance in developing CITP Web Seminars, a member-only benefit available to credential holders.

***InfoTech Update:** What is your role regarding technology within your firm?*

Natalie Hoffmann: Anything related to technology falls under my umbrella, including external computer consulting, internal IT and payroll software development. I also provide technology management for our financial services company, Honkamp Financial Services.

***ITU:** How do you leverage your technology knowledge to pass on this information to your clients?*

NH: I do this by taking the experience of working with many different kinds of businesses and combining it with education from seminars and the annual AICPA's TECH conference, as well as networking with others in the industry. When we begin to work with our clients, we evaluate where they are with regard to using technology and what they to accomplish in the long-term. We then use technology applications and processes to make them more efficient and get the information they need to grow their business.

My firm's group of outside consultants focuses on the application side. We are a SAGE MAS 90 and MAS 200 reseller and master developer. We're selling, installing, implementing and customizing these products to automate businesses.

We also get involved with clients in cases where they have existing software and want to make better use of what they have. They don't want to switch systems, so when we walk in, we look at their processes and review the situation, using our accounting and technology knowledge to help them be more efficient.

***ITU:** Over the last several years, what three technologies have been important to your firm?*

NH: Security, first. Because of our firm's payroll business, we are SAS 70 certified, and through the certification, we have to make sure all of our security is updated. Technology has gotten a lot more complicated than in the past, but you also have to make sure everything is more secure. We are locking everything down appropriately.

Second, paperless processes. We've been handling paper the old fashioned way with PDFs and directories, but now we are moving toward becoming paperless and are building the infrastructure to support this. For us, we'll be able to work from anywhere, any time. From a disaster recovery perspective, we will be able to recover everything. Today, with paper files, if there were a fire, all of our documents would be gone. We don't have hurricanes in Iowa, but in light of seeing Katrina and the mass destruction that occurred, it does make you wake up and realize that something like complete destruction could happen very quickly. Also, as we have grown and need space in our building, we have less room for storage.

Natalie Hoffmann, CPA.CITP

Along the lines of paperless, we also want to add a client portal to enhance our interaction with our write-up clients. This will make it quicker and easier for a client to access their reports and to send us their data files to import. The focus is on automation and streamlining processes as much as we can to minimize manpower and avoid duplicating effort. For example, we have customized MAS 200 to

Continued on page 10

ITU Profile - Natalie Hoffmann *continued from page 9*

interface with our clients' banks in order to perform an automatic bank reconciliation.

The third technology is a process more than an actual technology, and that's Business Continuity, with more a formal, written, structured plan. This is a major focus. And, once you test the plan, you do not realize the steps you missed.

ITU: Last year's Top Technology was Information Security, and as of press time, we have yet to finalize the 2007 list. Do you predict this will once again be at the top of the list, and if so, why?

NH: Yes – I think it will once again be the number one technology. Security is on the top of the mind for *everyone*. With all of the viruses, hacking and related stories, and with all of us depending on the Net and using it day-in, day-out, I think this usage exposes us to even greater potential risk. Plus, the usage of wireless can expose us to increased risks.

ITU: If you were stranded on a dessert island with only one technology gadget, application or process, what would it be, and why?

NH: I'd have to say that I would have to have batteries; what good are gadgets if they run out of power? ●

E-BITZ

E-BITZ focuses on practical applications of various technologies to enhance a practice or business. Her columns in 2006 focus on "Honorable Mentions" in the 2006 Top 10 Technologies Program.

E-BITZ WITH SUSAN BRADLEY

Technology as an "Outsourced" Warm Fuzzy

"Can I call you back in an hour? Our computer systems are down." "Oh, I'm sorry, may I put you on hold; my computer is acting up right now." "Our system is down, may I call you back?"

You've heard every one of these excuses and you've even probably given a few of them yourself. It's about technology and how it … or rather "IT" (information technology) *doesn't* do it. What if you did not have to deal with "IT" anymore and let someone else handle "IT?"

In the technology consulting industry, companies calling themselves "Managed Services Providers" are, in reality, doing exactly what they've done for years – being the outsourced Chief Technology Officer (CTO) for an accounting firm. In this day and age in which we live and breathe technology, we need to ask ourselves – in trying to do it all, including our own internal IT – if this *is* the right thing to do.

As fast paced as technology is moving, keeping up with "IT" is getting harder and harder, but our needs for secure, dependable solutions are not decreasing. Perhaps we need to step back and ask ourselves if we truly have the staff and resources on hand to do right by our firms and client base. For a smaller firm that focuses on accounting technology, do we also have the resources to best manage our own internal technology?

Our needs to build our businesses around secure, dependable solutions are increasing. We need to ensure that we see our technology as a "warm fuzzy" or an investment, rather than a beast of burden and a cost center to our firms. I recently spoke with two companies, Evolvetech and Mobitech, about how they manage the technology for their clients, and asked the leaders of both companies if a CPA firm should always assume that just because we depend so much on technology, we should be the best judge of solutions for our own firms.

"Technology experts use accounting software in their firms on a daily basis; are they qualified to do their own taxes?" asks Dave Sobel, head of Evolvetech (*www.evolvetech.com*) in Fairfax, Va. The changing landscape of technology means that keeping up with a technology infrastructure is indeed a full-time job for his company and Amy Luby's as well. Amy is head of Mobitech (*www.mobitechonline.com*) in Omaha, Neb.,

Continued on page 11

E-Bitz with Susan Bradley

continued from page 10

an organization focusing on solutions for small- and medium-sized businesses. Dave and Amy see that while CPA firms have unique needs, each industry has its own particular challenges.

For example, while CPA firms may fall under specific rules and regulations for data handling, Amy states, "We approach all of our clients with the same high-level security solutions because we take security very seriously, whether our client is a CPA firm, a group of attorneys, a cleaning company, real estate firm or anyone else."

Dave sees that the power of technology matches a solution to the right problem. As he monitors firms that have similar problems in different industries, he can build "best practices" from the body of knowledge that naturally occurs.

In conversations with Dave and Amy, both stressed that the key need for CPA firms includes a well-managed, solid infrastructure that assists the business and is not a cost center to the firm. CPA firms need to centralize and secure their data, communicate better with clients and work from anywhere. Both Amy and Dave use a combination of technology and client education to ensure data security.

Their services, while providing a firm with a comfort factor, still need to start on the basis of trust and an agreement. Just as CPAs provide engagement letters to clients, you also should ensure that you have a written understanding with your technology consulting firm that provides you with managed support. The AICPA, in fact, requires such an understanding in its ethics rules as explained in an article from The Outsourcing Institute (*www.outsourcing.com/content.asp?page=01b/other/oe/q105/aicpa.html&nonav=false*).

We typically think that such an understanding is only needed if you send client data overseas. The AICPA understands that these types of arrangements mean that you have a trust relationship with another firm and need assurances from the firm that it has the policies and procedures in place to reasonably assure the proper handling of the sensitive data.

"Remote management is always done via secure methods, ensuring that access to data is protected and only available to those authorized to do so," says Dave, who indicated that his firm's handling of confidentiality and security is paramount to his clientele.

Mobitech understands the needs for secure solutions to its small business client base. Amy explained the process her firm uses to ensure security: "We take security very seriously and always approach security by providing as many layers as necessary. Generally, for our CPA firms, the (Microsoft) Small Business Server Premium's ISA firewall is a *must* for providing a layer of security for these firms. We will couple that with a business-class hardware firewall, complex password policies and end-user education to provide as many layers of security as possible."

For many small CPA firms, having someone on staff full time to ensure the firm stays up to date with technology and remains ever vigilant would be cost prohibitive. However, hiring and outsourcing this role means that such a standard of care can, and typically does, place small firms that use managed service providers for their technology needs at a higher level of security and efficiency than large firms that try to attain "best practice" goals.

"Our role as a technology advisor is of key value to a CPA firm," says Dave. "As a managed service provider, our capabilities range from CTO to field technician – roles that a CPA firm would have difficulty filling in a cost-effective manner. As a partner, our success is tied to *your* success; we are always working to find more ways to deliver solutions and business value to make you more money, more efficient or reduce your costs."

AICPA
Top Technologies 12
Outsourcing

Hiring an outside resource to perform all, or portions, of an organization's internal IT support, transaction processing, application support or special projects.

Continued on page 12

E-Bitz with Susan Bradley *continued from page 11*

So what's the real value in outsourcing? Both Amy and Dave say that being able to focus on your strengths and allowing you to grow your business, rather than worrying about trying to keep up to date on the latest technology strategies, is *the* key value. Both are leaders in the IT industry and travel to key industry conferences to maintain this cutting-edge philosophy that they bring to their firms.

If you are an accounting software implementer, you can even consider partnering with your managed service provider to offer a joint service to your client base. Strategic partnerships between managed service providers that ensure the technology backbone of your clients' firms are stable and controlled. Combined with your role as accounting technology implementer, they can be a perfect fit for both of you. Bringing stable, secure solutions for the technology and the accounting infrastructure for you and your clients can be a "warm fuzzy" for everyone.

Susan E. Bradley, CPA.CITP, MCP, GSEC, is a principal with Tamiyasu, Smith, Horn and Braun in Fresno, Calif. Contact her at *sbradcpa@pacbell.net.* Note that the opinions expressed here do not reflect an endorsement or recommendation from AICPA.

AICPA IT Section

American Institute of Certified Public
Accountants
Information Technology Section
201 Plaza Three, Harborside Financial Center
Jersey City, NJ 07311-3881

ISO Certified