

## Meet CFUS



Joseph C. (Joe) Hibbitt  
Principal, President  
Los Angeles, California



Manny Mangahas  
Principal, VP—East Coast Operations  
Clifton, Virginia (Washington DC)



Burnie Reed  
Principal, VP—Midwest Operations  
Dallas, Texas

## CFUS Update!

**Industry: Manufacturing**

**Service: Database Application Development**  
**Technology : Oracle**

Converted legacy financial systems to a centralized custom Accounts Payable system. Coordinated with multidepartment representatives to ensure a transparent rollout.

**Industry: Education**

**Service: Application Development**

Developed migration strategies from current client/server reporting application to a web-based portal. Setup standards and procedures for backup and disaster recovery

## Use a VPN to Increase Small Business Productivity

As workforces get more and more decentralized and telecommuting becomes more widespread, businesses of all sizes have come to depend on virtual private networks, or VPNs. A VPN is a secure, private network that runs on a public network (usually the Internet). VPNs can allow remote workers secure access to your network, just as if they were at their desks in your office. If you or your employees are routinely away from your office and need access to your company's network, a VPN is an inexpensive way to increase productivity — without sacrificing security.

The name "virtual private network" gives you a clue about how VPNs actually work. VPN software programs "carve out" a section of the Web, and allow only authorized users to access it. This virtual network runs on top of an existing network and

is private. Hence the name.

Users who provide the correct login information are granted access to the VPN gateway at the office. Once they're connected through the gateway, they can access the network just as if they were at their desks — reading and sending e-mail, opening and storing files, or working on specific local applications.

To create a secure link between a mobile user and the network, you need a **VPN client** and a **VPN gateway**. The VPN client is a software application that's installed on the mobile computer of the remote user, and the gateway is a program or computer on the network end that lets in authorized users and keeps out unauthorized ones.

To provide additional security, the client encrypts data before it

sends it out, and the gateway decodes it once it arrives. This communication between client and gateway is known as tunneling.

Even a one-person company can reap the benefits of VPN technology. Both Windows Server and Windows XP have built-in VPN capability, so if your LAN runs on Windows Server, it's just a matter of enabling and configuring the VPN features. That's easier said than done, but you don't have to be a computer science major to do it, either.

Of course, there are many non-Microsoft alternatives, too — many designed for the home PC user. Many firewall applications also come with VPN capability, as a VPN gateway is very similar to a firewall. Both let trusted traffic in and keep intruders out.

## Technology Implications of Sarbanes-Oxley

Corporate America is currently facing major government-mandated change as a result of the Sarbanes-Oxley Act (Sarbox). While the act requires

near real-time reporting and companies to continually evaluate their financial controls and regulatory compliance, it is not explicit as to the technology

requirements and information technology (IT) solutions. In fact, Sarbox does not mandate any technology; however, it is difficult to envision compliance

without IT implications. Most companies will need to create an IT infrastructure for rapidly assessing and reporting critical events that materially impact a company operations and financial reporting.

Sarbox compliance may cause companies to examine and potentially redesign all of their financial business processes and supporting technology solutions. Convergence, simplification and centralization of information will be keys to compliance. Companies that lack records management (RM) processes risk legal troubles when disputes arise. A RM process evaluates documents for their fiscal, legal, operational and historical value and minimizes risks by periodically destroying unneeded items.

Many companies do not have good internal controls, especially when it comes to e-mail, content management and processes. The ramifications, especially in light of Sarbox and related rules, are now magnified. Gartner, Inc. estimates that by 2005, 90 percent of information that is not explicitly stored and managed by RM systems will be potentially recoverable using business continuity or forensic analysis tools, even if efforts are made to delete it. Compound this with the proliferation of e-mail at work and you have the potential for huge risk exposures. Improper destruction is a significant risk which can trigger a material weakness and criminal penalties. Companies should seek legal counsel in building retention guidelines and check with their internal auditors regarding materiality thresholds.

Three of the 66 sections of Sarbox have implications for content, document and processes technologies. Section 302 explicitly puts the accountability burden on chief executives with hefty fines and criminal ramifications for material financial misstatements. Section 404 requires companies to document financial reporting controls in great detail and create a system to monitor and test effectiveness. If management misses, or fails to correct, a material weakness, the company's external auditor is obligated to report it, which then becomes a matter of public record and a potential public relations nightmare for the company.

While section 302 received the most attention when Sarbox was enacted in July 2002, it is section 404 that is now receiving the most attention as compliance deadlines begin this June. However, it is section 409 which could trigger the most attention towards technology since it requires near real-time reporting for material events. This section has received little attention to date since the SEC has not yet decided upon final rules or implementation dates.

Many companies have gaps in their internal financial controls and relating technology processes. While Sarbox will not be the last piece of regulation corporate America faces, it is likely to remain significant, especially for those companies who report to the SEC.

Here are some best practices to consider when looking at technology options relative to Sarbox:

- Assess paper and electronic RM policy along with technology options relative to

government mandates as well as competitive best practices.

- Look at initiatives to merge content management (trusted repository, security, eSignatures, e-mail archiving for example) with process issues such as monitoring, documentation and auditable workflows. Enhancing content management capabilities can open up efficiency opportunities as well as strengthening controls and collaboration efforts. XBRL (eXtensible Business Reporting Language) is likely to become the standard in facilitating content integration.

- Enforce a standard approach to documentation and workflow to ensure accuracy of information and continuity across the organization.

- Establish a central repository for data. Data must be easily accessible and fully searchable by executives and auditors.

- User cooperation is vital for any RM program. All employees must be made aware of the importance of record keeping and the consequences of not complying with a RM program.

- Categorize e-mail based on content and apply retention rules per corporate counsel advice.

- Be skeptical of standalone or Sarbox specific solutions. Utilizing non-integrated systems can be costly from a training standpoint as well as not providing the flexibility of enterprise-wide solutions.

## Being Fit — Even Moderately— Cuts Stroke Risk

NEW YORK - Being merely moderately fit — walking briskly half an hour a day — can lower the risk of having a stroke, according to a new study whose findings apply to women as well as men.

Much of the previous research on stroke and

fitness has been on men and relied on participants to report their physical activity, said Steven Hooker, who heads the University of South Carolina's Prevention Research Center in Columbia and led the study. About a quarter of those in the new study were women, and everyone had a treadmill test to measure

his or her fitness level.

"It seems that benefits we've been observing in men for many years ... are also observed in women," Hooker said.

He said even those who were moderately fit had a lower risk of stroke. Most people can reach that fitness range by walking briskly for 30 minutes a day, five times a week, said Hooker, who presented the findings Thursday at the International Stroke Conference in New Orleans.

Stroke is the nation's third-leading cause of death. It occurs when blood flow to the brain is stopped when a blood vessel is blocked by a clot or bursts. Hooker said physical activity can help prevent blood clots and the buildup of artery-clogging plaque.

For their research, Hooker and his colleagues used data from a study of more than 61,000 adults at the Cooper Aerobics Center in Dallas. After taking a treadmill test, the participants periodically answered health surveys. The latest research divided the group into four levels of fitness and looked at how many of them had strokes, following them an

average of 18 years.

Overall, there were 692 strokes in men and 171 in women.

The study found that men in the most fit group had a 40 percent lower risk of stroke than the least fit men. The most fit women had a 43 percent reduction in their risk of stroke compared with women in the least fit group.

For moderate levels of fitness, the risk reduction ranged from 15 to 30 percent for men and 23 to 57 percent in women.

The lower risks held true even when taking into account other risk factors for stroke such as smoking, weight, high blood pressure, diabetes and family history.

Fitness is "a strong predictor of stroke risk all by itself," Hooker said.

The study's participants were mostly white, well-educated and middle-income or higher; other populations should be studied, he said. Fitness tests were only done when people entered the study so the researchers didn't know if their fitness level changed over time.

In its stroke prevention guidelines, the American Stroke Association recommends at least 30 minutes of physical activity of moderate intensity on most days of the week. The new study "is certainly consistent with all of the recommendations that we already have in place," said Dr. Larry Goldstein, a spokesman for the group and director of the Stroke Center at Duke University.

**Contact CFUS (corporate)**

The CFUS Corporation \* 4859 West Slauson Ave. Suite 219 \* Los Angeles, California 90056  
323.298.8502—office \* 310.388.5988—fax \* info@cfus.com \* <http://www.cfus.com>

Story Credits:

<http://www.allbusiness.com/technology/computer-networking-remote-access/3306-2.html>  
<http://wistechnology.com/articles/541/>  
<http://www.msnbc.msn.com/id/23291877/>  
<http://www.bodybuilding.com/fun/sclark16.htm>