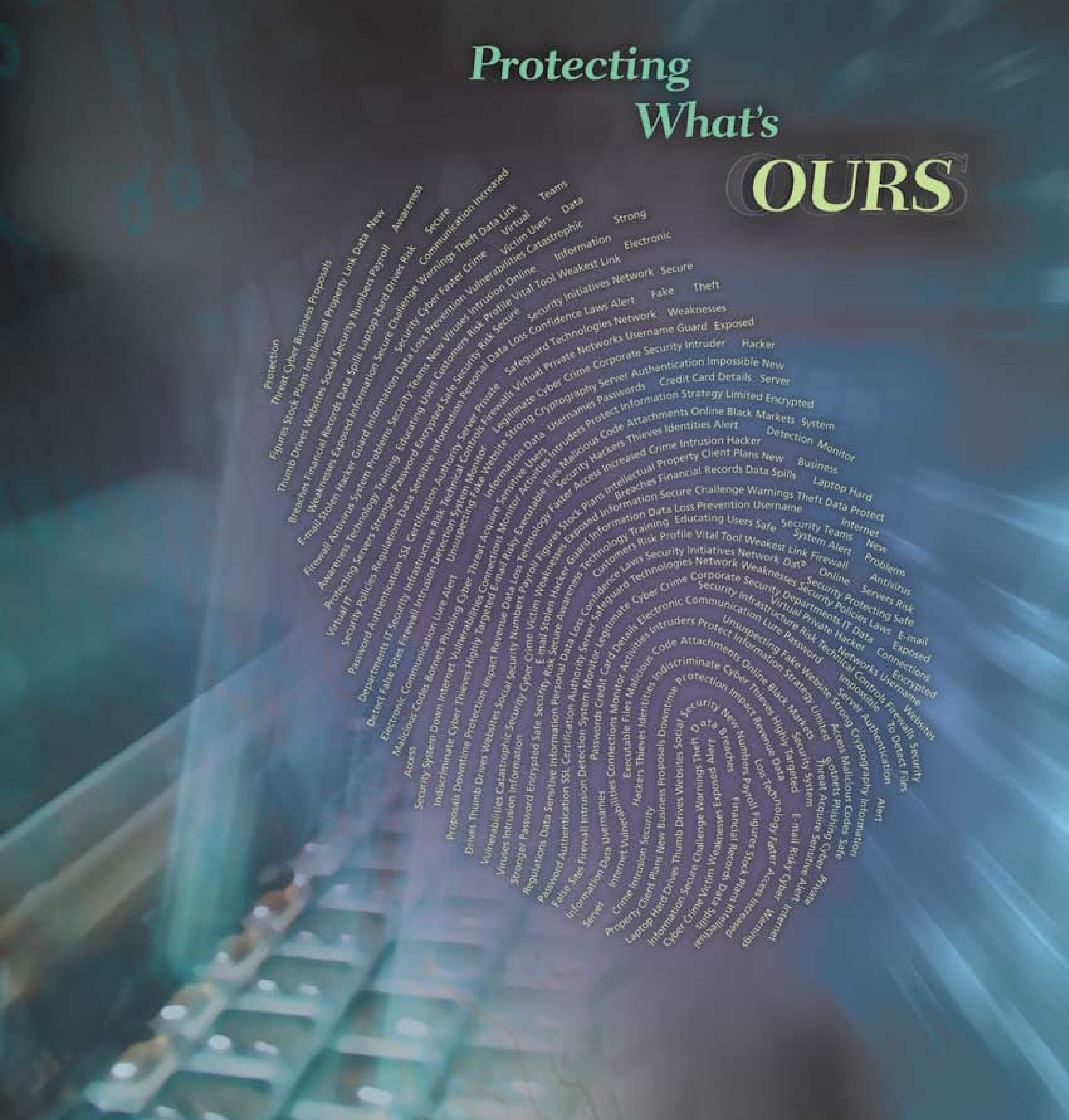
PBSJ

highlights

Fall 2008 | **PBSJ.COM**

Protecting What's OURS



PBSJ highlights

Fall 2008

2

8

10

12

14

CONTENTS

The PBSJ Corporation
John B. Zumwalt, III, PE,
Chairman and CEO

PBS&J
Robert J. Paulsen, PE,
President
Clarence E. Anthony,
Chief Marketing Officer

Editor
Kathy L. Botticello

Contributing Writers
Kathy L. Botticello
Timothy C. Kaiser
Barbara Mack
Lillian L. McAnally
Kelli Pharo
Kathy Pozzi

PBS&J Technical Contributors
Martin H. Brown
Devon S. Chalmers
John M. Finochiaro
Donna M. Huey, GISP
Michael M. Newton
John R. "Woody" Wodraska
Travis N. Reinke
Joe Hurston
Tom L. Boyette, CPP
Joshua P. Price, CFM, GISP
Robert E. Ensor, PE
Geoff Jacobs
Russ Johnson

Design and Production Manager
Rick DeCamp

Graphic Designers
Tilky L. Fernandez
Jenee L. Zaydon
Patrick K. Lockhart

Direct Comments and Inquiries to
PBS&J Highlights
482 S. Keller Road
Orlando, Fl 32810-6161
407.647.7275
800.284.5182
Fax: 407.838.1602
e-mail: 22895@pbsj.com

PBS&J VALUES…

Commitment to Our Clients

Commitment to Our Culture and People

Commitment to Our Company

Commitment to Our Communities and Surroundings

PBSJ .COM

2030 Sacramento General Plan and Environmental Impact Report

PBS&J is the lead consultant in the comprehensive revision of the City of Sacramento General Plan. The new 2030 General Plan is designed to incorporate contemporary planning practices including smart growth and urban infill strategies. It integrates principles of environmental, economic, and human sustainability throughout all elements. These principles define how the public can reduce vehicle trips, conserve energy and water consumption, reduce pollution, and enhance health and quality of life equitably for all residents.

For more on this please see ***www.pbsj.com/2030***

What's NEW

PBSJ FYI

The seasons are changing and so is *PBS&J Highlights*. Our updated look features more white space and gives us room to give you more information. The new format is cleaner, reflects a more contemporary feel, and is more representative of the direction we are moving.

Throughout the issue you will see buttons such as the one next to this column directing you to more online content and additional resources. These buttons will help *PBS&J Highlights* become even more interactive when PBS&J's new Web site debuts this December by directing you to new resources, technology, and more dynamic features.

Change is good. We would love to know what you think of the new look. Drop us an e-mail at 22895@pbsj.com. Enjoy!

Keeping Data Secure

In the Age of Internet Insecurity

Security on the Go

Cell phones, BlackBerrys, PDAs, USB drives (“thumb” or “flash” drives) let you conveniently travel with your data. But theft of mobile computing devices is on the rise, and many thieves admit to stealing not for the pricey device itself, but for the information stored on it. So, securing these devices—and having a record of any sensitive or legally protected data that is stored on them—is vital. Protect yourself and your data:

- Don’t let mobile devices out of your sight, and don’t be showy with your equipment. You risk attracting the attention of potential thieves.
- Write down make, model, and serial numbers or add a tamper-proof, bar-coded plate on the back that leaves a permanent indicator if it is removed, marking the device as stolen.
- Increase the physical security of devices by investing in a cable lock, beaconing software, lock boxes, or BIOS settings. Any of these improve physical security and deter theft.

The week leading up to September 11th annually is Global Security Week, and this year’s theme was “Cyber Crime—Don’t Become a Victim.”

Did you notice?

Chances are, you didn’t, because according to a 2006 Computing Technology Industry Association security report, “The person behind the PC continues to be the primary area where weaknesses are exposed.”

In 2007, no less an expert than Bill Gates, speaking to an annual gathering of 15,000 computer security experts, said: “Keeping information secure in this age of laptop-lugging workers is the tech industry’s most formidable challenge.”

The numbers for 2008 show the problem continues to grow despite the big names behind the warnings.

The San Diego-based Identity Theft Resource Center said it tracked public reports of 167 data breaches in the first quarter alone of 2008. (The center recorded 448 data breaches in 2007.) At least 8.3 million personal and financial records of consumers were potentially compromised by data spills or breaches at businesses, universities, and government agencies, according to its statistics.

Overall, businesses were responsible for roughly 36 percent of the data breaches or spills, followed by schools and universities (25 percent), government and military (18 percent), medical/health care (14 percent), and banking and financial (7 percent).

Most of the data spills in the first quarter of 2008 appear to have resulted from lost or stolen laptops, hard drives, or thumb drives. Insider access and the inadvertent posting of sensitive data to a Web site or through e-mail also were cited frequently throughout the report.

While some businesses—financial and retail, for instance—house such sensitive information as credit card numbers or bank balances, any company that employs people harbors valuable personal information like social security numbers, payroll figures, and stock plans. In addition, especially for professional services firms like PBS&J, there’s the question of intellectual property. “Client documents or new business proposals are the firm’s counterpart to a retailer’s listing of credit card numbers,” says PBS&J’s Marty Brown, chief information officer, “but protection from an intangible like downtime is important too. If we have to shut a system down due to a possible intrusion, it could have a considerable impact to our revenue. That’s as significant as data loss.”

It’s a fact that the benefits of technology—more information stored, with more people given faster access to it, boosting the nation’s productivity exponentially—have also increased the incidence of crime. Alarmingly, the nature of intrusion has changed, too.

Hackers Become Thieves

“A big shift is occurring,” said Brian Foster, vice president of product management for Symantec Corp., at a recent Educause/Internet2 conference for computer security professionals. “Hackers are becoming thieves, and everything from intellectual property to identities is being stolen in record numbers. Whereas the first breed of hackers was motivated by fame,” he explains, “today’s are financially driven.” “Hackers were highly visible, indiscriminate, and had only a few named variants. Today’s cyber thieves are silent and highly targeted.”

According to Symantec’s statistics, companies and organizations today send more than 70 percent of their intellectual property through e-mail, which is risky, considering that 40 percent of all malicious code trends deal with the sharing of executable files and 32 percent with e-mail file attachments. “Stolen information is then sold through online black markets to the highest bidder,” said Foster.

“Fending off the wiles of intruders while accommodating the needs of users is the challenge of any chief technology officer,” said John M. Finochiaro, PBS& J’s chief technology officer. “We look at things holistically,” he says, “and in that context, try to determine what levels of security to put up. Things like viruses will take systems down, and the Internet opens up a host of vulnerabilities. Because we have so many Internet connections—sites, as well as people accessing them—we have to run a thin line between what people should do and can do. Tools will monitor our systems’ activities, but because the Internet opens the door to so many intruders before the tools can go to work, we protect the company’s information with a ‘deny first’ policy. Access is limited, until an individual shows a need for specific information.”

The Ways In

If Finochiaro needs evidence to support that strategy, he need only point to the Department of Homeland Security (DHS). According to that agency’s statistics, more than one million malicious codes have been written, an increase of 500 percent, since 2007. On any given day, 40 percent of those codes are “botnets”—a collection of software robots, or bots, that run autonomously and on groups of “zombie” computers controlled remotely. In fact, says DHS, more malicious code is written than regular code—and more than 80 percent of organizations affected by botnets are not aware they’ve been compromised.

That code most frequently enters a company through phishing, “a very powerful, common cyber threat,” says Brown.

A good definition of the term is offered by Wikipedia: “Phishing is the process of attempting to acquire sensitive information such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication.” Communications purporting to be from popular social Web sites (YouTube, Facebook, MySpace), auction sites (eBay), online banks (PayPal)—or even IT administrators (Yahoo, ISPs, corporate)—are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake Web site whose URL, look, and feel are almost identical to the legitimate one. Even when using secure sockets layer (SSL) with strong cryptography for server authentication, it is practically impossible to detect that the Web site is fake.

Phishing has been phenomenally successful because “people are more trusting than you would believe,” avers Brown, “and most individuals are not trained to identify false sites or mischievous Web-based activity once it finds a way through a firewall.

“That’s why,” he explains, “intrusion detection systems are an important tool in a holistic approach to security. Firewalls were the first defense against external attacks. Now we have to monitor whatever gets past, to determine if it’s legitimate.”

A reflection of the new sophisticated cyber crime is the attention being paid to corporate security. “Ten years ago, there were few security departments,’” says Finochiaro. “PBS&J, as one example, today has a security department of four full-timers. The majority of companies have a dedicated staff, because business recognizes that somebody has to be in charge.” Finochiaro estimates that security accounts for about 10 percent of his IT budget, including systems and people.

Take Steps to Protect

For any organization considering improving security, the basics have been established. Here's what PBS&J's Devon Chalmers, technology controls manager, recommends for the security manager:

1. Assess the organization's security infrastructure. Look at the operational aspect of the organization, clarify how business is being accomplished, and see where there is risk.
2. Start building processes and procedures to bridge the gaps and remediate risk.
3. Develop a plan of action and prioritize tasks based upon the immediacy of the issues.
4. Depending on findings, develop and implement policies and processes to standardize the organization's threat posture.
5. Begin to work on new processes and standards, because security is ever-evolving.

Chalmers believes that most organizations have the basics down in terms of technical controls—firewalls, virtual private networks, username/password authentication, SSL, certification authority server, to name a few—"but a lot of work needs to be done on policy-based controls and standardization. The security landscape changes every day, and rules and guidelines need to be continually adjusting."

Organizations should not allow technology myths to cloud their judgment. Joanne VanAuken, a technology writer based in Syracuse, NY, has researched some of these myths:

Myth: Organizations are more secure now than they were a year ago.

Fact: Most companies have initiated the necessary steps to safeguard their company assets. However, new threats and technologies are constantly changing. System administrators must scan the network continually for known security weaknesses, keep their skills current, and, most important, re-examine security policies periodically. Business processes defined a year ago may not match the organization's current needs.

Myth: The presence or absence of regulations matters greatly when it comes to protecting customer data.

Fact: With or without a legal requirement, organizations should still safeguard their sensitive information. Failure to protect customers' personal data means a loss in consumer confidence, which results in lost revenue and government fines. Regulations and laws, such as HIPPA and Sarbanes-Oxley, are forcing executives to invest in information security initiatives, but don't be misled into thinking regulations mean data is protected.

Myth: External consultants know more about information security than in-house personnel do.

Fact: Network and system administrators often make good full-time security personnel because they handle security problems as part of their daily duties. Required skills may already be in-house, and may merely need some supplemental training. When additional training is not enough, consider using an outside consultant to get a fresh perspective.

Myth: Information security must be managed as a separate business unit to be effective.

Fact: Smart organizations are starting to realize that security has evolved into an enterprise-wide support division, rather than an isolated group dedicated solely to protecting servers. Security professionals can offer cost management, build a stronger focus on customer relations, and help identify and communicate growth opportunities throughout the organization.

Myth: Complex, frequently changed passwords will make an enterprise secure.

Fact: A 16-character password is not easy to guess; it's also hard to remember. Requiring users to change passwords every 60 days, means they'll be writing down their passwords, which is exactly what you don't want. Instead, create a flexible password policy that lets users create simple yet inconspicuous passwords. Written password security policies should be governed by the organization, not the end-user. However, each end-user must be held accountable for managing and safeguarding his or her own password. Passwords written on Post-It notes or stored in Excel spreadsheets are far bigger threats to security than password cracking.

Myth: The padlock icon present during an SSL session means data is safe.

Fact: This is untrue. That tiny padlock icon found at the bottom of a Web site is a sign that data sent between your device and the site is encrypted—it doesn't mean the Web site itself is safe. Moreover, sent-data isn't stored on the Web site, but on a server, and how well an organization safeguards its server is a bigger security risk than the communication transmission itself. Nothing is 100 percent secure, and even sites using 128-bit encryption can be compromised.

Myth: Increased security spending results in greater security.

Fact: This is false. Every company has a unique risk profile that will determine its required security investment. You can't generalize security needs. Instead, establish a risk management profile, manage those risks within a given budget and purchase wisely to meet the needed security level. Security is as much a matter of awareness as technology, so be sure to spend appropriately on training and educating users and customers. It's also vital to make security a visible and important part of your organizational culture.

Perhaps the biggest myth of all is that tools, devices, and procedures are the guarantors of data security. "They're not," says PBS&J technology controls manager Devon Chalmers. "The best security system is an aware and alert employee population. And this is the 'tool' that's most undeveloped."

Cell Phone Security:

- Set a password for your cell phone to lock the phone either after a period of inactivity or at a certain time each night. Most phones allow a user to receive incoming calls and dial 911 for emergencies even when the phone is locked.
- If you must store sensitive data on your phone—banking, medical information, passwords - consider keeping it on an external memory card that can be removed.
- Before you sell or give away your used phone, wipe out personal information in ways that it can't be recovered. Such a process almost always involves overwriting information in a phone's memory with zeroes or other spurious data.
- Some phones, such as the newest ones running Microsoft's mobile software, can be remotely wiped if the phone is lost or stolen. Other third-party software can delete a phone's information if a specially coded e-mail is delivered to it.
- Back up personal information onto your computer in case your phone is lost or stolen.

PDA Security

- **Password Access:** Use a password for switching on the PDA.
- **Wipe Confidential Information:** Software like EmergencyWipe can eradicate confidential information.
- **Content Encryption:** Advanced features, deactivated by default, can protect confidential data. By enabling internal content encryption, you assure that your data is not saved in raw text, which is very easy for hackers to read.
- **Password Encryption:** There is built-in password encryption/storage on the PDA's desktop called "Password Keeper."

The PDA is a continuously running code machine that's always on and always connected to a company's internal network. A hacking program has been developed that exploits the relationship between the PDA itself, a company's internal server, and the network connection to which both are attached. The hacking program works because intrusions can't be detected, since firewalls exist at the perimeter of the network. To protect company data, every employee who uses a PDA needs to take care that the device is secure.

The Weakest Link

As the statistics show, despite heavy investments in firewalls, antivirus systems, and other security technology, security breaches and their ensuing problems are getting worse not better.

So what's going wrong? The answer, according to Gartner Research, is that "80 percent of unplanned downtime is due to people and processes. Internal control is affected by people." For example, one employee opening or forwarding an e-mail virus can shut down internal systems for hours or even days.

Security teams have developed an acronym to describe the problem: PICNIC (Problem in Chair, Not in Computer or Person in Chair, Not in Computer). As Chalmers puts it, "It's incumbent upon me as a security professional to provide end-users with relevant information, but it's incumbent upon the end-user to act on it."

Minimally, security departments can send out routine e-mails to the employee population about new viruses or methods of intrusion. Some large companies have newsletters or posters that are part of ongoing employee education. Chalmers recounts one former employer that awarded prizes—through an employee suggestion program—for the best new idea to enhance security.

"The key is to get people thinking and involved," he says. "Ways to boost information security are all around us, in various formats. An end-user watching CNN or PBS can take the information and bring it to us. The information is there, you just have to go out and get it. With an organized program like a contest, you'll have four or five sets of eyes out there looking."

With a simple e-mail strategy, Chalmers estimates that "you reach the third that's really interested and the third that checks up on e-mail when they have time, and the other third that just deletes it."

What's Ahead

Today's tools—like Loadjack, firmware that's loaded on every PBS&J laptop allowing Chalmers to remotely erase or shut down a machine that has been reported stolen—continue to work well, although for every failsafe device, there's a hacker out there working to outmaneuver it. As a result, new techniques are on the way to guard important company information.

"One hot area is data loss prevention," says Chalmers, where data is protected all the way down to the desktop or laptop. "The industry is working on bridging the gap between people and interested outsiders. Let's say there's a type of document that we know end-users will receive, and they may decide to forward or share that document. We will secure that information all the way down to that machine unless we're able to determine the reason for it leaving the machine. For example, today I can send you a confidential document, and I have no control over what you do with it. You can forward it to any number of folks. With data-loss prevention tools, once I send it to you, that's it, you have no control other than reading it, maybe you can't even print it. With some very basic algorithms and software and end-point security, I can control what you do with it."

But Chalmers' highest hope is for the human factor, "because people do take work home and transfer it to their home computers. Better security really relies upon getting people more involved. Individuals are being targeted now. I really would like to see the day when people are more interested in protecting their private information."

Other experts say that just as humans are imperfect, so too are systems, and that portends for bigger problems.

Ian Angell, a professor of information systems at the London School of Economics, explains this point of view: "Systems are so complex that vulnerabilities are everywhere. The notion of accidents seems to have gone away," with the Y2K nonevent lulling us into a false sense of security. But as systems become more complex and are asked to work with other more complex systems, the chances of something unforeseen—and potentially catastrophic—happening increase, he believes.

What to do? "We'll all just have to live with it."

And in the meantime, the security team will continue to keep fighting the good fight.

> *"It's incumbent upon me as a security professional to provide end-users with relevant information, but it's incumbent upon the end-user to act on it."*

Train Employees Through:

- Informational e-mails
- Periodic "lunch and learns"
- Links to online educational resources
- Fun contests

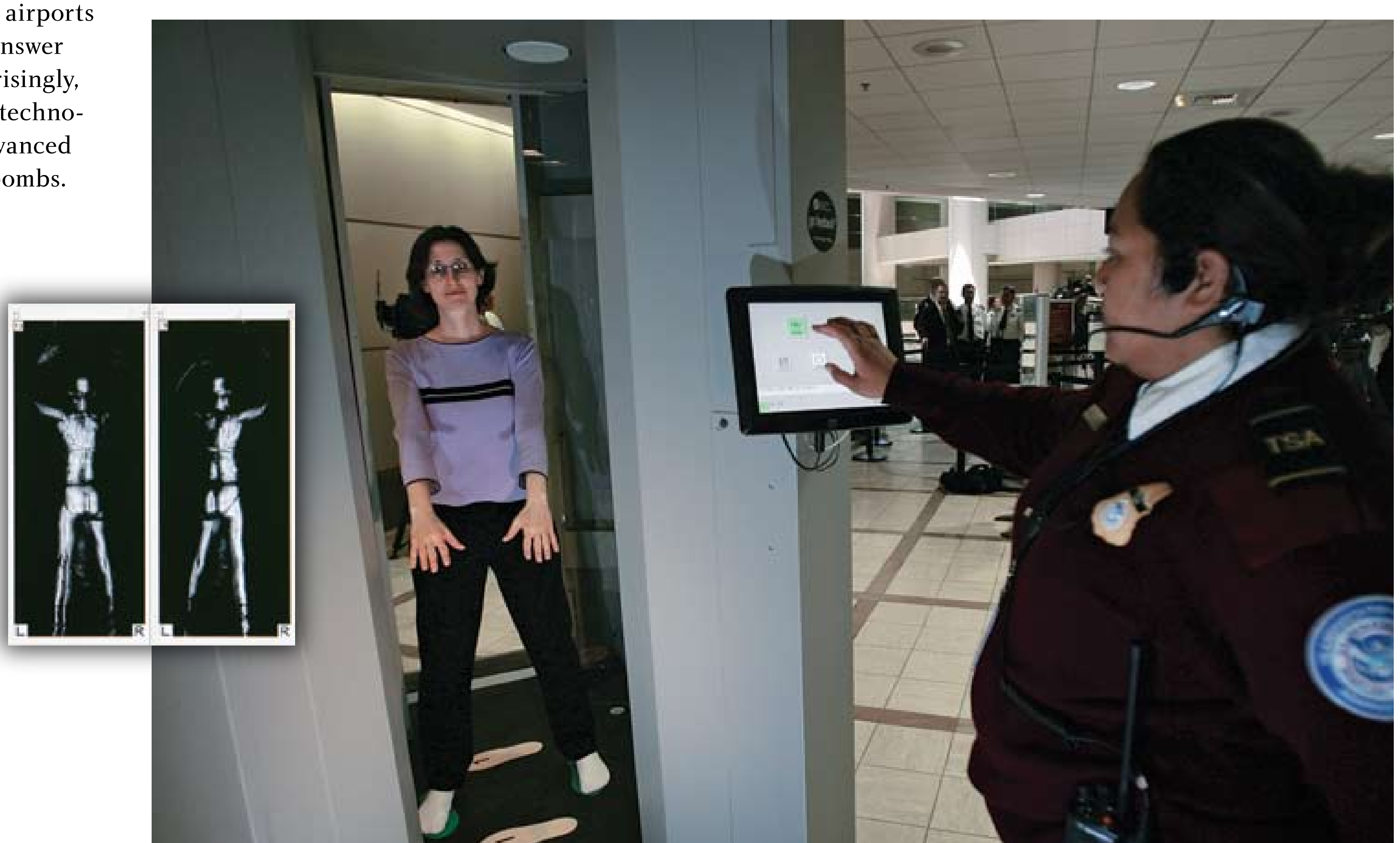
The bottled liquid ban of 2006 was a step toward protecting the flying public. Is there more that can be done?

Aviation Security Trends

Anyone around since the 1960s most likely remembers Tang, that orange-flavored, sugary powder that mixed with water to produce a breakfast drink good enough for NASA astronauts. Fast forward 40 years and Tang is taking flight again, only this time not as part of a manned spaceflight program.

In May of this year a London court reviewed evidence of a 2006 "liquid explosives plot" intended to take down seven planes headed for the United States and Canada. The ingredients of the explosive—hydrogen peroxide mixed with Tang, triggered by flash cameras. With the citric acid in the Tang acting as a catalyst, the explosion was intended to set off a larger HMTD (hexamethylene triperoxide diamine) bomb—made from easily obtained ingredients.

As concerning as it is to hear about this kind of subversive plan, it has become all too commonplace to the flying public since the events of 9/11. So what is being done to protect the public and make our airways and airports safer? The answer is, not surprisingly, much more technologically advanced than Tang bombs.



The Technology

Remember how not long ago you could carry your bottle of Evian through security and onto your flight? While the current bottled liquid ban may not be lifted anytime soon, new technology is being put in place to add one more layer of security in protecting commercial air travelers—bottled liquid scanners.

By analyzing the vapor intake of a bottle's contents, these devices recognize the properties of liquid explosives as they differ from the nonthreatening beverages the traveling public consumes.

And what bottled liquid scanners are to apple juice and spring water, a Cast*Scope* is to prosthetic devices and support braces—implements whose metallic components typically set off standard detectors. The Cast*Scope* uses backscatter x-ray technology to produce a safe, low-intensity x-ray view, as indicated by the radiation that bounces back from a person, as opposed to how it goes through them, as a typical x-ray works. And this technology is being used for more than just the Cast*Scope*. Because backscatter allows security to detect objects carried on a person's body, whole-body imaging systems are being implemented as an alternative to pat-down searches. Both of these imaging systems, while somewhat widely used internationally, have just recently come on the scene in domestic airports.

A similar tool, millimeter wave technology, projects radio frequency energy in the millimeter wave spectrum onto a traveler as they step into a portal. Like backscatter, millimeter wave returns information that displays as an x-ray view in three-dimensions. In 2007 Phoenix Sky Harbor Airport (PHX) was the first aviation facility to test millimeter wave technology domestically, while backscatter technology is being tested at several airports around the nation.

These new security devices are not without controversy, however, as the level of detailed information shared in the images concerns some travelers and privacy rights groups. To help alleviate these concerns, the Transportation Security Administration (TSA) assures the public that the viewing area for the images will be remote, secure, and the images will not be printed, stored, or transmitted.

These emerging technologies, and more, are a part of a multilayered plan to beef up airport and airway security. But are they enough?

A Game of Juggling Priorities and Managing Risk

Securing the nations' airports is a complex problem that extends far beyond the security checkpoint experience air travelers have come to know and dread. The airport screening checkpoint and the associated technology are part of just one of more than 20 layers of security being implemented by TSA to protect airports from, what in reality is, a limited number of threats. Airports, in turn, are just one component of an interconnected transportation infrastructure. Protecting America from terrorist threats and the impacts of natural disasters boils down to a game of juggling priorities and managing risk.

"We need to stop throwing sandbags at the breech in the dike, and assess whether or not the dike is worth saving," says Robert Ensor,senior engineer in PBS&J's Aviation division.

"Now that the initial response to 9/11 is past, government and the private sector need to acknowledge that we can't fix everything at the same time with dwindling, limited funds."

The Airports Council International, in their *North American Airport Capital Development Costs 2007-2011 Report,* estimates that between 2007 and 2011, $87.4 billion, or $17.5 billion per year, is needed to maintain and upgrade the nation's 3,400 airports. Much of this need is unfunded.

Ensor says, "Technology is getting better, and it will continue to improve. But technology only goes so far. As events such as 9/11 have shown us, we have to stop doing risky things and creating vulnerabilities. Now is the right time to put into practice the old adage, 'an ounce of prevention is worth a pound of cure,' and stop activities that create vulnerabilities that then cost billions of dollars to mitigate."

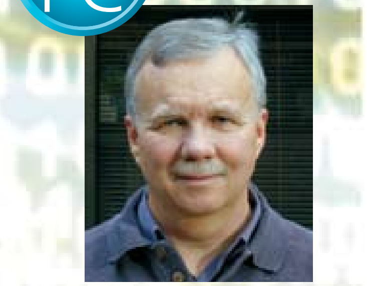
Ensor concludes, "There is some good news. There is a growing need in the area of facility management automated decision tools that can be used to assess risk, and plan and prioritize infrastructure improvements. The area of Geographic Information Systems (GIS) has great potential as a tool to analyze these complex systems and help government and the private sector make appropriate decisions."

Let's hope that emerging technologies, the funding to support them, and the vision to implement them all align to keep air travel safely on course, and breakfast drinks on our tables, where they belong.

Security in Numbers

Safety is probably not on most of our minds as we enjoy watching our favorite sports teams play in large stadiums and arenas or attend a company meeting at the city convention center. One of the reasons we can participate in these events without worrying about security is because of the prevalent use of spatial data in security planning. Spatial data is an inventory or database representing the assets that define a particular location and the characteristics of specific focal points. This information essentially provides us with the "where" and the "what" for security planning purposes. When this spatial data is contained in a Geographic Information System (GIS), it becomes possible for us to ask "What if?"

GIS technology determines relationships, trends, and patterns of different spatial data sets using a location as the common key. We are then able to use this information to extrapolate everything from traffic patterns during rush hour to event attendance and appropriate allocation of resources for event security and safety. And as the databases become populated with even more information and spatial data is referenced before, during, and after events, organizers can plan for and react to previously unforeseen happenings.



Russ Johnson, ESRI public safety and homeland security director
www.contingencytoday.com

Russ Johnson, public safety and homeland security director at ESRI, provided details on the various aspects of how GIS can be utilized for security planning at large-scale events.

"GIS technology benefits all aspects of emergency management and event security, including planning, mitigation, preparedness, response, and recovery," says Johnson. "It provides an integration platform that enables every agency involved to work in a coordinated, collaborative fashion."

Spatial data has been employed in support of security measures at events ranging from the Super Bowl to national political conventions and even presidential inaugurations. In 2005 PBS&J assisted the Mid-America Regional Council in how to best leverage spatial data across an eight-county region to support safety and security. In fact, hazardous materials accidents on roadways was cited as one of the larger safety risks in the region. The ability to use GIS for tracking chemical storage information, understanding roadway networks, and overall conditions and patterns enables quicker and more effective response to an accidental spill.

According to Johnson, "The challenge is to be proactive and diligent well before an event occurs. Preparing security well in advance of an event gives homeland security professionals and others the best chance to provide optimized protection and response capability." (To read Russ Johnson's article, "Geographic IT for Emergency Management and Event Security," visit ***www.contingencytoday.com***).

Just Scratching/Scanning the Surface

While employing GIS capabilities for security purposes may sound futuristic, we are just beginning to scratch the surface on how spatial data can be used in security planning. Or in the case of High-Definition Surveying (HDS), we could say "scan the surface." As GIS has given us a unique way to interpret spatial data, HDS is offering a safer, faster, and more detailed way of gathering it, while also providing new options and potential applications for security planners.

HDS or three-dimensional (3D) laser scanning rapidly collects detailed and accurate as-built data using a narrow eye-safe laser beam that "sweeps across" a target object, such as a bridge or building, gathering millions of closely spaced measurements in minutes. This nonintrusive method of data collection means HDS can be used in locations where operations must go unimpeded or where safety is an issue for example at a busy intersection, or in areas that are very detailed and difficult to measure like a machine room in a busy factory.

Scanned measurements are collected and grouped into compressed "point cloud" databases that can be manipulated on standard computers and displayed as dense representations of objects. This data can be viewed, navigated, and analyzed much like a 3D-model created in a traditional CAD system.

PBS&J has employed HDS technology to help develop security measures for the City of Atlanta's Department of Watershed Management. Security designers analyzed HDS scans of water and wastewater treatment plants to determine precise security camera placement. The data also provided detailed information on facility entry location and sizes for use in further threat analysis and security planning and design. "The ability to use point cloud data for view-shed/inter-visibility/line-of-sight studies to establish precise camera placement in order to secure vulnerable assets proved to be a significant benefit for Department of Watershed Management and the design team," commented Travis Reinke, PBS&J's national HDS project director. "In a time of heightened national security the use of tools such as 3D laser scanning to rapidly collect detailed 'as-is' conditions data is invaluable."

HDS technology has not yet been fully integrated for use with GIS or GPS, but Geoffrey Jacobs, a senior vice president with Leica Geosystems, developers of 3D scanners, foresees a day when the GPS system in your car will have a 3D representation of your route and final destination, offering a more interactive experience than with the typical 2D map displays.

Additionally, Jacobs thinks HDS will be a future complement to Building Information Models (BIM) that could utilize the scanned data to determine the placement of fire sprinklers or safety ladders.

"One of the drivers for BIM is for the increasing need to effectively address security planning for buildings," Jacobs wrote in an April 2006 edition of *Pro Surveyor* magazine.

We've come a long way from the days of of the backseat driver trying to interpret the newest Rand McNally (that's a roadway map for everyone under the age of 25) with the driver still insisting, "We're not lost." These days in our vehicle glove boxes, center consoles, or dashboards, maps have been replaced by GPS (global positioning systems) that tell us when we're lost or "almost there" depending on the driver. Not only has the use of spatial data given us an automated means to find our way home, but it is helping to make the world outside our homes more secure.

Building Information Modeling (BIM)

Building Information Modeling (BIM) is the process of generating and managing building data using three-dimensional (3D), real-time, dynamic building modeling software. The process produces a Building Information Model (also abbreviated BIM), which encompasses building geometry, spatial relationships, geographic information, and quantities and properties of building components.

BIM can help decrease errors made by design and construction teams by allowing the computer to inform team members about parts of the building that may be in conflict. The resulting error reduction can translate to cost savings and reduction in time required to complete construction. BIM can also be used in conjunction with HDS technology to improve building security features by determining the best placement for fire sprinklers, emergency exits, or security cameras.

In 2003 the General Services Administration (GSA), through its Public Buildings Service (PBS) Office of Chief Architect (OCA), established the National 3D-4D-BIM Program. OCA has led over 30 projects in its capital program, and is assessing and supporting 3D, four-dimensional (4D), and BIM applications in over 35 ongoing projects across the nation. The power of visualization, coordination, simulation, and optimization from 3D, 4D, and BIM computer technologies allow GSA to more effectively meet customer, design, construction, and program requirements.

PBS&J recently used a 3D laser scanning technology to collect detailed information for a hanger facility at the Roosevelt Roads Naval Station, a retired naval base on the eastern shores of Puerto Rico. The technology was able to capture data for every square inch of the 50,000-square-foot facility, including multiple offices and a large hanger bay, in less than 12 hours. From this data PBS&J was able to extract and tag every receptacle, outlet, sprinkler head, and light fixture in order to populate the detailed BIM. The data was not only used for asset management, but also renovation, retrofitting, and design.

When the Well Runs Dry

What are we doing to keep our water supply safe?

An old Scottish proverb says, "We'll never know the worth of water till the well runs dry." Water is essential to our survival. But with triple threat of bioterrorism, natural disasters, and dwindling funding/rising costs, delivering a safe water supply to customers has become more challenging than ever.

Environmentally-Safe Alternative

Chlorine, although cheap, is becoming less desirable to use in treating water, which is forcing officials to look for alternative means. The Department of Homeland Security (DHS) has identified chlorine gas transportation and storage as one of the top domestic terrorist threats. The owner of the Vortex Voyager, Vortex Pure Water, in cooperation with the University of Arizona's Water Quality Center, has spearheaded a project funded by DHS to develop chemical-free water purification technology for municipal use, which could significantly reduce or eliminate the nation's dependency on chlorine as a primary water treatment disinfectant.

Keeping Terrorism at Bay

When Congress passed the Bioterrorism Act in 2002, the U.S. Environmental Protection Agency (EPA) was charged with making sure utilities performed security vulnerability assessments and had an emergency response plan in place.

Earlier this year, the EPA granted $8 million to the City of San Francisco for a pilot program to develop and evaluate a drinking water contamination warning system for its drinking water supply. The contamination warning system involves online water quality monitoring, public health surveillance, sampling and analysis, enhanced security monitoring, and consumer complaint surveillance.

Our neighbor to the north is following suit. In the Canadian province of Newfoundland and Labrador, the Department of Environment and Conservation allocated approximately 75 percent of the FY 2008 budget be spent over the next two years for water safety. Within the Department of Municipal Affairs, another $6 million annually will be earmarked toward investing in infrastructure.

Disaster Preparedness

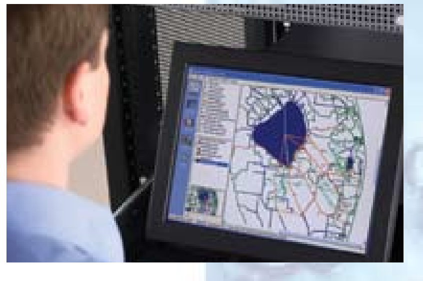
In May 2008, when the cyclone Nargis devastated the country of Myanmar, Floridian executive, Joe Hurston, went on a missions trip to deliver water purifiers to remote villages. Hurston, owner of Cartridge Source of America (CSA) in Titusville, Florida, manufactures printer cartridges and manufactures the Vortex Voyager®, a water purifier that uses ozone and ultraviolet light to destroy microorganisms and oxidize chemicals.

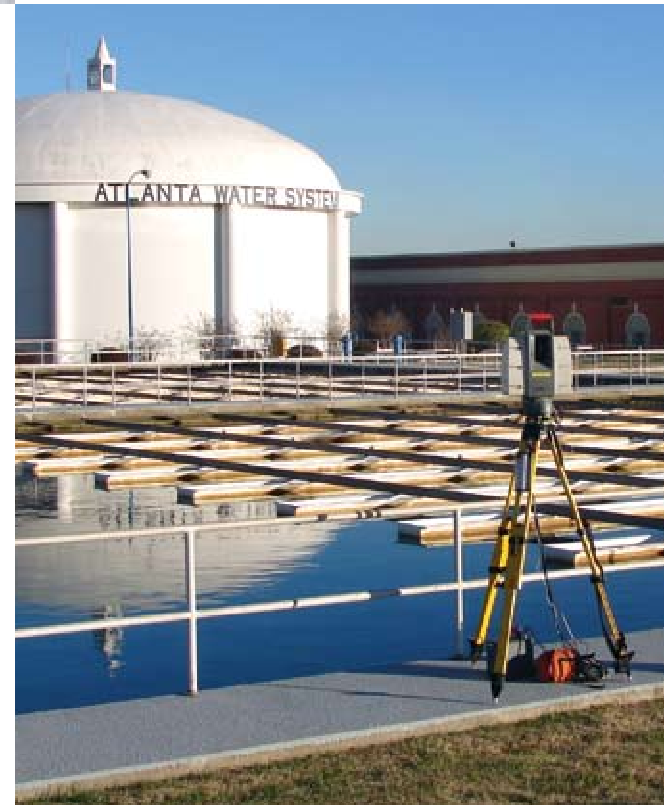
Through his nonprofit organization, Air Mobile Ministries, Hurston flies to disaster areas, donating the water purifiers to relief organizations in places like New Orleans, Haiti, the Dominican Republic, and Indonesia.

Years ago Hurston shared a simple idea with his friend, engineer Rolf Engelhard, inventor of the Vortex Voyager: bring potable water to remote or disaster-devastated areas. According to Engelhard, the filter can pump water from unsanitary freshwater sources such as a pond or a ditch, and turn it into potable, drinking water. No bigger than a backpack, each unit purifies about 30 gallons per hour, costs $1,500 to manufacture and takes about 20 hours to build. It also is equipped with multiple power options, including solar and battery capability.

Balancing the Cost vs. Funding Equation

Let's face it: supplying the public with safe drinking water is expensive. One of the biggest O&M challenges of water security is the cost of keeping up with technological advances. While most utilities have invested heavily in GIS (Geographic Information System) and SCADA (Supervisory Control and Data Acquisition), an industrial control system, to help improve facility security, there is still a need for a tool that helps support management decisions.





In his upcoming book, *The Future of Water*, John "Woody" Wodraska, national business sector manager for PBS&J's Water service, offers an alternative view of water management software. "Within the water industry and other utilities, however, most people agree that investments in GIS and SCADA have paid off. Yet these mapping and data collection tools have not eliminated the need for an experienced staff to review the data and make decisions about managing resources, building new facilities, or improving old infrastructure," explains Wodraska.

Wodraska and PBS&J senior project manager Kathleen O'Neil are managing sponsors in the development of a Dynamic Decision Support System for Integrated Resource Planning tool—D^2S^2 for short—that provides simulation and what-if scenario testing of water resource alternatives, giving decision makers a quantitative way to incorporate and communicate the uncertainty inherent with resource decisions. The tool also integrates regulatory constraints, financial costs, and demographic trends.

Despite the fact that technological advances multiply almost daily, many utilities are reluctant to update their antiquated systems, mainly because of cost. In response, some communities are developing innovative ways to generate additional revenue.

In 2004, the City of Atlanta initiated a homeland security surcharge to customers' monthly water bill to help subsidize the costs for the water's security infrastructure. For a seven-year period, this surcharge will help to pay for the $28 million in capital improvements needed for security such as a recent Department of Watershed Management (DWM) project to implement usage of three-dimensional (3D) laser scanning technology also known as High-Definition Surveying (HDS).

Through a joint venture partnership, Jacobs Engineering, PBS&J, and PRAD Group worked with the DWM to use HDS technology to capture images of the facility's exterior and create a 3D image. The data provided detailed information on facility entry locations and sizes for use in further threat analysis and security planning and design.

What's Next?

No one knows what the future may hold but one thing is certain—the demand for safe drinking water will certainly not abate. And as long as that need exists, the EPA will continue working with other federal agencies such as the Centers for Disease Control and Prevention, the Department of Homeland Security, Federal Bureau of Investigation, and the Department of Defense and water sector organizations to improve information on technologies and conduct research for water sector security.

FYPC

EPA Water Security Web site:
cfpub.epa.gov/safewater/watersecurity/index.cfm

Air Mobile Ministries:
www.airmobileindustries.org

Vortex Corporation:
www.vortexpurewater.com

D^2S^2:
For more information, e-mail Kathleen O'Neil at *kmoneil@pbsj.com*.

Department of Homeland Security:
www.dhs.gov/index.shtm

University of Arizona Water Quality Center:
wqc.arizona.edu/

Taking the Drug-Free Workplace to the Next Level

Drug-Free Work Week is a time each year to highlight the benefits that drug-free workplace programs bring to employers, workers, and communities. Drug-Free Work Week was observed this year October 20-26.

While most of us think we have heard all about the dangers of drugs in the workplace, according the U.S. Department of Labor (DOL), it's a message that many workers need to hear repeated. Consider this: according to the DOL, 75 percent of the nation's current illegal drug users are employed—and 3.1 percent say they have actually used illegal drugs before or during work hours. The odds are overwhelming that some of these people are working with you.

And these statistics only account for *illegal* drug use. A significant development in recent years is that many workers are now abusing *legal* drugs. These are not the stereotypical marijuana smoking, cocaine abusing drug users. Data from the latest National Survey on Drug Use and Health reveal an increase in prescription drug abuse. Complicating the problem is that most workplace drug-testing programs usually test for only illegal drugs, not prescription medications such as painkillers.

Ignoring or avoiding employee substance abuse doesn't help the situation. Abuse of alcohol or other drugs inevitably leads to costly and potentially dangerous consequences in the workplace unless action is taken to confront the issue.

Drug-free workplace programs have proven helpful in protecting employers and employees alike from the potentially devastating consequences of worker alcohol or drug abuse. Approaches to these programs are changing to keep pace with escalating abuse of prescription drugs and shifting employee needs.

Traditional approaches to a drug-free workplace have included:

Drug Testing—It can identify evidence of recent use of alcohol, prescription drugs, and illicit drugs. Currently, drug testing does not test for *impairment* or whether a person's behavior is, or was, impacted by drugs. Drug testing works best when implemented based on a clear, written policy that is shared with all employees.

Training and Education—Working Partners, a DOL initiative that raises awareness about the impact drugs and alcohol have on the workplace and provides information on how to establish drug-free workplace programs, offers a variety of resources, such as brochures, presentation materials, articles and fact sheets, and posters, to help employers provide drug and alcohol education in the workplace. All Working Partners materials may be reproduced and distributed without additional permission from the DOL. Organizations are free to incorporate their names and/or logos on all Working Partners materials.

FY PC

Information on promising drug-free workplace programs and additional free resources are available at the DOL Working Partners for an Alcohol and Drug-free Workplace.

http://www.dol.gov/workingpartners/welcome.html.

> *A significant development in recent years is that many workers are now abusing legal drugs.*

Internet resources provide answers to commonly asked questions about addiction, treatment, recovery, and screening as they impact workplace and workforce issues.

FY insight

Substance Abuse Information Database (SAID)

The DOL SAID provides information about and access to hundreds of documents and resources that may assist employers and others to learn about workplace substance abuse issues and develop drug-free workplace programs. Examples of items cataloged in SAID include sample policies, research reports, training and educational materials, and legal and regulatory information. Access the database at:

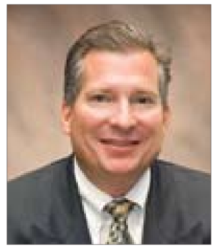
www.dol.gov/asp/programs/drugs/said/default.asp.

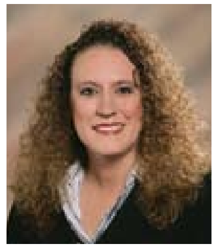
Promising new practices for a drug-free workplace include providing assistance or support to employees who have problems with alcohol and other drugs usually through some type of Employee Assistance Program (EAP).

Many companies, including PBS&J, offer EAPs, typically in conjunction with a health insurance plan. EAPs are intended to help employees deal with personal problems, including drug abuse, which might adversely impact their work performance, health, and well-being by providing employees with confidential access to professional counseling services.

The EAP is a benefit available to employees when outside help is needed to evaluate a problem and explore possible solutions before health and job performance are affected. Counseling is available for marital and family conflicts, emotional problems, stress, and financial and legal concerns, as well as drug and alcohol abuse. Participation in the program is voluntary and typically includes a free assessment, initial short-term counseling, and referral services for ongoing counseling or legal assistance.

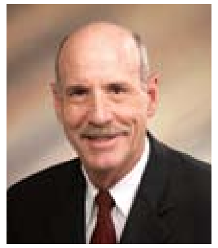
EAP programs are proving to be mutually beneficial to employees and their organizations. Employees receive the confidential, professional assistance they require while protecting their job status within the company and future career opportunities. Employers are able to offer an alternative to dismissal while demonstrating efforts to support employees. Everyone wins with healthy, dedicated employees, and a safe, secure work environment.

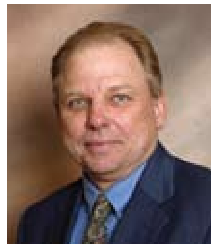

Michael Bagnasco


Marisol Elliott

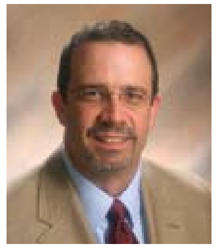
Marvin Fisher

Jennifer Marcy


Thomas McGill


Glenn Myers

Suresh Raghavendra


Thomas Singleton

SPOT Light

PBS&J PEOPLE NEWS

MICHAEL BAGNASCO, PG | **Houston, Texas** | **Environmental Sciences**

Bagnasco has joined PBS&J's central region sciences division as a senior geologist/senior project manager. With 22 years of experience in both the oil and gas and environmental engineering consulting industries, he has directed due diligence investigations and remediation of properties with contaminated soil and groundwater at both international and domestic sites. Bagnasco is a certified leaking petroleum storage tank (LPST) corrective action project manager.

MARISOL ELLIOTT | **Orlando, Florida** | **Transportation**

Elliott has been named PBS&J's group manager for aviation planning. She has 15 years of experience in project management, technical analysis, and strategic planning in government settings and airports. Elliott has a bachelor's degree in aviation management from the Florida Institute of Technology and a master's degree in public administration from the University of Baltimore.

MARVIN FISHER | **Dallas, Texas** | **Federal**

Fisher has been appointed to the National Board of Direction and appointed the chair of the new Education and Training Committee for the Society of American Military Engineers (SAME). He has been active in SAME for over 27 years, and has held a variety of local, regional, and national leadership roles. In 2005, he was inducted into the Society's Academy of Fellows.

JENNIFER MARCY, CFM | **Beltsville, Maryland** | **Water**

Marcy has received the Association of State Floodplain Manager's (ASFPM) John Ivey Award for Superior Efforts in Certification. The award was established by ASFPM in 2001 to recognize exceptional efforts to promote the professional certification of floodplain managers. She was the principal author and instructor for a certified floodplain manager examination preparation course that has been offered at ASFPM and other conferences nationwide.

THOMAS MCGILL, PH.D. | **Riverside, California** | **Environmental Sciences**

McGill will manage PBS&J's natural resources group in southern California. A recognized wildlife biologist, he has 30 years of experience with federal and state wildlife agencies, and has managed numerous habitat conservation planning, land use planning, and environmental efforts. He earned his doctorate in genetics and master's degree in ecology from the University of California.

GLENN MYERS, PE | **Miami, Florida** | **Transportation**

Myers received a "Best Paper Award" from the Federal Highway Administration (FHWA) for "The Salt Creek Bridge Replacement – The 18 Day Bridge," one of only three such awards given at FHWA's 2008 Accelerated Bridge Construction: Highway for Life Conference. Myers also recently became the newest voting member of the Precast/Prestressed Concrete Institute (PCI) Committee on Bridges. PCI's largest committee, the group oversees design, construction, and code requirements for precast concrete bridges.

SURESH RAGHAVENDRA | **Phoenix, Arizona** | **Transportation**

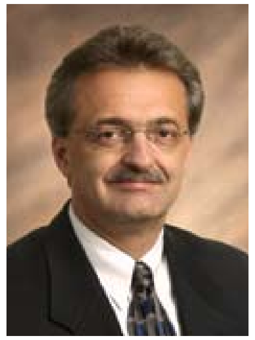
The American Society of Civil Engineers (ASCE) named PBS&J transportation project manager Suresh Raghavendra a New Face of Civil Engineering as part ASCE's National Engineers Week. Raghavendra is one of ten recipients recognized for their professional contributions, impact on society, and representation of the civil engineering profession.

THOMAS SINGLETON | **Tallahassee, Florida** | **Environmental Sciences**

As project director, Singleton's duties include directing PBS&J's total maximum daily load (TMDL) services, with responsibility for the company's TMDL water quality and watershed management activities in Florida. Previously he was a statewide team leader for the Florida Department of Environmental Protection's TMDL program. He has more than 34 years of professional experience in land and water resource management in both the private and public sectors.

CURRENT NEWS

Paulsen Named President of PBS&J



Robert J. Paulsen has been named president of PBS&J, the primary subsidiary of The PBSJ Corporation and one of the nation's leading architecture and engineering firms. He succeeds Todd J. Kenner, who resigned from the company effective August 22, 2008.

Paulsen is also chairman of PBS&J and vice chairman and secretary of The PBSJ Corporation's Board of Directors. He has been a director of the corporation since 2000. He joined PBS&J in 1986 and has been an officer of that company since 1993. Prior to his recent assignment, Paulsen served as the chief operating officer of PBS&J and as PBS&J's national director of transportation services. He is based in PBS&J's Orlando office.

PBS&J Announces Management Changes

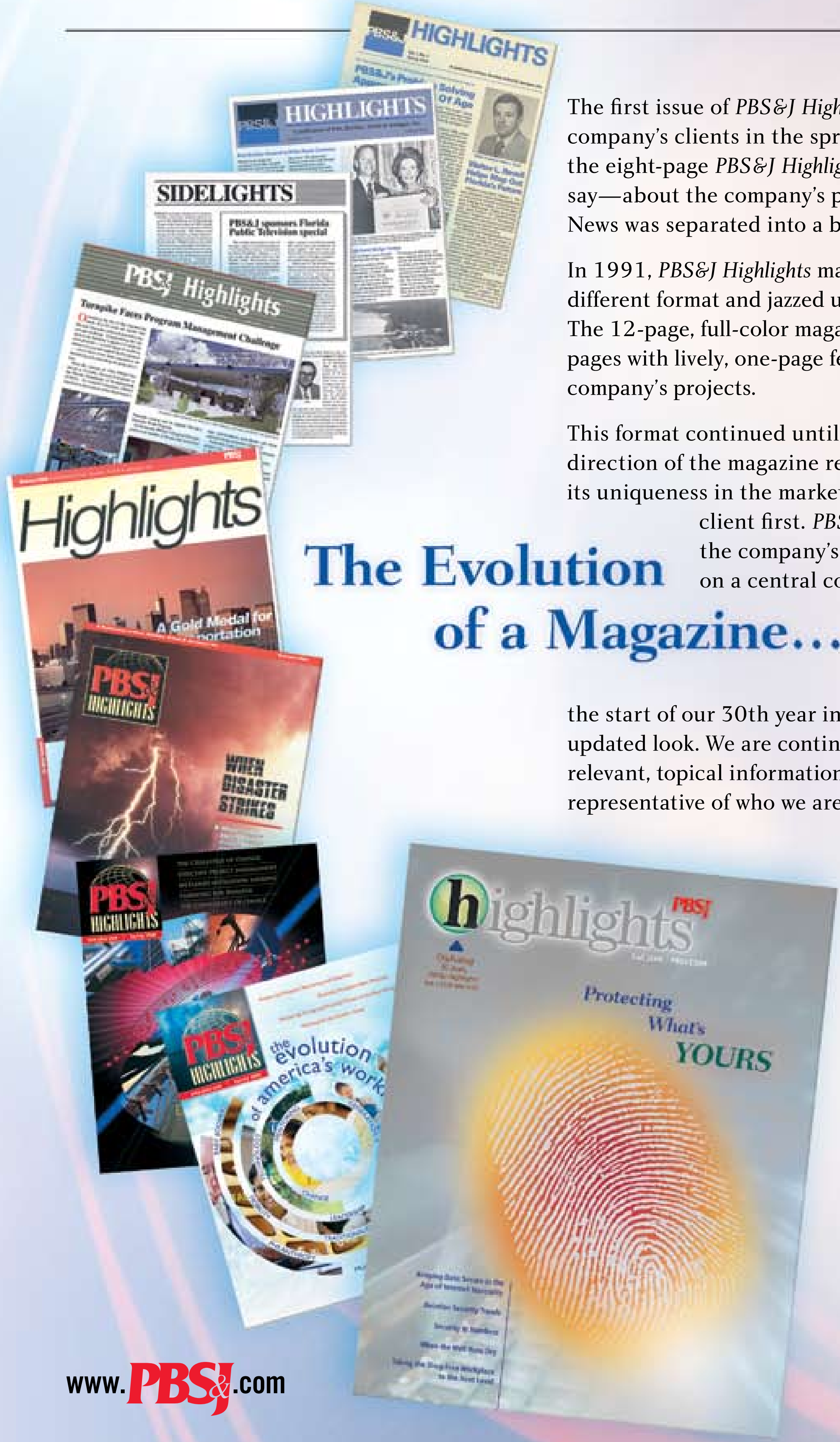
PBS&J has announced the following changes and additions in company management:

Wayne J. Overman has been appointed chief operating officer for PBS&J. Overman joined the company through its 1997 acquisition of Espey, Huston & Associates, Inc. Since that time, he led the growth of PBS&J's aviation practice to a level of national prominence. During the last year, he also served as deputy service director for PBS&J's transportation business line. He was elected to serve on the board of directors for The PBSJ Corporation in January 2008. Overman is a licensed professional engineer in 10 states. He splits his time between PBS&J's Nashville and Tampa offices.

Michael M. Newton has joined PBS&J as director of human resources. Most recently he served as vice president for Saint-Gobain Corporation's North American building materials division, where he was responsible for all aspects of human resources, including compensation, benefits, organizational development, labor relations, succession planning, compliance, recruitment, training, and development. Previously, he held the position of international general manager for human resources with Lafarge North America. Newton is located in PBS&J's Tampa headquarters.

John M. Finochiaro has joined PBS&J as chief technology officer. His 20 years of professional experience includes senior management positions for large, international organizations. He joins the company after eight years as chief technology officer for Sitel, a large, global business process outsourcing leader. Prior to his tenure with Sitel, John Finochiaro served eight years as director of information systems for Lozier Corporation. He is located in PBS&J's Tampa office.

Jeanne A. Yacoub fills a new position as director of PBS&J's project/program management office. In this capacity, she will help to further develop project management as a core competency of PBS&J. She joins PBS&J after 13 years with Shaw Environmental & Infrastructure, Inc., where she most recently served as vice president and director of operations for the company's Gulf Region. In addition, Yacoub served as the southeast regional director of project management. Yacoub holds professional engineering licenses in Virginia, Colorado, and Maryland and is an associate member of the Project Management Institute. She is located in PBS&J's Atlanta office.


HIGHLIGHTS
HIGHLIGHTS
SIDELIGHTS
PBS&J sponsors Florida Public Television special
PBS&J Highlights
Turnpike Faces Program Management Challenge
Highlights
A Gold Medal for Transportation
PBS&J HIGHLIGHTS
WHEN DISASTER STRIKES
PBS&J HIGHLIGHTS
the evolution of america's work
highlights PBS&J
Protecting What's YOURS

The Evolution of a Magazine…

The first issue of *PBS&J Highlights* arrived in the mailboxes of the company's clients in the spring of 1979. More newsletter than magazine, the eight-page *PBS&J Highlights* provided news—highlights, you could say—about the company's people and projects. In 1998 PBS&J's People News was separated into a back page section called Sidelights.

In 1991, *PBS&J Highlights* made the evolutionary leap to a vastly different format and jazzed up its pages with brightly colored graphics. The 12-page, full-color magazine sported a dedicated cover and filled its pages with lively, one-page feature articles covering a variety of the company's projects.

This format continued until 1997, when a major shift in the editorial direction of the magazine reflected the company's growing awareness of its uniqueness in the marketplace and PBS&J's philosophy of serving the client first. *PBS&J Highlights* would no longer simply recap the company's accomplishments, but instead would focus on a central concept and provide useful information on subjects of related topical interest.

Which brings us to 2008 and the latest reinvention of *PBS&J Highlights*. As we near the start of our 30th year in print, you will notice this issue has a new, updated look. We are continuing with the same central concept, and relevant, topical information but in a fresh, modern package that is more representative of who we are today and where we are heading. Enjoy!

www.PBSJ.com