A Special Advertising Supplement

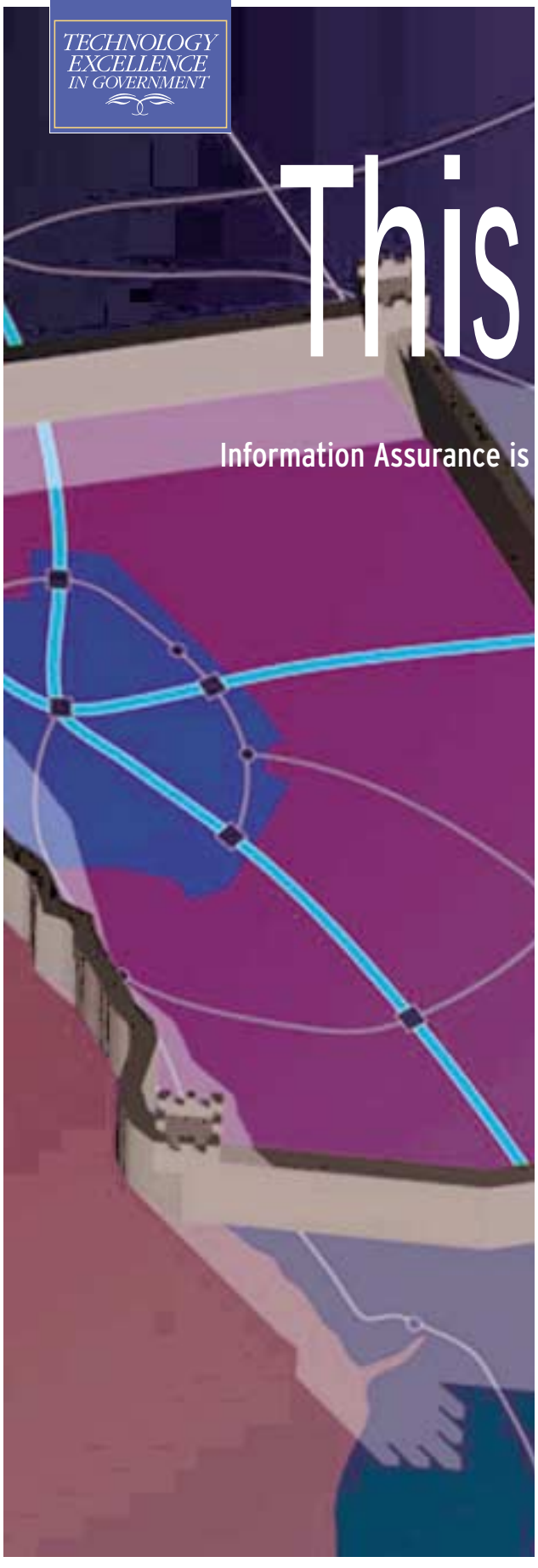
TECHNOLOGY EXCELLENCE IN GOVERNMENT | GCN Government Computer News

27th In A Series

Technology for Secure Government

At the Information Assurance Technology in Excellence in Government seminar, government managers learned how Information Assurance is becoming a formal process. Read how you can make it your process too.

Inside



This "IA" is Your

Information Assurance is becoming a formal process. Make it your process.

PERHAPS IT MAKES SENSE THAT A CONFERENCE on Information Assurance would try to determine exactly what IA is. Provided, of course, that a fixed definition is possible.

Certainly we can agree that IA is "different things to different people," as Susan Pequigney, director of federal programs at Internet Security Systems (ISS) Inc., told the conference.

Equally, there is some consensus to navigate by. For instance, just about everyone would agree that security and privacy on the Internet are two of the bigger "things" that IA programs must address.

Be aware (and consoled), the world has confronted this sort of thing before, noted John A. Jauregui, a former military technology expert now a manager in IT security with Peak Consulting.

"Do we think of the Internet as international waters?" Jauregui rhetorically asked the *GCN Technology Excellence in Government* conference. If so, we need to identify which waters we control and which belong to everyone, he said.

Do international waters begin right outside of our firewall, perhaps?

Jauregui noted that the history of aviation became the history of aviation accidents as flight increased. Then, it became the history of aviation risk mitigation as very exacting processes grew up around air safety — simply because there was so much air flight.

Expect IA in the Internet era to follow a similar pattern. It will become programmatic, embedded, very closely managed, the former Marine Corps official said. The focus on "process" begins now.

Know What You Got

The thing is, IA covers a lot of ground.

"Information Assurance is the ability to provide the right person with the right information at the right time

"IA"

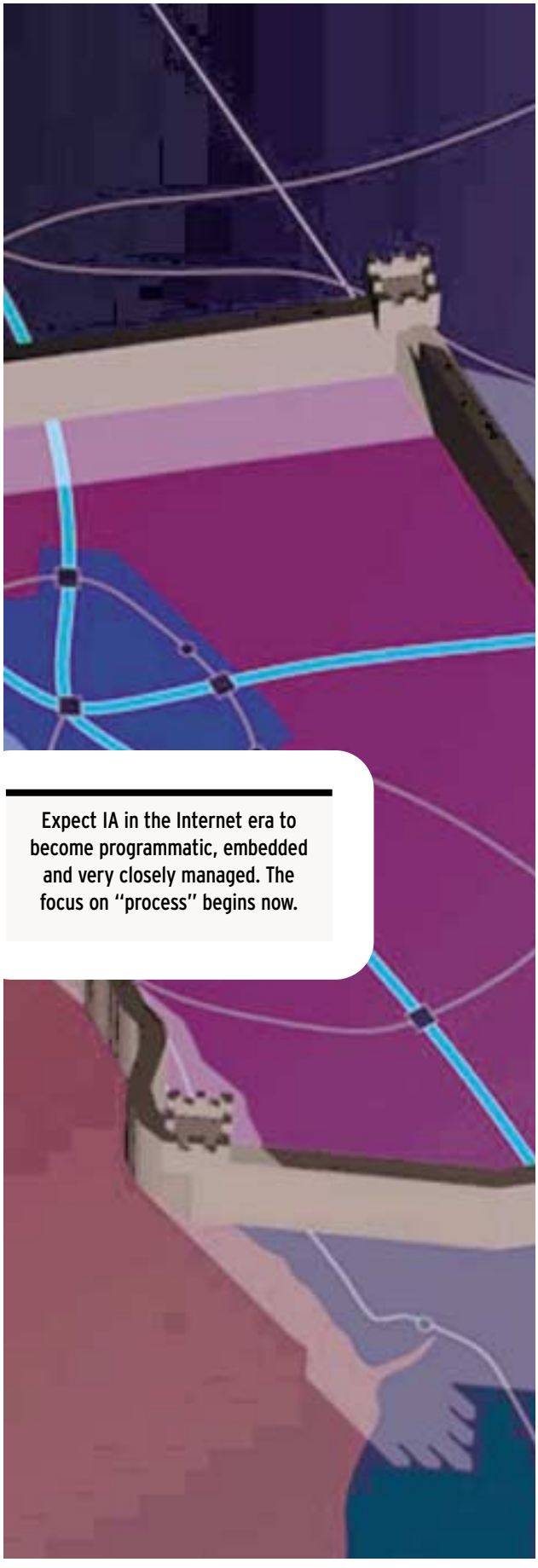
on whatever device that's relevant," said Sean Finnegan, a federal security manager with Microsoft Corp.

IA is also the ability to make sure the wrong person — the hacker, the terrorist, the thief, the virus creator, the mischief maker — is kept out of the loop, Finnegan said.

IA is accomplished a lot of ways. "IA from our point of view is being able to provide infrastructure," said Andrew Lehfeld, a PKI technical consultant with RSA Security. And Public Key Infrastructure is a big piece of the puzzle.

But the puzzle is bigger yet.

Jauregui noted that many organizations "don't really know what assets they have, so it's difficult for them to know what's at risk." A key to good IA policy is that agencies know exactly what they have and how vulnerable it is.



Expect IA in the Internet era to become programmatic, embedded and very closely managed. The focus on "process" begins now.

Manage What You Got

What you are shooting for is "an acceptable level of risk," advised Rick Westcott, a senior sales rep with VeriSign Inc. "I say acceptable because no security is 100 percent."

Just about anyone would tell you that risk mitigation begins by assessing what you have. After that, well, Robert Daniels, a PKI consultant at EDS Corp., advises that you do "penetration testing so as to make sure the sensors are working."

You do have sensors out there, right? Intrusion detection? A denial of service prevention strategy? A solid password policy? A crisis management plan?

Just about everyone involved in security and privacy will tell you that IA really has to be *managed.* "The question is, who controls the keys to the kingdom," asked Michael Pinckney, an account executive with BMC Software.

Pinckney thinks a central authority in your agency should have control over things like password synchronization, audits, adds/deletes/changes and other IA issues. But Daniels of EDS, a former Social Security

This "IA" is your "IA"

continued from page 3

Administration official, thinks IA often lends itself to distributed management — by necessity.

Infosec Thyself

If IA is "different things" it is also "different strokes for different folks." That's partly because systems either run at, or envision running at, variant "levels of trust."

The conference took a look at systems that seek to meet these levels of trust and federal projects meant to lay down the mandatory infrastructure upon which eGovernment and other New Economy processes can be increasingly leveraged by agencies.

As for infrastructure, some is just emerging and some well established. As for the established, The National Security Agency's long-standing Infosec program for performing assessments has been successfully transferred to 500 experts working in the public and private sector now, said Wilbur Hildebrand, chief of NSA's Vulnerability Assessment Services.

Long before GAO or the local IG or anyone else shows up to hold your security system's feet to the fire, you can hire an Infosec expert to confidentially assess your system and ferret out weaknesses. Visit www.iatrp.com for more information.

Long before GAO, or the local IG, or anyone else shows up to hold your security system's feet to the fire, you can hire and ferret out weaknesses. Visit www.iatrp.com for more information.

As for systems and programs now emerging, that's what the rest of this supplement is all about. ■

The conference, Information Assurance: Building Public Trust Through Secure Government Systems, was presented by the Council for Excellence in Government, the Digital Government Institute, GCN and Post Newsweek Tech Media Group.

Learn from Government Leaders!
Connect with Industry Experts!
Collaborate with Your Colleagues!
Make New Relationships!

Attend Technology Excellence In Government Programs!

Much of what you will read in this supplement comes from presentations by distinguished Information Assurance experts from both the public and private sector. They've all been on the front lines. They have "lessons from the trenches" to share and can help you with your business solutions.

And that's what they did with your government colleagues at the one-day Information Assurance Technology Excellence In Government seminar on May 17, 2001 in Washington, DC.

Presenters were:

- Fernando Burbano, CIO, Dept. of State and Chair, CIO Council's Critical Infrastructure Protection Subcommittee
- Judy Spencer, GSA & Chair, PKI Steering Committee
- Peggy Irving, Privacy Advocate, IRS
- Ruth Anderson, Program Manager, PKI and Computer Incidence Response Capability, VA
- Rebecca Canfield, INFOSEC Assessment Training and Rating Program (IATRP), NSA
- Jim Golden, Manager, Corporate Information Security, USPS

Attend the next TEG program on Wireless: Beyond The Hype
July 23, 2001, Marriott Metro Center, Washington, DC. See page 20 for details.

It's a PKI World

Public Key Infrastructure seeks to make eGov a region of the Internet where trust rules.

INFORMATION ASSURANCE IS AN IT DISCIPLINE that spans a breadth of processes, tactics and IT tools.

One of those processes (which comes with its own set of tactics and technologies), is encryption-based Public Key Infrastructure. It is the critical focal point of the effort to make "eGovernment" a region of the Internet in which trust is unquestioned.

By literal definition, PKI is the set of technical processes by which parties to an electronic transaction trade encrypted "keys" (strings of data) so as to authenticate each other's identity and legitimacy to do business.

But what PKI is, exactly, is not nearly as significant as what it does.

Judith Spencer, the GSA official who chairs the federal PKI Steering Committee, called PKI "the only total solution available today" for making the Internet trustworthy.

PKI is the only total solution available today for making the Internet trustworthy. It's not perfect, it's not a panacea, but the idea is to reduce risk, and in many ways PKI is more secure than what we do face to face and on paper.

"PKI is the key to government doing real business on the Internet," Spencer told the recent TEG conference on Information Assurance. "It's not perfect, it's not a panacea, but the idea is to reduce risk, and in many ways PKI is more secure than what we do face to face and on paper."

VA Did It

The end product of the PKI process is the creation of a "digital certificate," an electronic file that essentially records and authenticates the entirety of a specific computer-based transaction.

These certificates are often generated (and maintained) by third-parties such as the contractors under GSA's ACES program, the government's flagship PKI program. Some agencies generate their own certificates too. PKI of one sort or another is now proliferating in the federal government after years of plots and plans.

The Defense Department was among the first to develop its own approach to PKI but others like the Veteran's Affairs department have also developed agency-specific PKI.

Ruth Anderson, a VA program manager and security specialist, gave the TEG conference a look at how the VA will use its own PKI for internal government relationships and the GSA ACES program for the department's relationship with individual vets.

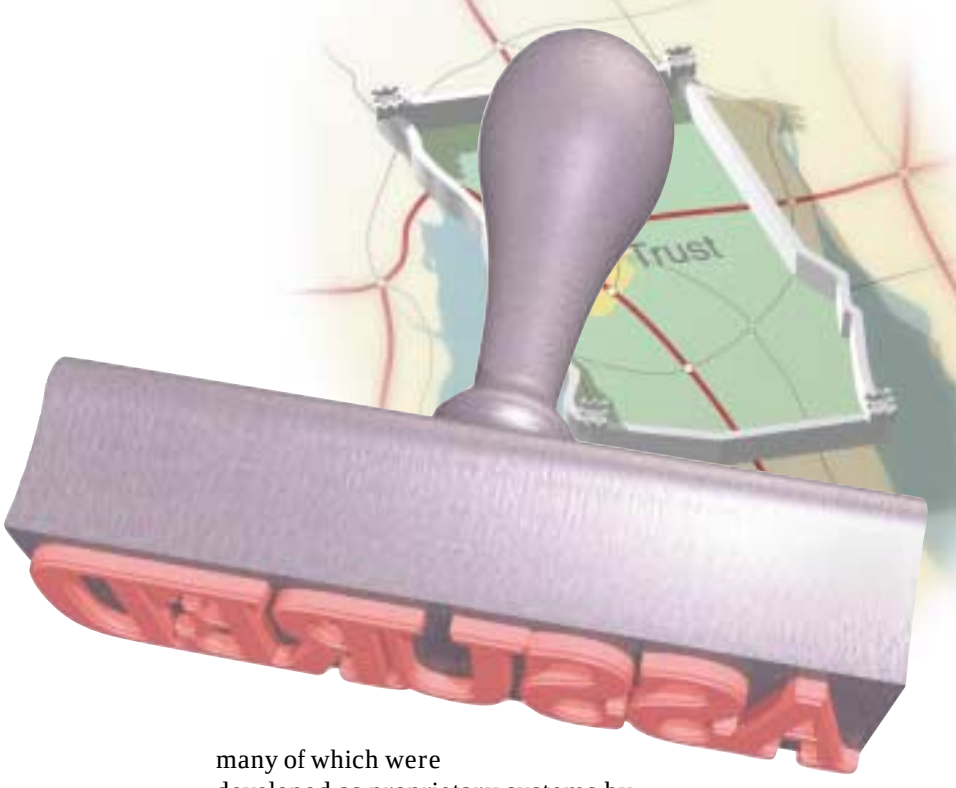
"We at VA don't have to worry about proofing [transactions with] 3 million veterans," Anderson said, explaining why ACES was the best fit for the "citizen" sector of the department's web presence.

Plus, an ACES certificate used by a citizen-stakeholder in VA should be re-useable later on in dealings with other agencies.

Good and Bad

VA started building its own internal PKI before ACES was available and has experienced good and bad as it has put together about 500 exacting PKI relationships, Anderson said.

The need to ardently protect medical data, and to develop a system that would interoperate within the Federal Bridge program for interoperable PKI, spurred VA to do-it-themselves starting in 1998, Anderson noted.



It's a PKI World

continued from page 6

She stressed that PKI has to be easy to use when the community it is serving is comprised of non-IT interests, such as doctors, nurses and hospital administrators.

She also advised that:

- PKI advocates get senior level buy-in early in the process;
- make sure they have firm policies in place;
- develop an implementation plan that takes into account the priorities of IT administrators.

Road to the Bridge

As for the Federal Bridge, it was expected to become an active production-level system earlier this spring, Spencer said. NASA and the Agriculture Department were to be among the first agencies to "cross-certify" in what officials call the Bridge's "membrane."

The state of Illinois was also on the agenda to be one of the first to enter the Bridge program. The national government of Canada, said to be ahead of the U.S. in PKI use, might also be a player in the Federal Bridge program, Spencer said.

Essentially, the Bridge's membrane is the place in federal cyberspace where disparate PKI certificates are given paths by which they can interoperate.

When fleshed out, the Bridge will accommodate the many PKI products available in today's marketplace, many of which were developed as proprietary systems by the competitive IT security industry.

Much of PKI interoperability boils down to making sure different directories can interact with one another. "That's where the rubber meets the road," Spencer said of directory compatibility.

Because ACES was developed to be a single PKI mechanism by which agencies can deal with the American public, it has been exempted from the Bridge program, which focuses on agency-to-agency or agency-to-special community of interest levels of assurance.

Essentially, the Bridge's membrane is the place in federal cyberspace where disparate PKI certificates are given paths by which they can interoperate.

But Spencer said the policies undercurrent in ACES PKI might be mapped to the Bridge so that ACES-based systems will be embedded in the membrane. She also said that the so-called "fat client" system used as a front end during the prototype phase of the Bridge might be eliminated by moving its functionality inside the membrane.

In addition to DOD, VA, NASA and Agriculture, PKI of one type or another is already being used for mission critical IA in the Federal Aviation Administration and the Patent and Trademark Office.

Within the next few months, ACES is expected to become a real driving force of new eGovernment systems in the Social Security Administration, the Environmental Protection Agency, FEMA and NIST.

PKI in government is happening. It's happening right now. ■

Getting the IA Message

Information Assurance is evolving into a full business process.

WE HAVE BEEN PRODUCING GCN INFORMATION Assurance and IT security supplements for almost ten years now. It seemed like a good time to catch up on how much progress is being made.

So, we asked Rich Smith, vice president of federal operations at Internet Security Systems (ISS) Inc., one of those multi-part questions all full of a decade's complexities.

We pondered: "Are people getting the message that IA must be approached with a broad brush that includes policies as well as technology?"

"The question covers a lot of territory," Smith replied. "Do people understand that the Internet and related technologies are built to foster reliable communications first and security only as an afterthought? Absolutely.

"Do users and administrators understand that security management extends beyond the firewalls and antivirus? The situation is changing for the better. But the complexity and the expense of a proper security management system still lead to a significant amount of underfunding and underperformance when it comes to protecting digital assets."

ISS provides intrusion detection and vulnerability assessment systems, and is one of the most prominent suppliers of remote security management services, including full outsourcing.

ISS provides intrusion detection and vulnerability assessment systems, and is one of the most prominent suppliers of remote security management services including full outsourcing. ISS customers include most every major federal agency, 21 of the 25 largest U.S. banks and the top 10 telecommunications companies.

Getting Aligned

Smith worries that "policy" might be a misleading term these days where security and privacy are concerned.

"The term security policy has become so generic that it carries little meaning," he said. "For some organizations, 'policy' means a couple of pages detailing what happens if an employee is caught misusing corporate assets. For others, it means a comprehensive, standards-based audit."

Such audits derive from standards like ISO/IEC 17799, which guides organizations as they design, deploy and manage security systems, Smith noted.

But most organizations are neither so lax nor so formal about security policies. "This situation will improve as more organizations realize that the risk management process is the same for valuating physical assets in a warehouse as digital information on a server," Smith said.

"Once information is recognized as a form of currency, then security becomes much more imperative. Once information protection is recognized as a coherent business process, procedures and funding are much easier to secure. And that transition is rapidly making its way into mainstream business and government agencies alike."

Indeed. Smith said the "recognition" is a two-way street, with advanced companies like ISS understanding that "solutions must meet a business process rather than just deliver a technological system."

ISS aligns itself to how agencies operate rather than imposing solutions. "The end result is greater security transparency and improved cost efficiency for a wider range of IA solutions," he said.

To learn more about how a company like ISS aligns with customer IA missions, visit the Case Studies section of www.iss.net. ■

TECHNOLOGY EXCELLENCE IN GOVERNMENT

Executive Viewpoints

Top executives from Information Technology leaders give their views on important topics facing government when implementing outsourcing solutions.

Question:

Are there any chronic security "soft spots" that you think IT managers need to pay more attention to as they further build their systems out?

Craig Harper
Director of BMC Federal Operations, BMC Software

A. Perhaps the biggest "soft spot" in security is protecting against internal threats to our networks. We all know security is an issue – we all call attention to and address protecting our organizations from an external threat – but theft of proprietary information, negligence, and even sabotage from inside an organization is a more frequent and often more damaging danger. It costs businesses even more in lost revenue. BMC Software helps government network security executives manage access and security on their networks, which is just as important – if not more so – than managing the hardware.

Robert Daniels
Senior PKI Consultant, Global Information Assurance Services Group, EDS

A. Federal IT managers face many challenges in dealing with security. Constantly evolving technology, coupled with the increasing threat environment and newly discovered system and application vulnerabilities, has made security a necessary, full-time job within government IT staffs. Unfortunately, the expertise and skills required to address the security of IT systems and networks are in short supply and high demand. As a result, federal IT managers and their staffs find their efforts primarily focused on system maintenance issues, such as keeping systems running and upgrading applications, as well as trouble-shooting user problems. This rarely allows them to address the security of their IT infrastructures, allowing vulnerabilities to go unchecked and threats to build, putting their systems and sensitive data at risk.

Rich Smith
Vice-President of Federal Sales, Internet Security Systems

A. Technology is, by definition, a fluid entity. It evolves, and information protection must adapt accordingly. Although many organizations have strong security procedures for protecting networks and servers, the two most glaring underprotected segments remain databases and desktops. Security strategies that do not take these two areas into account will find themselves at significant risk for intrusion, even with robust security policies and substantial investments in people, processes and technology.

Advanced database systems like Microsoft SQL Server, Sybase Adaptive Server and Oracle have powerful programming languages that can mimic many operating system functions. Clever attackers can coopt or author these "stored procedures" to advance misuse against other targets – even if the database's host has been properly hardened and is being monitored for unauthorized activity.

Desktops provide a different but equally important type of security challenge. It used to be that desktops could be easily protected because they resided within set physical facilities and behind firewalls and intrusion detection systems. Remote offices, telecommuters, home workers and wireless technologies (Metricom Riccochet, 802.11, WiFi, BlueTooth) have all but obliterated that assumption. Since work can take place from almost any location, either inside or outside the corporate firewall, each desktop that access a corporate resource must be considered a potential access point for attack or misuse.

Executive Viewpoints

Question:

Are there any chronic security "soft spots" that you think IT managers need to pay more attention to as they further build their systems out?

Sean Finnegan
Security Program Manager, Microsoft Federal

A. The greatest security "soft spot" continues to be the inability of IT shops to properly manage their systems and keep them secure. No software is perfect and all products have bugs that may affect security. With each new product that an IT shop adds to their environment an added burden is placed on administrators to stay abreast of new security patches that must be installed. Furthermore, the more products that are introduced into the environment the wider the skill set of the IT staff needs to be to maintain this.

Different products are often required to meet specific business goals or are the result of a legacy application. However, many agencies today continue to purchase and integrate in products that provide the same functionality – this just increases the complexity of the system and the number of avenues of attack.

Microsoft provides in Windows 2000 a comprehensive security framework that can be leveraged by business applications. These same services are also leveraged by our Back Office suite of server products to provide a tightly integrated solution. In addition, the Windows 2000 Active Directory provides a robust tool for centrally maintaining the security configuration and software on all machines in the enterprise.

Dow A. Williamson
CISSP Manager, Market Development RSA Government, RSA Security Inc.

A. Yes. Federal IT executives should place increased emphasis on ensuring the authenticity of the people, devices and transactions they encounter in their e-government environments. They should do this not only because it's the right thing to do in order to protect both government and citizen information...but, also because legislation is emerging which requires such due diligence. The good news is that there are many levels of authentication from which to choose. The key is to find the solutions that meet an agency's unique needs. Passwords are weak...certificates sitting in a browser are not so good...tokens provide strong, two-factor authentication...and certificates protected by a second or third factor, provide even greater security. The key to a successful implementation is working with a solution which can offer you choices.

Nicolas F. Piazzola
Vice President, Government Markets, VeriSign

A. While many federal IT managers recognize that a robust PKI is a essential component of an IA strategy, they often don't realize that it is a complex system security issue that must be addressed in a comprehensive way. A robust PKI infrastructure requires technology, personnel, practice and policies. There is a tendency, particularly among those inclined to operate their own infrastructure, to under estimate the cost and complexity of not only acquiring, but also maintaining a robust, scalable and available PKI-based security infrastructure.

The Privacy Challenge

One violation and it could be all over.

MUCH EGOVERNMENT TO DATE HAS BEEN ABOUT agencies building new electronic relationships with each other or out to special communities such as procurement interests.

The cost-savings and efficiency boosts related to systems like GSA Advantage! are simply enormous. However, eGovernment's ultimate crucible is the transactional relationship that has begun forming between agencies and American citizens. Even in the pioneer stage, programs like the IRS eFile option or Firstgov.gov give us a glimpse of how fluid and efficient the future can be.

And the potential cost savings simply spiral to orders of magnitude as entire methods of transacting business are altered from torturous paper-based processes to instant electronic completion.

What can undo all of this in the blink of an eye?

Privacy issues.

Peggy Irving, a lawyer and chief privacy advocate for Internal Revenue Service, told the recent TEG conference on Information Assurance, "Privacy is the number one concern of the American people."

That is to say, the entire electronic edifice that underpins eGovernment can crumble with a single violation of privacy, or even the threat of a violation.

The extent to which this is true was illustrated several years ago when the Social Security Administration's neat new online access to taxpayer payment and benefits info was undermined by newspaper articles alleging that your privacy "might" be violated on the system.

"Might be" is good enough to clobber systems when privacy is at stake. SSA was compelled to return to a process of spending millions to mail statements to defend against what "might be."

The Privacy Police Cometh

How delicate is this issue? Congress passed 400 bills last year that related to privacy, Irving said. There are another 600 or so proposals in the works right now relating to Internet privacy, she said.

Things are getting tougher as "privacy" is more broadly defined to encompass everything from credit card number protection to the renting of mailing lists to marketing interests. If your phone rings, your privacy is immediately put at risk—or so goes today's mantra.

"The public fear is related to the collecting of information, not the fear that government will spill the beans," Irving said. This fear has translated into a world increasingly dominated by lawyers and judges, many of whom seek to further carve privacy into a domain that must be policed (even though the Constitution does not expressly ensure a right to privacy).

How delicate is this issue? Congress passed 400 bills last year that related to privacy. There are another 600 or so proposals in the works right now relating to the Internet privacy.

Historically, fraud and other criminal statutes relate to information on the basis of its use. Today, if you obtain my credit card number, you will commit a crime only when you use it to make a purchase.

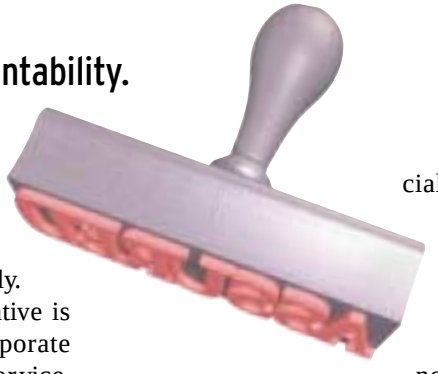
Privacy law increasingly seeks to defend information itself. Just your having my address on a database could be a crime next year.

The present undercurrent of controversy that surrounds this issue is propagated by a professional lobbying sector that elevates privacy above the right to do business.

You probably should at least look at the issue this way as you prepare to launch what Irving calls a "privacy strategy." American corporations are doing just that right now, issuing new mandates on privacy and "selling" their willingness to keep consumer information private. ■

The Business Of Government

Think Information Assurance and accountability.



IN THE PAST, MANY AGENCIES HAVE PURSUED better IT security policies in response to governmentwide mandates. This is another way of saying agencies have sometimes gone about IA grudgingly.

But in the eGovernment world the IA imperative is business-driven, said Jim Golden, manager of corporate information security for the United States Postal Service.

"For us, security is a business issue," Golden told the recent TEG conference. "It is not just a federal mandate. A great deal of our presence is based on trust."

Virtually no federal agency operates more closely to the American people than USPS. It occupies 38,000 post offices nationwide, and would rank number 11 on the Fortune 500. Almost every American sees at least one mail carrier or one Postal vehicle every day. Most of us don't drive six blocks without seeing a mail box.

With 7,000+ networked offices and 2,000+ external system users, USPS has absorbed some heavy security requirements. USPS.com gets 8 million hits per month. Security for the web site, like all other IT assets, is centrally managed in accordance with the Y2K model, Golden said.

Of course, IA is a little different than Y2K was.

IA-"Accountability"

"Y2K was neat. I knew exactly what the challenge was. Security is something you have to do every day," Golden advised. USPS uses Infosec guiding principles that focus on how IT security relates to public trust, business issues, risks and costs, and best practices.

Infosec guiding principles also stress that every person in an agency has a security responsibility, not just special experts.

Golden said USPS frames policies around its "business interest, personnel, and the public." USPS is a good barometer on eGovernment overall because it is a financially self-sustaining enterprise. Thus, all IT investment must contribute to the health of the bottom line.

Golden stressed it is not enough to have policies and procedures, "you must enforce them." He also suggested that security policies be written "in English," with a focus on the business mission.

There's plenty of tech work too. Vulnerability scanning and intrusion detection must be ongoing, he said. USPS maintains a team of experts at the ready in case of a major IT catastrophe.

USPS uses Infosec guiding principles that focus on how IT security relates to public trust, business issues, risks and costs, and best practices.

The risks associated with IA must be signed off on by senior leaders in agencies, and their decisions must be informed ones, Golden said. He and his staff produce informational videos and circulate them to aid security awareness.

Golden said he is not afraid of working with anyone, including the USPS Inspector General's office, to help identify weaknesses in systems.

As for tactics, USPS protects its network infrastructure by controlling entry/exit points, persistently monitoring usage, vulnerability scans and remediation, and intrusion detection.

Platform protection encompasses identification and authentication processes, critical events monitoring, real time intrusion detection and monitoring, and server hardening.

Certification of a system's readiness to withstand threats "is all about doing what you said you were going to do at the beginning of the process," Golden said. Golden stressed "accountability" during the conference. Think IA-A. ■

Moving Out Smartly

Headlines might blare, but the federal IA glass is better than half full. If you don't think so, ask industry how government stacks up.

WHENEVER A FEDERAL AGENCY WEB SITE IS hacked, whenever a congressional "report card" is released, government IT security and the issues surrounding Information Assurance rocket to the front page of the newspaper.

Boy, what a mess, the public is suddenly told.

The fact is, however, that there is no evidence that federal IT is less protected against computer threats like viruses and denial of service attacks than any other segment of the worldwide portfolio of electronic resources.

Indeed, a panel of IT security industry experts told the recent GCN/Post-Newsweek TEG conference on Information Assurance that many U.S. government systems are at the forefront of IT security technology and have been for years.

"If anything, I see a lot of agencies well ahead of the curve in terms of penetration defenses, auditing, intrusion detection, disaster recovery and all the tools that go into protecting a network infrastructure against external threats,' said Andrew Lehfeld, a PKI technical consultant with RSA Security.

"If you look at the government as a sector within the larger marketplace, I would have to rate government one of the early adapters of IA technology," said Rick Westcott, a senior sales rep with VeriSign Inc.

The only part of the American private sector comparable might be banking and brokerage interests, "because if they don't build a high level of trust into their systems, they are out of business," Westcott said.

Industry experts attribute most of government's IA savvy to legislative mandates like Critical Infrastructure Protection laws compelling agencies to take preventive measures.

Industry experts attribute most of government's IA savvy to legislative mandates like Critical Infrastructure Protection laws compelling agencies to take preventive measures.

RSA's Lehfeld and others on the industry panel said they are especially impressed with the work of the intelligence agencies and the Defense department, but that good security is no longer found only at the sharp end of the federal IT blade.

Protecting The Public

Robert Daniels, a PKI consultant at EDS Corp. said that agency security consciousness is usually acute "in any system that is being built out to the public like those that IRS, Social Security and the Veteran's Administration have running now."

Such agencies are re-engineering business processes to focus on IA imperatives as they extend new eGovernment resources, he noted.

Laws and policy enforcing new privacy measures are spurring agency IA consciousness, too. Michael Pinckney, an account executive with BMC Software, put the health care sector on the list of public and private systems that are especially fortified, in part because privacy laws regarding medical records are getting tougher all the time.

"With health care as with the IRS, you have systems being built around the stipulation that only those who need access to sensitive information will get access," Pinckney said.

Federal systems might simply be more prone to falling under the spotlight of national publicity. "If they had report cards in the private sector, I guarantee you that while there would be some organizations that rate very good, there would be others not so good," said Susan Pequigney, director of federal programs at Internet Security Systems (ISS) Inc.

Who has the edge?

Government might have some advantages and disadvantages vis a vis the private sector, said Sean Finnegan, a federal security manager with Microsoft Corp.

He noted that intelligence agencies and DOD sectors "have been doing Information Assurance for a long time. It wasn't until the Internet came along that most commercial entities started caring about security."

But Finnegan thinks many private sector organizations now have an edge on agencies in that they are better able to "focus on exactly what they are deploying and why they are deploying it." Many agencies are more decentralized, and run "a wider range of products, applications, operating systems and platforms," than most companies, he said.

If the private sector has another IA edge on government it might be its willingness to outsource security requirements to expert companies, said Pequigney of ISS.

"We're seeing a tremendous amount of outsourcing in the private sector, and we are only right now seeing it get started in the government sector," she told the conference.

The fact that many agencies were involved in security long before other IT interests certainly explains part of any on-going reluctance to outsource. But even the Central Intelligence Agency has recently collaborated with industry to help foster new commercial IT systems.

Pequigney said outsourcing is a natural fit for "smaller agencies who can not afford to invest in implementing and managing a complex IA architecture." For larger agencies, the economy of scale might even be better, especially if IT staff drain continues.

Outsourcing is a natural fit for smaller agencies who can not afford to invest in implementing and managing a complex IA architecture. For larger agencies, the economy of scale might even be better, especially if IT staff drain continues.

Pinckney of BMC Software noted that his company focuses entirely on providing central management tools, so that IA is a less manpower-intensive task from the get-go. Daniels of EDS said the prominent integration company offers a "wheel of services" because "nothing is static about IT security" and the threats against it.

Keeping Up

Can agencies with limited IT security budgets keep up? Westcott of VeriSign noted that once trained on something as exacting as Public Key Infrastructure, government experts tend to jump to the private sector anyway.

RSA, VeriSign and other companies provide PKI that can run completely out-of-house while generating the digital certificates authenticating users of new federal web systems.

"Even if you're running your own PKI," VeriSign's Westcott told the federal IT audience, "you are probably using consultants to do a lot of it for you." The step to fully outsourcing PKI and other IA operations might boil down to one issue. "Does it have to be located down the hall where you can physically see it," he said.

Pequigney of ISS likened IA outsourcing to consumer home security.

"My home has sensors and alarms on the doors and windows, but I wouldn't buy a computer system to monitor it, or hire three people to do shift work in my house," she said. "I just give that part of it to the home security company to do on a remote, service-level basis." ■

Tips From The Trenches

From getting top management backing to giving support personnel the power to deploy security measures, there are of things you can do right now to boost Information Assurance.

Get Top-Down Support

The key elements of a security infrastructure include:

- A strong commitment from management to provide sufficient resources to get the work done and to support security policies and procedures.
- A well-defined site security policy.
- A well-developed security awareness training program.
- Clearly defined, implemented and documented security policies and procedures, which are supplied to everyone within your agency.
- A strong flow of information to and from the appropriate groups.
- The right people and the right tools to do the job.

Pick 'em Off with IDS

Intrusion detection systems (IDS) are particularly useful because:

- The earlier you detect an attempted attack the better chance you have of preventing a serious and potentially expensive system compromise.
- Knowing the types of attacks that are directed against your site helps you tune your defenses.
- Detecting attackers and preventing them from using your site as a springboard to attack other sites may save your organization from embarrassment and/or legal costs.

The Tools Are

The following tools are essential to IT security:

- Host-based Auditing tools
- Networked Traffic Analysis tools
- Security Management and Improvement tools
- Firewall, Filtering and Proxying tools
- Network-based Auditing tools
- Encryption tools
- One-Time Password tools
- Secure Remote Access and Authorization tools.

Best Practices Performed

A number of practices will ensure that your security infrastructure is sound. The following tasks are well worth performing and include:

- New System Installation Security Audits help ensure conformance to existing policies and a standard system configuration.
- Regular Automated System Audit Checks can reveal "visitations" by intruders or illicit activities by insiders.
- Random Security Audit Checks are your way to test for conformance to security policies and standards (by checking for illicit activity), or to check for the existence of a specific class of problems (e.g., the presence of a vulnerability reported by a vendor).
- Night Audits of Critical Files are a way to assess the integrity of critical files (e.g., the password file) or databases.

Source: The SANS Institute

This PIA Is Your PIA

Take advantage of the IRS and CIO Council Privacy Impact Assessment (PIA) framework to help you assure citizen privacy.

As tough as privacy issues might be for federal agencies to deal with as they shift to eGovernment systems, you do have help.

Your inter-agency CIO Council, in conjunction with the Treasury Department's Internal Revenue Service, has already produced a best-practice Privacy Impact Assessment (PIA) framework.

The IRS PIA was advanced by the CIO Council as a model most agencies can use. It is based on guidelines that spell out what you need to know, do, the specific issues to address, and who you need to include in the process of making systems privacy-ready.

The PIA encompasses the mandates of the 1974 Privacy Act (as amended), the Computer Security Act, and very stringent IRS confidentiality and disclosure rules. It recommends that specific systems be submitted to the guidance of a Privacy Advocate in your agency.

"The PIA is a process used to evaluate privacy in information systems," says the framework. "The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by the Privacy Advocate."

The IRS mandated that new systems, systems under development, or systems undergoing major modifications (such as conversion to eGov applications) complete the PIA process.

At the core of the process is the identification of key participants. As well as the Privacy Advocate, the framework names the system owner, the system developer and the CIO as the critical players.

It is this group that must be trained and fluent in the techniques of assuring privacy. It is also this group that "should reach agreement on design requirements to resolve all identified risks." The PIA gives the CIO the responsibility of resolving disputes.

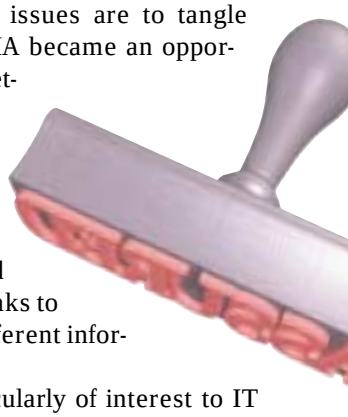
Bi-Partisan Pressures

Peggy Irving, the chief privacy advocate for Internal Revenue Service, told the recent TEG conference on Information Assurance, that Congress has taken interest in the PIA and that powerful lawmakers including Sen. Joseph Lieberman, D-Conn., might be inclined to mandate that the PIA be applied governmentwide.

Irving also noted that Internet and eGov privacy is generally regarded as a bi-partisan priority on Capitol Hill. The Office of Management and Budget is already requesting that agencies submit privacy information along with system development budget requests, Irving said.

Through an overarching policy, the PIA resulted in specific IT guidance on cookies, web site privacy statements, and cautions such as reminders that links to other sites will lead users into different information collection policies.

As difficult as many privacy issues are to tangle with, Irving noted that the IRS PIA became an opportunity for the agency to institute better data standards in forms, and reduce data elements overall.



Though an overarching policy, the PIA resulted in specific IT guidance on cookies, web site privacy statements, and cautions such as reminders that links to other sites will lead users into "different information collection policies."

Section V of the PIA is particularly of interest to IT folks, as it provides guidance on issues regarding the data in your systems, access to it, its attributes, and administrative control matters.

You can get your digital mitts on a copy of the PIA by visiting http://www.cio.gov/docs/IRS.htm. ■

GCN

CUSTOM MARKETING SERVICES

Post Newsweek Tech Media Group

8601 Georgia Avenue, Suite 300, Silver Spring, MD 20910 • 301/650-2200 • Fax 301/650-2111 • *www.gcn.com*

Jeffrey Erlichman: **Associate Publisher/Marketing** • Thomas Trezza, Jr.: **Sales Manager** • Robert Green: **Writer** • Kelly Bryant: **Design** • Bill Reuter: **Art**