

# CIO SPOTLIGHT

INFORMATION SECURITY

## Emerging and Evolving Threats

Strategies for  
Securing the  
Enterprise



Best Practices for Fighting Back • Positive Identification  
Stopping Spyware and Spam • New Help for IT

# CIO SPOTLIGHT

## INFORMATION SECURITY

APRIL 1 *CIO* · APRIL *CSO*  
VOLUME 1, NUMBER 1



- 4 Taking Control:  
Best Practices for  
Fighting Back
- 12 Identity and Access  
Management:  
Knowing Who's Who
- 14 Spyware and Spam:  
Worse Than Ever
- 16 Networks and  
Infrastructure:  
New Help for IT



## TAKING CONTROL:

# Best Practices for Fighting Back

**S**ECURITY THREATS become increasingly diverse, sophisticated, coordinated and virulent almost by the day. For example, after just 24 hours in the wild last autumn, a variant of the Bagle virus, spread by spam, became one of the most prolific viruses ever, rapidly replicating itself and bogging down corporate e-mail servers. Meanwhile, tools available on the Web make it easier than ever for even amateur hackers to launch attacks.

That explains why more than half of the chief security officers queried at the second annual CSO Interchange conference in December 2004 listed as their top security concerns worms, viruses, Trojan horses and regulatory compliance. In the same survey, 62 percent said they don't receive early enough warning about Internet-related threats, while fully 80 percent acknowledged that such attacks have hurt their companies' bottom lines.

No question about it: Keeping up with constant security threats is a significant challenge. But as more organizations become aware of their vulnerabilities and shortfalls—too often learning the hard way—they're fighting back. No wonder security-related spending has grown steadily over the past

several years while investment in other technology areas stayed flat or declined. In fact, 86 percent of businesses plan to increase their security investments this year, according to research from Framingham, Mass.-based IDC.

"Companies buy insurance, employ security guards and decide how much to invest in screening employees based on experts' calculations of expected risk, the cost of a loss and the cost of insurance to protect against that loss," says Rebecca Wettemann, an analyst at Nucleus Research Inc., a Wellesley, Mass.-based market research firm. She recommends that organizations apply the same kind of risk-benefit evaluation to their IT infrastructures. "IT managers can add

# Meeting Compliance Challenges

**H**OW ARE ENTERPRISES dealing with Sarbanes-Oxley and other new laws and regulations that have an impact on their IT security? Among the common approaches:

**Standardizing IT security governance efforts.** After passage of the Sarbanes-Oxley Act, Allstate Corp. turned to the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT), which help ensure alignment between business strategies and technology investments. Allstate, the Northbrook, Ill.-based insurance giant, uses COBIT to evaluate IT governance, obtain benchmarks for assessing automated controls embedded in key business processes and assess application-support team control activities.

The big-picture payoff: Allstate has achieved consistent controls to improve the efficiency and effectiveness of its business.

**Using certified auditors.** "As IS auditors travel throughout an organization, they are able to see and verify which parts of the information security policy are being complied with, and can offer suggestions on improving compliance or making suitable updates to the policy," says Marios Damianides, CISM, CISA, CPA, a New York-based partner in the Technology and Risk Services Group at Ernst & Young. "The IS auditor also comes across systems or situations that are not adequately

addressed in the policy and offers guidance on those. An active IS audit function can make the difference between an effective, living IT security policy and a dormant one."

Damianides is also international president of the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI), both based in Rolling Meadows, Ill. More than 1,300 ISACA Certified Information Systems Auditors (CISAs) are currently employed as CEOs, CFOs, CIOs or IS security directors. About 11,000 more serve as audit directors, managers or consultants in IT operations, security or auditing positions.

**Centralizing access control.** Affymetrix Inc., a Santa Clara, Calif.-based biotech firm, takes compliance seriously. Protecting the company's valuable intellectual property is a strategic necessity. Thanks to a solution from Encentuate, of Foster City, Calif., Affymetrix got out-of-the-box compliance for 13 of 15 applications directly affected by Sarbanes-Oxley. In addition, simplifying sign-on and password management for 1,000 employees generated savings of more than \$200,000 in just six months.

"Compliance requirements are forcing companies to strengthen their security, often at the expense of user convenience," says Encentuate founder and CEO Peng Ong. "The best solutions will allow IT to strengthen security and at the same time provide users with increased convenience. We call this enterprise access security—a single solution that will allow an enterprise to simplify, strengthen and track access across information systems."

value by clearly understanding the relative costs and benefits of different technology strategies and by working with the risk experts to map the best strategy for the organization," she says.

## Got mandate?

What you do about protecting your company against such threats depends on the nature of your business as well as its culture and leadership. Are your company's executives oblivious to the risks? In that case, you'll need to start by educating them. On the other hand, if they are aware of recent threats, they're likely already demanding action.

Either way, once you have a mandate to improve IT security, it's wise to begin with these components:

- A thorough assessment of the threats your enterprise faces, including all vulnerabilities and risks
- Solid security strategy goals, with tactics detailed in a company security policy
- An implementation approach that fits your organization's processes, culture and infrastructure
- The right tools and solutions, chosen for their concord with your needs, goals and methodology
- Dedication to proper ongoing management and maintenance.

"Targeted attacks, as well as worms and viruses like SQL Slammer and Nimda, are proof positive of the need to have a comprehensive corporate security policy that is approved and adopted by the senior management team," says Betty Johnson, vice president of IT at the Santa Cruz, Calif.-based Nonprofits

## Encryption Technology: Core Strength Behind Products and Solutions

**Solution Provider:** SafeNet Inc. is a global leader in information security. Founded more than 20 years ago, SafeNet offers complete security solutions—a full spectrum of best-of-class security products encompassing hardware, software, chips and intellectual property, keeping current product rankings and ratings.

SafeNet's core strength is the encryption technology behind its products and solutions. The company has been awarded 43 distinct patents, with 31 additional pending and provisional patents—many of which are also patented in various countries around the globe. As further evidence of its known leadership in the field, SafeNet has attracted more than 300 encryption engineers, building one of the largest teams of its kind in the world.



**Product and Service Offerings:** SafeNet technology is the *de facto* standard in remote-access client software and the market leader in USB authentication tokens that eliminate user names and passwords; SSL acceleration devices providing fast and secure online transactions; licensing products preventing software piracy; high-assurance security products; and SecureIP Technology licensed to Internet infrastructure manufacturers, service providers and security vendors.

**ROI:** “Our partnership enables us to offer a complete solution to our customers that is OMA DRM v2 com-

pliant while meeting the demands for increased security and flexibility,” says Cees Geel, marketing and sales director for SafeNet partner Philips Software. “Through this cooperation with SafeNet, a respected world leader in the field of mobile security, we have an ideal partner to complement our own extensive in-house DRM expertise and help strengthen our solutions yet further,” Geel says.

“SafeNet’s technology is silicon-proven. They are a profitable, financially sound company with an international presence,” says Sunil Baliga, vice president of marketing and business development at K-Micro (Kawasaki Microelectronics), a leader in advanced yet affordable ASICs. “Thus, partnering with a trusted vendor such as SafeNet will help K-Micro

quickly grow in markets that need security technology, including fiber-to-the-premises (FTTP) and network printers.”

**Customers:** Samsung, Texas Instruments, Nokia, Ericsson, NEC, ARM, Bank of America, NetGear, the U.S. Departments of Defense and Homeland Security, Adobe, the U.S. Internal Revenue Service and scores of other government, financial institutions, midsize firms and OEM customers.

**Contact information:** [www.safenet-inc.com](http://www.safenet-inc.com)  
410-931-7500  
800-696-5308

Insurance Alliance Group of Companies, which provides liability insurance for charitable nonprofit organizations.

### The starting line

“CIOs and IT managers need to take part in risk identification and, at a high level, understand controls and vulnerabilities,” says Phebe Waterfield, CISSP, a senior analyst at The Yankee Group, a Boston-based research and consulting firm.

More important, in her view, is understanding business risks, what controls are in place to mitigate those risks and

where those controls are weak or vulnerable. “The implications of this for security policy, information sharing and IT governance are, simply, visibility,” she notes. “Regulations require more visibility and greater definition around IT process and procedure. Loose processes and vague policies are no longer acceptable because they do not ensure that IT systems are operated securely.”

Chances are your campaign to reduce your organization’s vulnerability and risk will be anchored by one of these kinds of security projects:

# Managing multiple user accounts, passwords and authorizations can quickly go from overwhelming to all but impossible.

## ...Securing your network

Doing business online—even just a small amount—means changing the way you handle network security. This transformation can range from reconfiguration to a redesign of the architecture itself.

**Aligning what you have.** As enterprises open up their IT environments to the Internet, network-perimeter security techniques must adapt to two often-conflicting demands:

- The need to protect against the ballooning volume and variety of threats as well as a tightening margin between discovery and malicious exploitation of vulnerabilities.
- The need to provide easy connectivity and data access for mobile and home-based workers and outsiders, such as partners and suppliers. Obviously, such arrangements provide welcome collaboration capabilities, but they can also cause vulnerabilities that could compromise sensitive information and network security.

As a result, you may find yourself re-segmenting your network to make parts of it more secure—but at least that provides the opportunity to build closer alignments among IT, security and business needs.

**Meeting demands for connectivity.** Longer term, you may need to consider new network architectures that can isolate low-security subnets (such as one with employee information that's neither mission-critical nor confidential), as well as security policies that reflect individual business units' network security considerations based on their risk, availability and access requirements. By combining such technologies as virtual private networks (VPNs) and Secure Sockets Layer (SSL) with identity management solutions, you can enable secure, enterprise-to-enterprise partnering and collaboration.

## ...Standardizing/integrating IT infrastructure

In many corporate IT environments, the approach used to create and implement applications and systems could be summed up as seat-of-the-pants at best. Security risks, holes and vulnerabilities abound.

In the long term, you can resolve that situation by developing standards regarding software development and acquisition. That job is more easily accomplished in enterprises that are already oriented to process rationalization using methodologies such as Six Sigma and TQM, which can inject security standards and tests into existing process controls and templates.

## ...Complying with new laws

To meet regulatory requirements such as the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, the Patriot Act and the Health Insurance Portability and Accountability Act (HIPAA), your organization may need to create a set of security controls and a dedicated team to oversee them. That group should, in fact, be separate from IT, which should cede the reins over vulnerability assessment, intrusion detection and similar tasks.

Indeed, if your enterprise is affected by such regulations—and virtually all organizations are—you can expect formal IT security governance reviews to be in your future. That's because some regulations require that certain parts of an organization's information systems are sufficiently secured and the actions of authorized staff (read: systems administrators) monitored. IT staff watching IT staff doesn't meet the laws' requirements; often a separate security-control operation is needed to meet the audit requirements.

## ...Managing identities

How you approach the authentication, authorization and access control challenges inherent in enterprise-wide identity management will likely depend on what kinds of problems you need to solve.

If you're seeking help for the infrastructure you have now, implementing password management or account provisioning solutions can ease the burden of supporting your current application portfolio and provide a reduction in help-desk costs.

If you're doing business online, or preparing to do so, you already know that managing multiple user accounts, passwords and authorizations can quickly go from overwhelming to all but impossible. Rationalizing these efforts with an enterprise-wide identity infrastructure via a lightweight directory access protocol (LDAP) directory and a Web single sign-on (SSO) engine offers a foundation for:

- The kinds of federated identity capabilities on which inter-enterprise partnering, such as supply chain relationships, depends
- The centralized authorization services necessary to use Web services architectures, which can help reduce software development and maintenance costs. **CIO SL**



## IDENTITY AND ACCESS MANAGEMENT:

# Knowing Who's Who

**H**OW DO YOU GAUGE trustworthiness? With a handshake?

Intuition? A look at the other guy's driver's license?

To protect against a growing number of threats, IT infrastructures must include built-in ways to establish the credibility of employees, customers, partners and suppliers. How that's accomplished—via tasks involving provisioning, authentication, authorization, access control and auditing—is what identity management is all about.

"We must ensure that patient health information is protected and provide audits for patients who wish to see who had access to their health care records," says John Hummel, CIO and senior vice president of IS at Sutter Health Network, based in Sacramento, Calif. That means knowing exactly who users are as they log into the organization's systems.

The solution: software and procedures that can assure the identities and manage the access rights of all users, devices, applications and organizations that are attempting to interact with a company's IT resources. The Stamford, Conn.-based research and consulting firm Gartner Inc. reports that costs of identity-management solutions vary from \$5 to more than \$25 per user, but reductions in help-desk costs alone can make the technology a good investment.

Automating provisioning—that is, handling user access capabilities automatically, rather than manually—can generate significant savings as well. According to Gartner, automatic provisioning for a dozen applications in a 10,000-employee enterprise can cut costs by \$3.5 million over three years and produce a return on investment of nearly 300 percent. Such impressive returns come chiefly from a decreased need to manage user access (an annual reduction of 14,000 hours) and a 6,600-hour-per-year drop in help-desk hours. And automatic user provisioning and de-provisioning make the process of initiating, changing and ending individual access rights faster and less prone to error.

### Beginning with a directory

Most identity management systems are founded on a directory or directory service that hierarchically lists and categorizes users, devices, applications and organizations, storing such identity attributes as authentication details and access rights.

Traditionally, several distinct programs have handled these functions: One does user provisioning, another deals with passwords, a third stores authentication information. Each program, along with individual user access-control lists, must be separately maintained, synchronized and kept up to date.

These days, companies are looking for solutions that will eventually provide federated, enterprise-wide, single sign-on solutions. The objective: systems that are interconnected so that workers logged into their corporate intranets can seamlessly access partners' systems with authentication, authorization and access credentials automatically recognized and accepted across enterprises.

The goal, according to Rebecca Wettemann, an analyst at Wellesley, Mass.-based Nucleus Research, a market research firm, is "to manage integrity and security without locking down communications in a way that negatively impacts the business."

Rather than developing a single blanket policy, companies should identify key areas where documents and communications are most sensitive and look for appropriate technology to manage them. "Digital identity management coupled with digital content management and document-management solutions are good starting points," Wettemann says, "particularly if they support different access and audit levels for different users, groups of users, and types and pieces of content."

### The importance of federation

Identity management solutions will increasingly be based on Web services and federated standards designed to enhance the exchange of identity information between organizations with an EDI- or a PKI-like exchange of trusted identity characteristics. So perhaps someday in the not-too-distant future, you'll be able to count the number of passwords you use in your job on one hand.

Key to that effort is the establishment of a single identity management standard, such as the XML-based Security Assertion Markup Language, that everyone can embrace.

# Community Medical Center Improves Patient Information Security



**Customer:** Community Medical Center is the largest regional health-care provider in central California, with 16 facilities, more than 850 beds and 6,100 clinical and non-clinical employees. Community has 200 applications (legacy, desktop and Web), more than 5,000 users and 2,600 desktops—of which more than half are shared by multiple users.

**Objectives:**

- Achieve regulatory compliance—access control, audit logs, stronger security
- Provide secured access in a shared workstation environment
- Offer simplified and faster access to all applications in a highly complex and heterogeneous environment
- Revoke access for departing employees and contractors
- Use one ID badge to access both building and information systems



**Solution:** Encentuate offers an Enterprise Access Security solution that simplifies, strengthens and tracks access to information systems. The Encentuate solution is unique in that it automates sign-on/off, manages strong authentication and provides audit reports by user. Deployment is fast and cost effective because Encentuate requires no change to existing applications, uses existing ID badges and is adopted rapidly by users.

**Results/Benefits:**

- Immediate regulatory compliance
- Faster access to electronic information
- Satisfied and more productive staff
- Dramatic reduction in help-desk calls
- No need for extensive systems integration
- Ability to transparently increase security without user involvement
- Unified access across physical and information systems
- Minimal investment because the solution leverages existing infrastructure

**From the Customer:**

“The Encentuate TCI product simply works. It is easy to implement and provides a new level of convenience for both IT and for our users.

Encentuate simplifies the process of IT administration, streamlining our security management and providing consistency between platforms. Encentuate provides

our users with one secure password to our applications and flexibility to manage how users access applications, something other vendors have not easily been able to provide.”

—George Vasquez, Director of Technology Services, Community Medical Center, Fresno, Calif.

**Contact information:** [info@encentuate.com](mailto:info@encentuate.com)  
[www.encentuate.com](http://www.encentuate.com)  
 650-312-8300

Currently, several standards are battling for domination.

The competition isn't deterring identity management solutions providers, however. Encentuate's TCI solution, for instance, includes sign-on automation, integrated access across information, network and physical access systems, support for physical access cards as second-factor authentication and a roadmap that leads incrementally from passwords to a strong digital identity.

“As the future unfolds, network access devices will have to be built with strong protective shields, such as firewalls,” notes Peng Ong, founder and CEO of Foster City, Calif.-

based Encentuate. “All network access devices will have to become self-secured nodes.” The implication: Access control will move from location to identity, from where to whom.

“Until now, companies have had to make impossible choices,” Ong continues. “They could opt for a client-based point solution that makes life easy for users but does not provide layered security upgrade possibilities. Or, they could choose to integrate multiple server-based solutions, which is an expensive proposition. What's needed is a solution that combines convenience for users with central administration, all in a fast-to-deploy package.” **CIO SL**



## SPYWARE AND SPAM:

# Worse Than Ever

**O**NCE CONSIDERED mainly a problem for unprotected home computers, spyware now threatens enterprise security, turning corporate computers into spam-generating machines and wreaking other havoc. Two-thirds of consumer PCs are infected with some sort of spyware, according to estimates from the Framingham, Mass.-based research and consulting firm IDC, whose analysts describe infiltrating corporate firewalls with malicious spyware as an easy process.

Spam, meanwhile, costs U.S. businesses \$4 billion annually in lost productivity, according to estimates from The Yankee Group, a Boston-based research and consulting firm. A recent *CSO* magazine Sensor Survey identified spyware as the No. 2 security-related concern (behind “blended threats” combining the characteristics of viruses, worms, Trojan horses and malicious code with server and Internet vulnerabilities). Spam, or unsolicited bulk e-mail, was No. 3 because it clogs networks and serves as a vehicle for other security threats, such as viruses, worms and Trojan horses—all listed individually among the CSOs’ top 10 concerns.

“My greatest concern is really spam—the cost and effort of keeping up with spam is tremendous—as well as viruses and worms,” says John Hummel, CIO and senior vice president of IS at the Sacramento, Calif.-based Sutter Health Network.

### Why you should care about spyware

Spyware is software that, without authorization, selects private information on a computer and sends it to a third party.

The problem began with adware, which often appears benevolent because it offers users “free” screensavers, download accelerators or other applications. Home users typically install those programs without realizing that they’re likely subjecting themselves to pop-up ads, erratic browser behavior and other side effects.

Now employers face related problems: the loss of network bandwidth due to unsolicited advertising traffic, overloaded help-desk staff who must clean up adware-laden desktop and notebook computers, and liability risks because users can be unwillingly exposed to unsavory Web sites.

In addition, spyware can carry:

- **Keystroke logger/screen capture software** that surreptitiously installs and hides itself and then records keystrokes and screenshots that can be used to reconstruct a user session, enabling the theft of passwords and other confidential information. Such information can be used to break into networks and databases.
- **Hacking programs** such as password crackers and Trojan horses that, once successfully deployed on unsuspecting

## Richard Petty Driving Experience Blocks Multiple Internet Threats

### CASE STUDY

**Customer:** The Richard Petty Driving Experience gives racing fans the ultimate thrill of racing in a mega-horsepower stock car around a competition-style speedway. Founded in 1994 by NASCAR legend Richard Petty, the Concord, N.C.-based company currently operates 20-plus tracks nationwide, offering enthusiasts a chance to experience everything from a 165-mph ride with a professional driver to the adrenal rush of taking 40 laps behind the wheel.

#### Objectives:

- Block spyware from infiltrating the network
- Prevent spam from degrading e-mail server performance
- Stop employee Internet abuse

#### Solution:

SurfControl e-mail and Web filters provide robust multilayer protection against escalating threats from spyware, phishing attacks, spam, pornography and viruses. SurfControl E-mail Filter manages employee e-mail usage and significantly reduces security threats, legal liability, network abuse and loss of productivity. Through risk recognition, flexible rules, reporting and administration, SurfControl Web Filter manages employee Internet access and stops malicious software, inappropriate content, recreational surfing and other threats.



#### Results/Benefits:

- Decreased spyware incidence by 45 percent
- Reduced individual mailbox spam by 95 percent
- Filtered 35,000 spam messages in the first week alone
- Enabled end-user management of spam to prevent loss of legitimate e-mail
- Implemented blacklisting to block known spam servers
- Reduced time spent on e-mail administration
- Tracked Internet usage by employee to investigate suspected abuse

#### From the Customer:

“Because we are a well-known organization, we get hit with a lot of spam. The day I installed

SurfControl E-mail Filter, 4,000 messages were filtered out immediately. My users really like the end-user spam management feature. They get to look at their own mail and help manage the system, which reduces the time I spend managing the product. And before SurfControl Web Filter, we had no way to track Internet abuse or usage. SurfControl’s reporting is a big benefit because it lets me track these activities. We’ve also seen a decrease in spyware.”

—**Kevin Craig**, IT Director, Richard Petty Driving Experience, Concord, N.C.

**Contact information:** [info@surfcontrol.com](mailto:info@surfcontrol.com)  
[www.surfcontrol.com](http://www.surfcontrol.com)  
831-440-2500

users’ computers, can be used remotely at any time to break into other systems.

- **Dialer programs** that can be used to change local dial-up Internet service provider telephone numbers to costly long-distance numbers.

### Best practices for dealing with spyware

Here are some techniques for protecting your company, computers and employees from spyware and adware:

- **Teach your users about the risks** associated with downloading adware, shareware, freeware and other programs from the Internet. Where possible, forbid them from doing so.

- **Train high-risk workers to recognize signs of threats.** You’ll want your help-desk staff, for instance, to be able to recognize both human and automated attempts to elicit passwords.
- **Develop protections for gateways.** URL filtering can be used to block known adware sites; download filtering can neutralize adware programs and reduce their bandwidth consumption.
- **Boost protections for clients.** Keep in mind that people accessing your network remotely won’t be affected by gateway controls. Institute protective measures such as keeping client browser software patched and locking down desktop computers so that new applications can’t

be downloaded unless they're on an approved list.

- **Implement two-factor authentication**—that is, two ways of determining identity, such as a password and a fingerprint—especially if you're concerned about password theft.
- **Clean up desktop systems** using anti-spyware tools such as those from Tokyo-based Trend Micro and Islandia, N.Y.-based Computer Associates.

## Best practices for deflecting spam

Make no mistake: Spam represents a genuine security threat. Unsolicited junk e-mail blocks the availability of resources and, when it carries a virus, becomes an immediate danger to the health of the enterprise. Following are some ways to reduce the flood of spam:

- **Don't list e-mail addresses on your Web site.** Use a fill-in-the-blanks e-mail form or a graphic image of an e-mail address with no HTML code.
- **Server-side encode your e-mail addresses.** You can avoid displaying e-mail addresses in HTML code by encasing them in a server-side encoder that generates addresses on the fly.
- **Disguise e-mail addresses.** The idea is to fool the automated Web spiders, but not the humans who are looking for addresses. Thus, `jdoe@xyz.com` is disguised as `jdoeDELETE@xyzTHIS.com`.
- **Use less obvious e-mail addresses.** Rather than `jdoe@xyz.com` or some similarly rational address scheme using variations on employee names, consider making addresses less intuitive to thwart brute-force dictionary spamming.
- **Use e-mail aliases.** Create "front" addresses so that the real e-mail address is shielded by another address—or even several addresses—on which you place filters that admit desired e-mails and quarantine or delete the rest.
- **Authenticate incoming e-mail.** One prevailing technique is a "challenge-response" system based on the philosophy that "good" e-mail comes from legitimate senders that are on your approved list. With such solutions, when e-mail comes from unapproved sources, your server automatically replies with a message instructing senders to confirm their identities. Once they've done so, they're added to your list and their e-mails are accepted.
- **Don't become part of the problem.** This means hardening your hosts and servers to eliminate vulnerabilities, finding and getting rid of spyware, closing open relays and, of course, carefully controlling access.

In addition, products such as the Web and e-mail-filtering solutions from SurfControl plc, which is based in Cheshire, England, can block sites that host spyware, software download, instant messaging and other potential threats. **CIO SL**

# NETWORKS AND INFRASTRUCTURE Help for IT

**T**HE NUMBERS TELL IT ALL. Fully 78 percent of those participating in the 2004 Computer Security Institute/FBI Computer Crime and Security Survey detected virus attacks in their corporate networks, while nearly 40 percent reported intrusions. More than half had found that their systems had been used in unauthorized ways; more than a third had discovered that users had been able to access information they weren't authorized to see.

"The reason why firewalls exist is because of an oversight in the design of the first generation of networked computers," says Peng Ong, founder and CEO of Foster City, Calif.-based Ecentuate Inc. "We just did not expect that computers would be connected to so many other computers, and we did not design them with sufficient security. As network access devices—such as PCs, laptops, PDAs and phones—get more mobile, the traditional way of securing them by putting them in a 'secure' environment has become unworkable."

While it seems like absolute security for IT networks and infrastructures remains a futuristic idea, welcome new solutions are emerging to address enterprise-wide security needs.

## Integrating threat management

Wherever you begin in your quest to improve enterprise information security, you'll eventually find yourself considering narrowly focused point solutions, especially if they offer leading-edge capabilities. And so you'll have to consider the pros and cons in this version of the age-old debate between the virtues of point versus integrated solutions.

Certainly the arguments for integrating threat management are appealing:

- Too often information security and physical security are separate, uncoordinated endeavors. Physical security issues—such as building designs offering clear sightlines, no hidden stairways, and so on—tend to get short shrift.
- Point solutions handle a limited set of tasks that too often trigger false alarms, may not reveal larger patterns and are difficult and costly to centrally manage. Intrusion-detection systems (IDSs), for instance, use either signature files or heuristics to predict attacks, but are too often wrong. Vulnerability-assessment scanning systems spot network

# Supporting Sound IT Practices



**Solution Provider:** The Information Systems Audit and Control Association® (ISACA®) is a global leader in IT governance, control, security and assurance. ISACA is dedicated to supporting individuals in achieving high levels of organizational performance and conformance through the application of sound information security, IT assurance and IT management practices.

**Product and Service Offerings:** The association strives to provide the elements needed by any growing professional discipline: original research, practical education, career-enhancing certification, industry-leading standards and best practices, a network of like-minded colleagues, professional resources and technical/managerial publications. ISACA administers the globally recognized Certified Information Systems Auditor® (CISA®) and Certified Information Security Manager® (CISM®) certifications. The association hosts international conferences and training events, and publishes a leading technical publication, the *Information Systems Control Journal*.

**ROI:** In the three decades since its inception, ISACA has become a pace-setting global organization. ISACA's CISA certification has been earned by more than 38,000 professionals. Its CISM certification uniquely targets the information security manage-

ment audience and was recently named by *Certification* magazine as one of the top 10 new certifications. More than 5,100 professionals have achieved the CISM designation, and CISM continues to grow in stature and influence.



“The business market has become truly global. Management and control over IT transcend geography, and, as a result, certifications that are internationally recognized are critical to ensure a consistent approach, background and skill set,” Marios Damianides, CISA, CISM, and a partner at Ernst & Young LLP, told

*Certification* magazine in January 2004. ISACA provides that consistency in IT management and control not only with its global certifications, but also with its highly regarded standards, research, educational opportunities and membership program.

**Customers:** ISACA recognizes that it must provide products, services and benefits to the wide range of IT professionals who work to ensure reliable information and systems. ISACA's constituency includes IS auditors, IT security managers, academics, consultants, internal auditors, CIOs, external auditors, CEOs and a host of others.

**Contact information:** [www.isaca.org](http://www.isaca.org)  
[info@isaca.org](mailto:info@isaca.org)  
 847-253-1545

hosts in need of software patches but tend not to help administrators figure out what to fix first, since they can't incorporate IDS scans and predictions.

Some IT security solution providers are addressing these weaknesses with integrated threat management solutions that combine key elements in point security solutions.

One example: Securify Corp. of Cupertino, Calif., whose solutions address overall infrastructure security. Under Securify's approach, a traffic-policy engine inspects all network traffic, classifying it as either good or bad and giving administrators a complete, real-time view of network-security status. This information is then integrated with IDS and

vulnerability assessment functionality to pick up on attacks, anomalies and weaknesses.

## Updating security infrastructure

Thanks to the Internet, old approaches to enforcing static network-security perimeters are giving way to newer, more dynamic ones. Organizations need dynamic infrastructures able to automatically enforce security policies enterprise-wide by:

- **Limiting users to the resources they're authorized to access.** This policy makes it easier to lessen the risk of data exposure and minimize the impact of attacks.

# Informing your non-IT colleagues about the risks of poor security is just as important as keeping your own staff up-to-date on the subject.

- **Continually monitoring traffic for both policy violations and threats.** This practice makes it simpler and less costly to sustain business continuity because threats can be more quickly spotted, contained and addressed.
- **Screening devices and users.** That means verifying credentials and scanning devices for policy and configuration compliance as well as the presence of threats (such as viruses) before granting access.

Currently, several initiatives aiming to build solutions that screen devices and granularly enforce security policies are in various stages of development. These include Cisco's Network Admission Control (NAC) access management, Microsoft's Network Access Protection (NAP), and the Trusted Computing Network (TNC), from an industry alliance—the Trusted Computing Group—that includes such vendors as Symantec, Trend Micro, Network Associates, and Juniper Networks.

Meanwhile, companies such as San Francisco-based Vernier Networks, offer network access-management appliances that complement firewalls and can be deployed at the network edge.

## Incorporating encryption

Regardless of the kind of network you operate, encryption technology can help you stave off network attacks, especially when used in concert with strong authentication, firewall, intrusion detection and security-assessment technologies.

It's true that even encrypted information can be captured by attackers. But actually deciphering that information requires the right encryption key. In addition, crypto-based authentication typically frustrates hijackers because the data being illicitly inserted can't be properly authenticated.

You can strengthen security by injecting encryption into multiple network layers or adding it to hosts, switches and so on. To maximize security at the links between your corporate systems and your network access points, you can implement encryption safeguards so that information is secured before it gets sent out onto the open Internet or into a partner's intranet.

Encryption solutions provider Safe Net Inc. of Belknap, Md., recommends taking the following steps to minimize encryption deployment risk and cost:

- Opt for federally-endorsed (NIST, ANSI) security

strength, such as Triple-DES.

- Integrate public key infrastructure (PKI) technology for strong authentication and digital certificates.
- Plan scalable network and security management systems if your enterprise runs large networks with thousands of nodes
- Use carriers that offer a secure ATM or frame-relay public data network service.
- Build solutions that integrate ATM or frame-relay with IP solutions to ensure that your security policy evolves in response to your business needs.

## Staying on track

The daily bombardment of new threats and vulnerabilities—a new virus, another round of “phishing,” spyware-laden spam attacks—can drive CIOs and their staffs to distraction. So it's important to maintain your focus on what matters most.

“We desperately need to pay more attention to assessing risk and vulnerability, and measuring security,” says Phebe Waterfield, CISSP, senior analyst for The Yankee Group, the Boston-based research and consulting firm. “We cannot manage what we cannot measure.”

Informing your non-IT colleagues about the risks of poor security is just as important as keeping your own IT staff up-to-date on the subject. “Once non-IT managers and staff are educated about security, they become much more effective at identifying security risks in their own processes and projects,” observes Betty Johnson, vice president of information technology at The Nonprofits Insurance Alliance Group of Companies, which provides liability insurance for charitable nonprofit organizations.

Annual security audits and penetration testing conducted by outsiders can also help stave off disaster. “This testing validates existing security controls, exposes security weaknesses and offers the opportunity for immediate remediation,” Johnson points out. “Choose a vendor that is a recognized leader in the field of security testing. And take the time to perform due diligence—that is, research scope, check references and so on, before initiating a service agreement.”

Above all, be honest. Don't try to skirt the real issues regulators are targeting: privacy, identity theft and fraud. Says Waterfield: “It's tempting to aim to pass the audit with as little effort and cost as possible—but it's important to tackle the issue with ethics and integrity.” **CIO SL**

## Ensuring Effective IT Governance

**Solution Provider:** The IT Governance Institute (ITGI) was established in 1998 to advance international thinking and standards in directing and controlling information technology. By hosting conferences and offering original research and case studies, ITGI assists enterprise leaders and boards of directors in their responsibilities regarding IT governance. ITGI helps ensure that IT is aligned with business objectives, delivers value, is measured, mitigates risks and is properly allocated.

**Product and Service Offerings:** To provide guidance to organizations of all sizes and industries around the world, ITGI developed Control Objectives for Information and related Technology (COBIT), the internationally accepted framework for control over information, IT and related risks. Other ITGI publications include:

- *COBIT Security Baseline*
- *Board Briefing on IT Governance, 2nd Edition*
- *Information Security Governance*
- *IT Control Objectives for Sarbanes-Oxley*
- *IT Governance Implementation Guide*

**ROI:** According to the *IT Governance Global Status Report*, more than 91 percent of executives recognize that IT is vital to the success of their businesses—but more than two-thirds of CEOs aren't comfortable answering questions about governance and control over their IT processes. That's the case despite the

impact of the Sarbanes-Oxley act and increased scrutiny worldwide focusing attention on the IT processes that underlie financial systems.

According to the *Global Status Report*, companies that place IT on the board agenda reported:

- Better measurement of IT performance
- Better management of risk and IT resources
- Better delivery of business value through IT
- Better alignment of IT with company strategy



**Customers:** IT governance activities are implemented by international businesses, government entities and other organiza-

tions. Case studies focusing on specific implementations are available at [www.itgi.org](http://www.itgi.org). Organizations profiled include:

- Allstate Corp.
- Charles Schwab & Company
- Ernst & Young AG/Switzerland
- Datasec, Uruguay
- U.S. House of Representatives
- Mendoza, Argentina
- Curtin University of Technology, Australia
- City of Mesa, Arizona

**Contact information:** [info@itgi.org](mailto:info@itgi.org)  
[www.itgi.org](http://www.itgi.org)  
 847-590-7491