

**NETWORKWORLD<sup>®</sup>**

**EXECUTIVE GUIDE**

# Compliance

**can** be an opportunity for  
**Network Improvements**

COMPLIMENTS OF

**ciena<sup>®</sup>**

## Table of Contents

---

<a href="#">Introduction</a> .....	3
<b>Advice from the experts</b>	
<a href="#">Risk management, internal controls are key to Sarbanes-Oxley compliance</a> .....	5
<a href="#">Mismanaging information can lead to embarrassing compliance problems</a> .....	6
<a href="#">Achieving compliance means striking a balance between risk and cost</a> .....	7
<a href="#">Compliance drives companies to replace legacy apps</a> .....	9
<a href="#">Compliance: A horse is a horse</a> .....	10
<b>Real-world tactics for achieving compliance</b>	
<a href="#">Management software takes on compliance role</a> .....	11
<a href="#">Compliance drives interest in identity management</a> .....	13
<a href="#">Continuous data protection is vital for compliance</a> .....	14
<a href="#">Users look to existing software for compliance help</a> .....	15
<b>The dark side of compliance: What happens when things go wrong?</b>	
<a href="#">Worst-case scenario: Can an IT professional end up going to jail for a compliance violation?</a> .....	16
<a href="#">Kaiser Permanente patient data exposed in major breach of privacy laws</a> .....	18
<a href="#">LexisNexis: 280,000 more possible data theft victims</a> .....	19
<a href="#">Companies rush to plug 'data leaks'</a> .....	20
<b>Show me the money: How mandates are affecting IT budgets</b>	
<a href="#">Regulatory requirements have IT jumping through hoops, although mandates also drive bigger security budgets</a> .....	22
<a href="#">Regulatory requirements, mainly Sarbanes-Oxley, continue to squeeze IT budgets and staff</a> .....	23
<b>Hidden wrinkles in the compliance scenario</b>	
<a href="#">How compliance can impact your data center</a> .....	26
<a href="#">How compliance can be complicated by outsourcing deals</a> .....	30

---

# Introduction

**F**ederal regulations such as the Health Insurance Portability and Accountability Act and the Sarbanes-Oxley Act are driving increased corporate spending on key IT areas such as security, authentication, access control and document management.

According to AMR Research, U.S. companies will spend \$15.5 billion on compliance-related activities this year. Spending on Sarbanes-Oxley alone is expected to increase from \$5.5 billion last year to \$6.1 billion this year, as companies try to automate many of their processes.

Preliminary research from Nemertes Research shows that security will grow from 2.4% to 4.8% of the average company's IT budget in 2005, an increase attributed almost entirely to the demands of regulatory compliance.

For example, at Network Health in Cambridge, Mass., administrators OK'd a doubling of the IT department's security budget to achieve HIPAA compliance. "HIPAA brought the visibility up to senior management, and we made five additional purchases for security purposes that probably wouldn't have been on the radar without it," says Eben Berry, IS manager.

At the Red Robin Gourmet Burgers restaurant chain in Colorado, "SOX was very much the driver for getting Configuresoft Enterprise Configuration Manager and other tools," says Bill Randall, the chain's IT director. "When we knew SOX was coming down the pike, we used it as an opportunity to better document our procedures," he says. The company also rolled out NetIQ's Security Manager to centrally monitor and analyze network logs.

"At the beginning of the year, we hadn't budgeted for this at all," Randall says, but the company analyzed SOX's requirements and decided that automation was the way to go.

Similarly, WellSpan Health in Pennsylvania decided to

deploy Courion's user-provisioning software to centrally track how 6,000 users accessed applications. "For HIPAA, we had needed to more robustly manage IDs," says CIO Buddy Gillespie. "It cost us between \$75,000 and \$100,000, but it was reasonable enough to fit into our HIPAA budget."

## Compliance tools and tactics

Regulatory compliance is a broad mandate that encompasses a variety of specific technologies. Here are some tools and tactics being used by companies to keep the auditors happy:

- ❑ **Security event management:** Calpine, a San Jose power producer recently installed an appliance from SEM vendor Network Intelligence to get a handle on logs and to more easily generate reports. "We were literally overwhelmed with security data and information. We were seeing 1,200 events per second from our firewalls alone," says Sean Curry, infrastructure engineering manager at Calpine. He adds, "We are in the second phase of [the Sarbanes-Oxley Act], and it has given us the ability to prove we have a segregation of duties because of the data it collects. It also makes getting reports to non-technical people easier."
- ❑ **Identity management:** Corporate requirements to adhere to compliance regulations and a need to automate and secure electronic interaction among partners are the major issues driving inter-

## Introduction

est in identity management, according to users and analysts. “There is an awareness occurring among business folks that security is not baked into infrastructure and applications, and that identity and access management play a key role and serve as a cornerstone for applying controls to address information security and compliance auditing issues,” says Earl Perkins, a Gartner analyst.

- ❑ **Continuous data protection:** CDP is a relatively new technology so definitions vary somewhat, but CDP software is aware of all changes in data as the changes occur and it saves both the changed data and the metadata describing the change (a timestamp and pointers to where the changed data is located). It also enables users to recover literally from any point where a change has been made.
- ❑ **Data leakage protection:** This threat entails employees leaking sensitive data about customers, finances or intellectual property in violation of security policies and regulatory requirements. Sometimes it’s by mistake and sometimes the employee is looking to make a financial gain, but the products are able to monitor sensitive information and block outgoing e-mails or instant messages containing it.
- ❑ **Security operations center:** Regulatory pressure is driving the development of security operations centers. “SOX is a good example of a proactive driver for SOCs,” says Diana Kelley, executive security adviser at Computer Associates’ eTrust division. She adds that SOX calls for executive management to take responsibility for establishing and maintaining an adequate internal control structure. “That means you need the correct and effective controls on your business reporting. And once you have them, you need to monitor and maintain them, and a SOC is an effective way to do that.”

Companies also are finding that existing network monitoring and management tools can do double duty, continuing in their basic function as well as providing the reports needed for regulatory compliance.

This executive guide will cover the range of compliance issues, including strategic advice from today’s top thought leaders, nitty-gritty tips on what tools to deploy, and examples of how your peers are dealing with compliance.

# Advice From the Experts

## Risk management, internal controls are key to Sarbanes-Oxley compliance

■ By Daniel Blum

Good information security professionals don't need a regulation to tell them it's important to protect their business. But, overprotecting the business? That's another matter.

Section 404 of the Sarbanes-Oxley Act's (SOX 404) focus on internal control has been a welcome call to action for some; others say it goes too far. A variety of companies and industry associations presented the Security Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) with a litany of complaints and suggestions at the SEC's public roundtable last month.

The backlash against SOX 404's high documentation, testing and audit costs probably will lead the PCAOB to rein in overzealous auditors. The SEC also might provide more relief for small companies, which already obtained an extension of their compliance deadline to July 2006.

Beyond such changes, few would advocate throwing the baby (SOX's investor protections) out with the bath water (excessive SOX 404 audits). Besides, SOX 404 compliance brings its own rewards for companies, if scoped correctly.

PCAOB's current guidelines call for companies to develop internal controls based on risk management considerations — what risks to accept, avoid or transfer before rushing in with protective measures. Moreover, the cost of protections should be proportionate to the consequences they prevent or other benefits they bring to the business. If SOX is causing your company to increase emphasis on risk management, that's a good thing in itself.

SOX risk management runs a bit sideways to traditional risk management, which focuses on preventing major losses. SOX doesn't care, so to speak, whether the company loses money, as long as it accurately reports on losses. Therefore, SOX remediation should pay the most attention to locations, systems and applications that deal directly with large amounts of financial information. Companies should make sure that auditors do the same.

Along with scoping, companies must develop a control framework for SOX. This framework, consisting of control objectives and control activities, should be based on the nature of the business and its information security program. It should contain no more and no less than is required to protect resources in scope for SOX compliance.

While SOX compliance is expensive, much of the effort is reusable. Every company should be doing risk management, for example. Many control activities — such as

deploying firewalls, access controls and audit logs — represent best practices you should be following anyway.

While SOX compliance is expensive, much of the effort is reusable. Every company should be doing risk management, for example. Many control activities — such as deploying firewalls, access controls and audit logs — represent best practices you should be following anyway.

SOX 404 itself is unlikely to go away. Companies should treat its mandate as an opportunity to strengthen risk management, information security and compliance to a growing body of regulations — not just SOX. The trick is to document control frameworks for SOX and any other regulations in such a way as to limit the scope of SOX audits but reuse appropriate security practices and control activities across the business.

*Blum is senior vice president and research director with Burton Group, an integrated research, consulting and advisory service. He can be reached at danjblum@yahoo.com.*

Advice From the Experts

## Mismanaging information can lead to embarrassing compliance problems

■ *By Johna Till Johnson*

I've written a fair amount lately on the topic of "information stewardship." In case you've missed it, information stewardship is the discipline of ensuring that an organization's data is:

- ❑ As accurate and complete as possible (data-quality management).
- ❑ Appropriately secured, with access granted only to appropriate parties (information protection).
- ❑ Auditable and compliant with pertinent privacy and disclosure guidelines (indexing and records retention).
- ❑ Stored on the most appropriate and effective mechanisms (information life-cycle management).
- ❑ Reliably backed up and available in the event of a failure (business-continuity planning and disaster recovery).

So far, I'm finding that few organizations have a consistent, coherent framework covering all these points — much less the technology and processes to manage it. Moreover, most of the companies tell me that information stewardship (though they usually don't call it that) is the single-most critical strategic challenge they're facing.

I agree. While it's hard to pin hard-dollar numbers on the cost of an ineffective information-stewardship policy, several recent events highlight the urgency. Recently, Time Warner announced that it lost sensitive data, including names and Social Security numbers, for 600,000 employees. Time Warner's data was on back-up tapes maintained by storage facility provider Iron Mountain and was apparently lost in transit to the storage facility. In February, Bank of America lost back-up tapes containing credit-card records for more than 1 million government employees, and ChoicePoint was attacked by identity thieves who gained access to sensitive customer data.

That's not all. Famed investment bank Morgan Stanley was recently ordered to pay a whopping \$604 million in a legal suit, primarily because the company said it was unable to find e-mails pertaining to the case. (Effective records retention and indexing is a key component of information stewardship.) And a recent study by Financial Executives International found the average cost of Sarbanes-Oxley compliance to be \$4.4 million, using a base of 217 companies with average revenues of \$5 billion.

The bottom line is that companies need to move now to create and adhere to effective information-stewardship policies. Start an information stewardship task force today, and include participants from within corporate finance,

As noted cryptographer and security guru Bruce Schneier says in a recent article in *Communications of the ACM*, "In the information age, virtual privacy and physical privacy don't have the same boundaries. We should be able to control our own data, regardless of where it's stored."

legal and compliance teams, as well as IT.

But that's not enough. Our entire legal framework needs to be revamped and rethought in the context of information stewardship. Recent court cases have reached contradictory conclusions about which information can be considered private, or what legal hurdles are required to disclose it. As noted cryptographer and security guru Bruce Schneier says in a recent article in *Communications of the ACM*, "In the information age, virtual privacy and physical privacy don't have the same boundaries. We should be able to control our own data, regardless of where it's stored."

Amen.

Step 1 is for organizations to tackle the problem within their own boundaries. Step 2 is to rethink the broader public policy on information stewardship in the context of 21st century technology.

Advice From the Experts

**Achieving compliance means striking a balance between risk and cost**

■ By David Lawson, Network World

Best security practices don't exist. If they did, the company implementing them would be spending too much money trying to secure its information, and worse, more than likely stopping the business from operating. The best practice an organization could do is to evaluate its risk, comply with applicable standards at the minimum level required, and implement just enough control to achieve that state.

There are organizations, such as certain three-letter government agencies, or R&D aspects of firms with high-value intellectual property, transactional or money transfer systems, that require best and state-of-the-art security. For most of the IT world, successful IT professionals balance the cost and onerousness of security controls, and IT costs in general, to obtain an appropriate and acceptable level of risk.

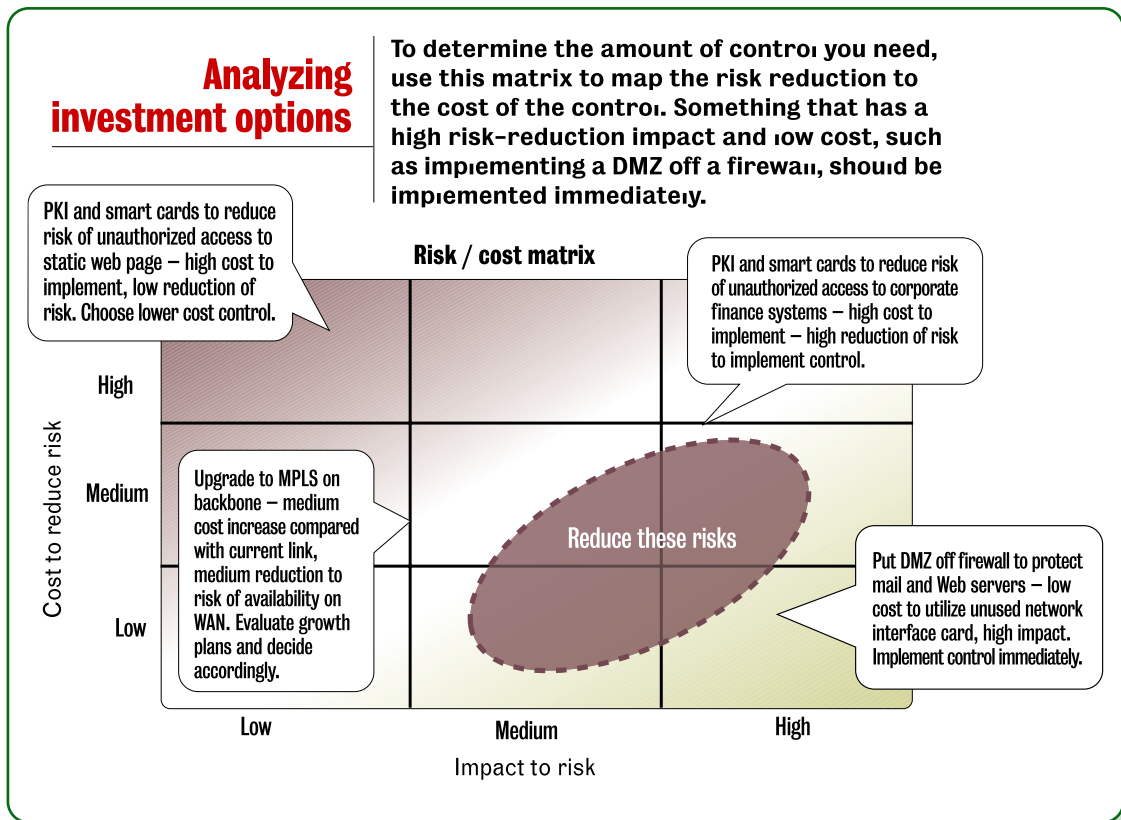
The Food and Drug Administration's Web page on information security states that GxP is the current standard for various regulatory compliance areas for pharmaceutical companies. GxP represents Good Practices, not best prac-

tices. That is, Good Manufacturing Practice or Good Clinical Practice. This is a bit odd: Good enough was the plan of the day for manufacturing life-saving drugs.

Looking further, building codes define "minimal acceptable standards" that homes, lots and structures have to meet to be used. Similarly, in the legal community, there is the standard of the reasonably prudent person. Doctors and other professionals are typically only held to a standard of reasonable or ordinary care, not excellent or the best possible care.

So IT and business professionals should not be asking for best practices, they should determine appropriate and reasonable controls to protect information and maintain compliance with federal regulations. Interestingly, even the regulatory guidelines allow flexibility in approach to controls, as long as the information is adequately protected and based on the use of a documented risk assessment to determine this reasonableness and appropriateness.

To determine if you're spending the appropriate amount on security controls, perform risk assessments for every significant technology decision. Documenting the outcome and how you arrived at your decision helps your organization meet regulatory and legal requirements, and earns you the respect and admiration of the business units and bean counters.



## Advice From the Experts

Take, for example, a network architecture migration. Engineers presented a fully redundant, resilient design for a branch office. The design specifications were based on what the engineers termed a "best practice" and on input from the remote workers who said they had to be on the network, or their work would grind to a halt.

A risk assessment was performed. Although important, the remote site could be down for several hours before a significant effect would be felt by the overall organization. The office and network staff overestimated the importance of the operation to the business and built a design almost four times as expensive as it needed to be, based on the cost to buy highly available equipment and twice as much of it. The security/risk team suggested a lower level of availability equipment and saved the organization money. The best practice was too much for the job.

Most people who aren't accustomed to abstract risk concept tend to group threats together as a "bad thing that could happen." Listing threats as one makes the procedure easier to IT and business to follow and provide valid input. Group similar things together and gain consensus on the final list.

There is a simple, facilitated procedure to do this, normally at one of the meetings that is already a part of the design and decision-making process. The National Institute of Standards and Technology 800-30 process says to identify threats and vulnerabilities and identify controls mitigating those risks already deployed ("current controls"). Keeping those in mind, estimate the likelihood of the threat and the impact of the exploit of the vulnerability. This defines the "risk".

The easiest way to do this is to make a list of all the threats and vulnerabilities. Most people who aren't accustomed to abstract risk concept tend to group threats together as a "bad thing that could happen." Listing threats as one makes the procedure easier to IT and business to follow and provide valid input. Group similar things together and gain consensus on the final list.

The goal should be to have a reasonably sized list - 10 to 50 is a good amount. For example "unauthorized access to a Web application" can catch all the hacking, exceeding authorized access, and looking at other information risks to

a company. From this list, rate each one as high, medium or low for probability and impact. This should be fairly simple to do: Most people intuitively know viruses occur frequently, and natural disasters don't.

Use this list to gauge the amount of control you need. Obviously a high probability/high impact risk needs more control to bring it to a medium/medium, or a low/medium. Something that reduces a high/high to a low/low has normally reduced too much risk and cost too much. Use a simple chart (see graphic below) to map the risk-reduction to the cost of the controls. A high-risk reduction impact that has a low cost should be implemented immediately.

For example, an internal firewall to control access to payroll and finance is critical for Sarbanes-Oxley Act compliance. However, a high cost/low reduction control, such as using similar firewalls to segment every server in the company, is probably a waste of money.

A successful IT professional leader should focus on how much risk needs to be alleviated, and how much will various controls cost to do that. When you really do need to implement an additional control, this process will help you pick the least-expensive one.

As David Lynas, executive director of security organization The SABSA Institute, says, "Spend absolutely every penny you need to on security... but not a penny more."

*Lawson is vice president/director of the Global Security Practice and Facility Security Officer at Greenwich Technology Partners. He can be reached at [dlawson@greenwich.tech.com](mailto:dlawson@greenwich.tech.com).*

## Advice From the Experts

**Compliance drives companies to replace legacy apps**

■ By Zach Nelson

Neil Young says it's better to burn out than fade away. Maybe in life that's the case, but in the world of legacy applications, fading away is, realistically, what usually happens. There are many reasons why companies keep a portion of their IT infrastructure on legacy applications — oftentimes from fear of pulling the plug. These firms should consider this: The power of moving at least their core applications over to a modern, integrated system can deliver huge benefits. Here are three reasons why:

- ❑ The competitive factor. Some 95% of our clients adopt NetSuite to replace patched-together legacy systems that can't share essential data. The lack of transparency throughout the system, these firms have found, seriously hampered their ability to compete. Compare tracking an order in a legacy system to a modern, Web-based integrated application. Order management is a process that starts from the first point of customer contact and ends with the fulfillment of the order. Older systems required a great deal of expensive customization to link this process across a salesforce automation module, ERP system, order management application, and then the warehouse and fulfillment systems. Often glitches will remain - data, say, must be entered multiple times at multiple points and customer information usually remains siloed throughout the system.
- ❑ Regulatory issues such as the Sarbanes-Oxley (SOX) Act. Depending on the industry, the process of managing customer data must be relentlessly tracked and ready to be produced to auditors at a moment's notice. Other new regulations, especially privacy laws, touch upon customer data. Here, the main challenge is that too many systems are providing access to customer data. Ultimately, SOX is about the processes for managing data, not the data itself; therefore, reducing the number of legacy applications required to run your business will certainly make SOX compliance easier and less expensive.
- ❑ Newer systems are far easier to use. User interfaces in legacy systems, especially first-generation ERP systems, rarely match the way people actually do their jobs. They also require the intervention of highly (and expensively) trained IT staff. Consider predictive analytics, an essential component to most marketing and sales systems today. To use them in legacy systems, engineers trained specifically in these methodologies must do the programming. Newer applications, by contrast, have

analytical applications built directly into the marketing and sales operations. A typical business user can program and use this embedded functionality with little or no assistance.

Also, when the application is delivered through the Internet, users have 24/7 access to real-time data. In an integrated Web-based system, data never has to be entered more than once - the most common origin of mistakes - and its status is available to everyone from the accounts receivable department to customer service to a sales rep trying to land yet another order with the same customers.

*Nelson is president and CEO of NetSuite, a provider of integrated business application software. He can be reached at [znelson@netsuite.com](mailto:znelson@netsuite.com).*

There are many reasons why companies keep a portion of their IT infrastructure on legacy applications — oftentimes from fear of pulling the plug. These firms should consider this: The power of moving at least their core applications over to a modern, integrated system can deliver huge benefits.

## Advice From the Experts

**Compliance: A horse is a horse**

■ By Dave Kearns

One of the hottest topics over the past year is "compliance auditing." Regulations from the Health Insurance Portability and Accountability Act to the Sarbanes-Oxley Act require that computer access to data not only be tightly controlled but also heavily monitored, logged and audited. Some regulations require auditing all users and resources and being able to tell — at any point in time — which objects could possibly access which other objects and why they should be able to.

This is a far cry from the typical forensic auditing that network professionals did just a few years ago, when audit logs were really only read after a problem had occurred in an attempt to determine who (or what) might have caused the situation. Still, there also have been major advances in these security-monitoring functions.

Let's say there's a very up-to-date horse ranch, with sensors all over the barns wirelessly connected to the ranch network. Constant monitoring of comings and goings of horses and cowboys is logged. Access to individual stalls is controlled with proximity cards, and a verifiable record of who can access which horses is always available.

One morning, it's discovered that the barn door is open and all the horses are missing.

Old-style audit logging would require that we now sit down and read through the logs to discover who was (probably) the last cowboy to leave the barn. "Probably," because if that cowboy didn't lock the door, then there's no record of him leaving. We need to match up all entrances and exits to see where there was an entrance (logon) without a corresponding exit (logout). But the horses are still gone.

If the rancher has good regulatory compliance auditing tools, he could query the command console to see who had access to the barn - and to each horse's stall - during the hours that the security breach might have taken place. He can show the federal investigators whether he was in compliance with all regulations regarding horses, barns and data security. But the horses are still gone.

An up-to-date ranch network armed with sensors, detectors and rules would have noted that the barn doors were unlocked after the time set for them to be locked. It would have noticed horses out of their stalls at a time they should-

n't be. It would have noted a human presence when none had logged on. And it would have responded by locking the door before the horses got out.

What about your company's "horses"? Can you stop them from getting away?

*Kearns, a former network administrator, is a freelance writer and consultant in Silicon Valley. He can be reached at [wired@vquill.com](mailto:wired@vquill.com).*

Some regulations require auditing all users and resources and being able to tell — at any point in time — which objects could possibly access which other objects and why they should be able to.

# Real-world tactics for achieving compliance

## Companies are turning existing management software into compliance tools

■ By Denise Dubie

Growing demands to get their networks in line with compliance regulations and maintain consistent policies are forcing many companies to reassess how they secure and manage their networks.

Network management technologies such as traffic monitoring, packet analysis and policy-based management are finding their way into new and existing security tools. Systems management vendors are adding security capabilities to perform vulnerability scans, distribute patches and help customers maintain compliance.

For example, Lancope and other vendors are developing products to baseline typical network traffic and perform ongoing monitoring to detect problems that might indicate a security breach. Others, such as Elemental Security, provide technology to help IT managers establish policies and monitor network events against the policies to ensure that networks remain compliant. Current security event management (SEM) vendors are adding more automation, remediation and policy-based management features to evolve their tools from simple log-collection products into security-compliance tracking tools.

"I wanted a centralized area where I could see all the security events for the company, but I saw more than just security issues," says Matthew Keogler, senior security and network engineer at AutoTrader.com in Atlanta. Keogler installed an SEM product from GuardedNet about two years ago and said it not only provided a dashboard of security events but also helped him discover unknown network security threats. "The product immediately showed me misconfigured servers and some network issues that are related to security. I still use it from time to time to patrol and clean up the network."

The trend toward securing networks with network management technologies has attracted not only a slew of newcomers but also Cisco - with its Network Admission Control (NAC) initiative - and IBM. Industry watchers predict that it's only the beginning.

## A hot market

According to The Yankee Group, the overall security industry in 2004 generated about \$12.9 billion in revenue, and of that SEM accounts for a modest \$250 million. Yet the research firm projects by year-end, the SEM market will grow by more than 30% to about \$330 million. In fact, by 2008 Yankee Group says security management will be an \$800 million market.

"This is an area that is going to attract big systems management vendors, like BMC, Computer Associates, HP and IBM," says George Hamilton, a senior analyst with The Yankee Group.

For instance, systems management vendor Altiris last week announced its Altiris Security Suite, which couples vulnerability scans with remediation tools. NetIQ earlier this month unveiled its Security Compliance Suite, which lets users perform vulnerability scans, security log

management and compliance-report generation by using a combination of centralized console software and distributed agents on managed machines. At its annual users' conference in two weeks, HP also is expected to introduce compliance management wares.

Often referred to as security information management (SIM), SEM technologies appeared a few years ago with vendors promising to take the legwork out of collecting and making sense of thousands of event logs spit out of intrusion-detection systems, firewalls and other devices. The products typically consist of software, servers and agents, or probe appliances that collect logs from devices.

While the task seemed simple - apply the event collection and correlation technologies of network and systems management tools to security devices - the products provided IT managers with much-needed respite from poring over log data.

"We were literally overwhelmed with security data and information. We were seeing 1,200 events per second from our firewalls alone," says Sean Curry, infrastructure engineering manager at Calpine, an independent power producer with 102 sites across the country and headquarters in San Jose. "We had six firewalls that produced 60 gigabytes of log data per day - each. It was difficult to back up, difficult to compress quickly, difficult to use for reports."

About 18 months ago, Curry installed an appliance

Network management technologies such as traffic monitoring, packet analysis and policy-based management are finding their way into new and existing security tools.

Advice From the Experts

## Blurring the lines

Customers can benefit from network management products that can spot performance problems and security threats.

Technology	What it does	Available from
<b>Network-anomaly behavior detection</b>	Monitors traffic flows and inspects packets to provide an early warning of potential security threats.	Arbor Networks, Lancope, Lumeta and Q1 Labs.
<b>Policy-based management</b>	Combines tools to create internal and external compliance policies with ongoing monitoring and enforcement features.	BindView, Elemental Security, Lockdown Networks, NetIQ and Procera.
<b>Security event/information management</b>	Automates the collection of log data from security devices and helps users make sense of it through a common management console.	ArcSight, eIQnetworks, E-security, GuardedNet, Intellitactics, netForensics, Network Intelligence and OpenService.

from SEM vendor Network Intelligence to get a handle on the logs and to more easily generate reports, which had become more in demand because of the company's internal IT governance initiatives. He says while the product was used initially as a tool to reduce manual labor and better manage log data, it now helps Calpine stay in compliance.

"We are in the second phase of [the Sarbanes-Oxley Act], and it has given us the ability to prove we have a segregation of duties because of the data it collects. It also makes getting reports to non-technical people easier," Curry says.

As companies face compliance challenges, security management vendors are adding out-of-the-box reporting tools to help ease the process. Companies such as ArcSight, eSecurity, Network Intelligence and eIQNetworks this year have separately released products specific to reporting on compliance regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbox and the Gramm-Leach-Bliley Act. The tools generally provide report templates specific to regulations, which helps IT managers automatically generate detailed compliance reports.

Rick Casteel's purchase of TriGeo technology centered on ongoing HIPAA compliance, but he says the tool has evolved to automate security remediation tasks. The vice president of information security at Upper Chesapeake Health System, a healthcare provider for Hartford County in Bel Air, Md., says the TriGeo software helps him monitor

some 30 servers and 600 client machines for malicious activity, investigate port scans and track malicious behavior. More important to HIPAA, though, are the automation features that Casteel says TriGeo provides.

"HIPAA requires us to prove a business continuity planning, which means we have to prove that no matter what we can keep services running," Casteel explains. He says TriGeo notifies the IT team of events that could affect its HIPAA compliance and automatically generates trouble tickets to the help desk before a user notices the problem. "We can be paged that the service has stopped, set a rule that if this happens then restart the service, and the software does it automatically."

As SEM vendors continue to tap customers' compliance concerns, Yankee Group's Hamilton says enterprise scalability and storage capabilities will hold some back. He also warns the technology - and the smaller niche companies - will become acquisition targets for vendors such as HP and IBM that have begun promising to help IT departments get a better handle on IT controls and policies. Hamilton expects to see the technology serve as a cornerstone for vendors' IT governance strategies.

"Security management vendors have gotten a lot of attention in the enterprise market because of the present state of urgency over compliance," Hamilton says. "But the value of the technology is much broader and will be about putting defined IT controls in place and constantly monitoring those controls. Compliance is just one piece of that."

## Advice From the Experts

**Compliance drives interest in identity management**

■ *By John Fontana*

Corporate requirements to adhere to compliance regulations and a need to automate and secure electronic interaction among partners are the major issues driving interest in identity management, according to users and analysts.

Those issues, along with others focused on privacy, trust, federation and rights management, are the highlights of this week's Digital ID World conference in San Francisco.

While identity management has focused mostly on IT tools such as directories, single sign-on and password management, observers say businesses are starting to realize how important identity is becoming in risk management plans. Experts say awareness will accelerate adoption of identity management.

"There is an awareness occurring among business folks that security is not baked into infrastructure and applications, and that identity and access management play a key role and serve as a cornerstone for applying controls to address information security and [compliance] auditing issues," says Earl Perkins, an analyst with Gartner, who will lead a panel on compliance auditing at the conference. "They finally understand this is all part of risk management, and I view that as a sign that identity management is taking a more rightful place in the minds of business folks."

However, Perkins and others realize that the technology issues are not yet solved. In March, Oracle's acquisition of Oblix was widely seen as the end of vendor consolidation and the start of a new task for vendors developing identity platforms, including BMC Software, Computer Associates, HP, IBM, Microsoft, Novell, Sun and RSA.

"All the platform players have the pieces that they think they need or wanted to buy," says Jamie Lewis, president of Burton Group, who will deliver a keynote speech at the conference. "But these suites are suites in brand name only. The vendors have a lot of work to do creating products that don't overlap, that are tightly integrated on features and functionality, that have a consistent management platform and are all tied together in a package that can be exposed through development tools."

Lewis says another major step is getting those disparate suites to interoperate using standard protocols.

A panel discussion at the conference on convergence of federated identity protocols, one of the most contentious areas of debate around identity standards, will feature the Liberty Alliance, IBM, Microsoft, RSA and Sun.

"Standard-based identity, policy and security interoperability is critical to all our members operating in complex

multi-vendor, multi-national environments," says Fred Wettling, chairman of the Network Applications Consortium, an end-user group. "One of the IT challenges is how do I reduce the labor burden that has been foisted on people by mandates such as Sarbanes-Oxley in order to become compliant? We need to figure out how we can automate and this is an area where standards-based interoperability is key."

In addition to those issues, a handful of vendors are expected to announce products. RSA plans to introduce Reporting and Compliance Manager, which provides analysis on the logs generated by RSA's access management platform ClearTrust. The reports focus on adherence to policy, policy changes, user activity and intrusion attempts. Epok plans to unveil the next version of its Trusted Data Exchange Server, which will include features for integrating identity management systems.

**By the end of 2007,  
Gartner predicts  
that nearly  
**10%**  
of companies will have  
deployed or be piloting  
projects that will  
include federated identity  
services.**

## Advice From the Experts

**Continuous data protection is vital for compliance**

■ *By Mike Karp*

What is continuous data protection (CDP), and why should e-mail admins look into it?

CDP is a relatively new technology so definitions vary somewhat, but the key points are that the CDP software is aware of all changes in data as the changes occur and it saves both the changed data and the metadata describing the change (a timestamp and pointers to where the changed data is located). It also enables users to recover literally from any point where a change has been made.

What is the difference between CDP and a snapshot? Snapshots capture changed data at regularly occurring intervals, on a defined schedule. With a CDP approach, each change is recorded at the time it occurs.

The purpose of CDP is to provide the best levels of granularity possible, which means being able to recover even the smallest quantity of changed data, even when that change occurred only a few seconds ago.

The purpose of CDP is to provide the best levels of granularity possible, which means being able to recover even the smallest quantity of changed data, even when that change occurred only a few seconds ago.

E-mail messages that arrive and are then erroneously discarded soon after their arrival run the risk of being lost forever, assuming in the worst-case scenario that the "Deleted" folder has been emptied. At best, this can result in serious interruption of your workflow, leading to all sorts of expense. At worse, people can go to jail if the lost data falls within the regulatory demands of the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA) and the like.

Lots of new CDP software is becoming available from vendors, and some of it is aimed specifically at providing protection to e-mail applications. An e-mail administrator would be foolish not to be aware of this trend.

When considering a CDP solution for e-mail, here are some things to look for:

- ❑ Recoveries should happen much more quickly than you are used to. CDP solutions back up data to disks (most likely, SATA), and recovery time objectives should be in seconds rather than hours.
- ❑ Make sure the new solution will coexist with the e-mail software you already have in-house. Your IT team is likely to come up to speed more quickly if the software doesn't require changes to existing policies.
- ❑ Can users do the recoveries themselves? The more advanced CDP implementations require little or no IT intervention and will place no drain at all on your helpdesk team.
- ❑ All solutions will include backup and archiving. A few will also offer a complete business continuity package, including remote replication for disaster recovery.
- ❑ There is no reason why regulatory compliance solutions can't be a part of a package like this. Find out whether the vendor you are speaking with offers a module for HIPAA, Sarbanes-Oxley, National Association of Securities Dealers (NASD) 3010, or whichever regulations answer your company's needs. Managing compliance and data protection from a single console (and storing all e-mail data and metadata in a single data repository) would be much easier than any alternative.
- ❑ Make sure whatever solution you consider will play nicely with Microsoft's new Data Protection Manager (DPM), the disk-to-disk back-up application scheduled to arrive from Microsoft by year-end. Find out if your vendor has thought this issue through.

Obviously, if the new software can also do away with the need to save multiple instances of an object (sent out 300 e-mails with an attachment to your coworkers? Exchange has saved 300 copies of the attachment!), that would be a very good thing indeed. It is easy to see how saving a single instance of an attachment sent out to multiple recipients at your site will save you all kinds of hardware investment down the road. Also, because single-instancing will reduce the size of your Exchange store, you can expect improved storage manageability, reliability and overall Exchange performance.

Application-versant CDP can be a great boon to protecting e-mail messages. IT managers in general, and e-mail admins in particular, would be silly not to look at this new technology.

## Advice From the Experts

## Users look to management software for compliance help

■ *By Denise Dubie*

When it comes to management software, there's something to be said for double dipping.

Take Aram Eblighantian's experience consulting for mailing giant Pitney Bowes.

He bought the BigFix Enterprise Suite last year to help his client get its patching processes under control. Never did he anticipate that he'd be using the same package to standardize client and server configurations across the company's network.

"I would have definitely considered buying another product, especially to collect and standardize configurations," he says. "Because [the BigFix suite] is agent-based, it can return a fair amount of information on the clients and systems in the organization, down to the hardware properties, the locations of the machines and who logs on to them. From there it segues into asset management, then change management and so on."

While budgets have loosened some in the past year, many IT shops remain in "get more for less" mode. This is encouraging companies to look closer at software that can be used not only for management, but also security, compliance and other jobs. Industry watchers say that vendors are even getting into the act.

"Every vendor is worried about keeping their customers and keeping them happy," says Jasmine Noel, a principal analyst at Ptak, Noel & Associates. "They will work to uncover hidden capabilities to ensure their product does not become shelfware."

Companies such as Altiris, Peregrine Systems and BMC Software have started pitching compliance with their desktop and systems management wares. Security information vendors such as ArcSight, Network Intelligence and OpenService are packaging their security event filtering products to also alert IT managers of compliance rules.

The key issue for customers is whether they risk stretching a product too far, says Stephen Elliot, a senior analyst at IDC. "IT managers need to determine if, say, a network management tool that can collect log data will give them the visibility they need into the security logs on network devices."

Before they start shopping for compliance tools, IT shops also might look closely at their current management tools to determine whether these products might help meet regulations such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act. AMR Research recently forecast that U.S. companies will spend about \$15.5 billion on compliance-related activities this year.

"There are tools that have strong workflow processes that can be used to address compliance," says Audrey Rasmussen, a vice president with research firm Enterprise Management Associates (EMA). "Some products are being sold as 'process out of the box' to simply document processes. Service management products can do that now, and the majority of vendors

would support configuring their software to meet compliance goals."

Jason Kennedy, senior analyst and system engineer at Tsunami Communications in Vancouver, Canada, says syslog collection tools, such as HP Network Node Manager, also could be put to work on compliance projects.

"If you have a syslog-enabled device, such as a firewall, you can point a monitoring tool at it to collect syslog data, and it will comb the data and flag anything that doesn't sync up with compliance or security policies," he says. Kennedy says SNMP-based monitoring tools could also be used to compile an inventory of IT assets to document for potential audits.

"For smaller companies, rolling out an agent-based asset management tool is just too much of a time and cost expense. Monitoring tools like WhatsUp Gold can poll devices and get information such as the make and model number, and what's in the [management information base]," he says.

"If you toy around with most tools and approach them creatively, you can find a few different angles to take and get more out of them," Kennedy adds.

Lynn Nye, president of research firm APM Advisors, says companies don't need to look too far to find a management tool that can serve multiple purposes.

"The Swiss Army knife of our industry is still the Sniffer where people never seem to run out of uses for it," he says.

"You can do more than just see traffic," Nye says. "Instead of buying software to see what's coming in and out of your network, you can use a Sniffer to develop a way to compare flows on both sides of devices so someone could analyze what is going on across a switch or router."

Companies also might find they don't need to buy special patch-management tools.

"People have a lot of different management tools, and one real good way to reuse your software distribution tool is for patch management," says Debbie Joy, director of next-generation networks for the western region of Unisys in Phoenix. "There is a lot of duplication among products."

"It's rare for IT departments to inventory the tools they have across the silos. It would be more practical to purchase a patching module from your systems management vendor than create a new relationship with a patch management vendor, and vice versa," she says.

Stretching management tools to handle network-security tasks is only natural, some experts say.

"Security management tools, including vulnerability and patch management, grew out of network management tools," says Scott Crawford, a senior analyst with EMA. "[Intrusion-detection systems] and [intrusion-prevention systems] are based on the ability to look at a packet, which is network traffic analysis."

He says security is a sensitive enough area that not everyone will be sold on double dipping.

"IT managers will buy a tool labeled 'security' because it's an area where they feel they can't get by with just a 'good enough' solution," he says.

# The Dark Side of Compliance: What happens when things go wrong?

## **Worst-case scenario: Can an IT professional end up going to jail for a compliance violation?**

■ *By Paul McNamara*

Prison? ... An IT guy? ...  
For violating HIPAA or Sarbanes-Oxley ? ...  
Could it really happen?

It's known as the "go-to-jail scenario" in IT circles, a confluence of events that might land a CIO or network executive not just in hot water, but behind bars. You've probably heard loose talk about this risk at industry conferences and in the press. But can an IT exec actually end up doing hard time - as opposed to being fired or fined - for violating one of these federal laws?

The jury is still out. Everyone we talked to pretty much agrees that the go-to-jail scenario is a long shot that would require overt bad deeds far beyond simply screwing up. But no one was willing to entirely rule out the possibility of a stretch in the slammer, either.

Clearly, the legislation and regulations governing the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act and the like include criminal penalties: up to 10 years in prison with HIPAA for "obtaining or disclosing protected health information;" 10 to 20 years with SOX for "destruction, alteration or falsification of records," just to cite two examples.

And a former cancer clinic worker in Seattle became the first person convicted of criminal charges under HIPAA last November. The sentence: 16 months for using patient information to fraudulently obtain credit cards. Experts say this case isn't all that instructive in terms of how these laws will be applied toward IT executives because this type of outright fraud has always carried the threat of prison.

But the reality is that more IT professionals are finding themselves in the enforcement cross hairs. "There's no question that more and more people from the IT world are becoming responsible for electronic records management," says Bob Williams, president of Cohasset Associates, a Chicago consulting firm that specializes in document management. Primary responsibility for electronic records management rests with IT in more than 70% of organizations, according to a Cohasset Associates survey of 2,200 records-man-

agement professionals. And with that primary responsibility comes vulnerability to enforcement penalties.

"Clearly Sarbanes-Oxley holds out prison as a possibility, but I think that it is more likely to occur for senior management than even a CIO," says Williams. That "more likely" is the type of caveat that experts sprinkle throughout their ruminations on this subject,

### **HIPAA CRIMINAL PENALTIES**

Any person who knowingly obtains or discloses individually identifiable health information in violation of the Administrative Simplification Regulations faces a fine of up to \$50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a \$100,000 fine, and up to five years in prison. Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of \$250,000, and imprisonment for up to 10 years.

which may or may not lend comfort to IT professionals who find themselves in a compliance-related crossfire.

"Maybe we should say it backwards: Can you definitively say an IT person would not go to jail?" says Jonathan Redgrave, an attorney with the Washington office of Jones Day, who specializes in electronic records issues. "You can't say that they wouldn't; it really depends on the facts of the situation."

The U.S. Department of Justice, which is charged with assessing alleged HIPAA violations sent to it from the Office for Civil Rights within the Department of Health and Human Services, couldn't provide much in the way of clarification.

If the Justice Department agrees that a HIPAA complaint warrants criminal prosecution, it will forward the case to the U.S. Attorneys Office nearest the infraction. "It is a case-by-case basis, and the scrutiny has to be made on each and every one to determine whether the government is going to prosecute," says Charles Miller, a spokesman for the Justice Department. As for hypothetical situations involving IT personnel, the government cannot offer blanket assurances about avoiding jail, he says.

## Advice From the Experts

**Where there's a will ...**

Willfulness of action would likely be a key component weighed by any enforcement authority, Redgrave says, and if an IT person was found to be a willing participant in any attempt to illegally access, delete or cover up protected records it is more likely that criminal penalties would apply. Simply doing a lousy job isn't likely to land one in jail, he says.

"Where you get the criminality is with obstruction of justice, like the Arthur Anderson situation," Redgrave says. "Let's say you are someone in the IT department at Arthur Anderson and you decide it's a good idea - even though you know the SEC is coming - to allow purges to take place or press the system operator to have the purge take place: You're getting closer to a problem."

Craig Rhinehart, director of compliance markets and products at FileNet, sees the threat in more cut-and-dried terms. "Yes, IT professionals can go to jail," he says. According to Rhinehart, the challenge for IT professionals will be balancing the immediate risk - an agitated boss at their door right this moment - against the future risk of being held accountable for a compliance violation that may carry criminal penalties.

"Some senior manager comes to an IT administrator and says 'I need to have access to these files.' If you give him access, you may have just become an accomplice to a crime," Rhinehart says. "You can't tell me that most mid-level or even senior IT managers [won't acquiesce] if the CEO or CFO comes marching into their office and says they need to check on a few things."

The key to avoiding that scenario is a clear set of policies and procedures for managing any information that might be subject to corporate governance laws or litigation, Rhinehart says. "If not, you leave the interpretation up to the individual and that's where trouble starts," he says. "If there's no clear policy in place you might be doing something that is technically illegal." You also might have a harder time fending off the executive who is demanding access to a particular set of records.

The bottom line is that preparation beats complacency, Redgrave says. "People talk about this and while it's not an everyday occurrence, there certainly is an element of risk such that the people involved really need to understand what they're doing."

**SARBANES-OXLEY: SEC. 1519. DESTRUCTION, ALTERATION OR FALSIFICATION OF RECORDS IN FEDERAL INVESTIGATIONS AND BANKRUPTCY**

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies or makes a false entry in any record, document or tangible object with the intent to impede, obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

## Advice From the Experts

**Kaiser Permanente patient data exposed in major breach of privacy laws**

■ *By Linda Rosencrance*

A disgruntled former employee at Kaiser Permanente, a health maintenance organization in Oakland, Calif., posted a link to a Web site containing the personal information of 140 Kaiser patients – an effort, she said, to call attention to a potential breach of privacy laws by the company.

The company is now seeking a restraining order in Alameda County Superior Court against the woman, known as the "Diva of Disgruntled," who posted the information on her Web log, according to Kaiser spokesman Matthew Schiffgens.

Schiffgens said the woman continued to post the information despite a cease-and-desist request from Kaiser, which learned about her allegations in January from the U.S. Office of Civil Rights – the enforcement arm under the Health Insurance Portability and Accountability Act. The federal agency began looking into the matter after the woman filed a complaint with it.

The company is investigating whether it had a hand in exposing the data.

According to Schiffgens, the data exposed included contact information such as names, addresses and telephone numbers, as well as medical record numbers that are unique identifiers within Kaiser Permanente. For a very small portion of the HMO's members, some routine lab information was also posted, he said.

Kaiser is now contacting the affected patients while it tries to determine on its own how the patient information became public. The former employee, whose first name is Elisa, said she stumbled on it while doing a search for information about the company; Schiffgens denied that the data would have been publicly available.

"We're aware of the individual's allegations as to Kaiser Permanente posting this information to the Web," he said. "Our investigations have not been able to determine that, and we continue to investigate how this information came into her possession. What I can say is that Kaiser had a Web site that made various different schematics available so that remote IT people could do their work and see the schematics of the systems they were working on."

Elisa, who described herself in an e-mail message to Computerworld as a former "Web coordinator" for the HMO, claimed that the Web site she found contained diagrams of Kaiser systems, as well as the confidential patient data. In fact, she said she accessed the site using Google.

"I had been trying to dispute my termination, but Kaiser would not allow (me) access to any of the documentation I needed," said Elisa, who was terminated in June 2003. "I was searching online for any information I could find. My former manager's name is on the systems diagrams, so they came

up in the course of research. There was no hacking involved."

Schiffgens said the diagrams, which at time were not behind a firewall or password-protected, were related to an application that generated letters for the lab reporting system. "The lab system itself was behind our firewall and was password-protected," he said.

The Web site showing the system diagrams is also now behind the firewall and password protected, he said.

Schiffgens also said the schematics had nothing to do with Kaiser's HealthConnect program – the system that will organize and integrate clinical information for the company's approximately 8.3 million members across the U.S.

"Kaiser has been trying to convince Congress that it should take a leading role in the development of a national Electronic Medical Record," Elisa said. "But Kaiser is a profoundly sloppy organization that lets part of its intranet leak online to be indexed by Google and allows either employees or consultants in highly sensitive areas to post system specs on a public Web site. The federal government needs to start asking questions about whether Kaiser can back up its promises when they start bidding for EMR projects."

With that in mind, Elisa said she included a link to the Kaiser site on her own Web site.

"I did not post this information: I linked to the original site, which seems to have been posted by a Kaiser employee or insider," Elisa said. "I found the Kaiser System Diagrams online at <http://tripod.docviewer.com> in July 2004. You can see the remains of the site and the fact it has been online since at least December 2002 at [http://web.archive.org/web/\\*/http://docviewer.tripod.com](http://web.archive.org/web/*/http://docviewer.tripod.com)," she said.

Elisa also said that, in her opinion, publicly distributing diagrams of systems that partly constitute California's transitional Electronic Medical Records system is an even bigger deal than the patient privacy issue. With that in mind, she contacted the Office of Civil Rights, which then contacted Kaiser officials about the potential breach.

"We are continuing that investigation and continue to have discussions with OCR," Schiffgens said. "On March 9, we asked the ISP to remove the posting (from Elisa's Web site). After we concluded that real member information was included in the site, we took swift action to contact the ISP and have it removed. But she reposted it twice, and the ISP removed it both those times."

In response, Elisa, who then posted a copy of the site she had made, said she planned to remove the post once the issue had been publicly aired.

"My intent was to take it down after the Office of Civil Rights had done a proper investigation or Kaiser otherwise came under public/government scrutiny," she said. "The site remained up while I was trying to figure out what to do next."

Officials at the Office of Civil Rights could not be reached for comment.

## Advice From the Experts

**LexisNexis: 280,000 more possible data theft victims**

■ *By Paul Roberts*

An internal investigation at the LexisNexis division of Reed Elsevier has uncovered evidence that as many as 310,000 more people may have had their personal information exposed to unauthorized individuals who compromised the security of a massive database of public and private information, including Social Security and drivers license numbers.

An in-depth review and analysis of two years' of search activity uncovered 59 incidents of unauthorized access to information, LexisNexis said in a statement. The news follows revelations in March that intruders used the IDs and passwords of legitimate LexisNexis customers to gain access to information on 30,000 people whose information was stored in "Multistate Anti-Terrorism Information Exchange," (MATRIX), a database and information retrieval system managed by LexisNexis's Seisint division. The latest report from the company expands the number of potential victims by 280,000.

An in-depth review and analysis of two years' of search activity uncovered 59 incidents of unauthorized access to information, LexisNexis said in a statement. The news follows revelations in March that intruders used the IDs and passwords of legitimate LexisNexis customers to gain access to information on 30,000 people whose information was stored in "Multistate Anti-Terrorism Information Exchange," (MATRIX), a database and information retrieval system managed by LexisNexis's Seisint division. The latest report from the company expands the number of potential victims by 280,000.

LexisNexis did not immediately respond to request for comment. Seisint collects data on individuals that is used by law enforcement and private companies for debt recovery, fraud detection and other services.

LexisNexis, of Dayton, Ohio, Monday sent letters notifying those whose information may have been viewed during the incidents, and will offer free support services to those who are notified, including credit bureau reports, fraud insurance and credit monitoring services for one year. Individuals who have been victimized will be able to receive fraud counseling services, the company said.

In most of the 59 incidents uncovered by the investigation, the hackers stole passwords and IDs from legitimate Seisint customers who were legally permitted to view the sensitive information. The company's infrastructure was not hacked or penetrated, nor was customer data accessed or compromised, LexisNexis said.

The company will be improving customers' password and ID administration and security, according to the statement.

The new disclosures from LexisNexis bring the Seisint MATRIX database compromise into a league with ChoicePoint, of Alpharetta, Ga., which agreed in February to tell 145,000 potential victims that ID thieves, in a breach of its database, may have gained access to personal information such as Social Security numbers and credit reports.

Data breaches at ChoicePoint, LexisNexis and elsewhere have made data brokers the focus of intense scrutiny.

Since disclosing its security breach, ChoicePoint has been the subject of a Federal Trade Commission inquiry into its compliance with federal information security laws, a U.S. Securities and Exchange Commission (SEC) investigation into possible insider stock trading violations by its CEO and chief operating officer, and lawsuits alleging violations of the federal Fair Credit Reporting Act (FCRA) and California state law.

In March, the company said it will stop selling sensitive consumer data to many of its customers, except when that data helps complete a consumer transaction or helps government or law enforcement.

Some members of Congress have also called for new laws that would regulate the type of information that can be gathered and shared.

A 2003 California state law, Senate Bill 1386, requires organizations that maintain computerized databases of personal information on state residents to notify them if the security of their private information is compromised. Experts have credited that law with prompting disclosure of the breaches at ChoicePoint and LexisNexis, even though many of those notified by the companies are not California residents.

## Advice From the Experts

**Companies rush to plug 'data leaks'**

■ *By Ellen Messmer*

The threat entails employees leaking sensitive data about customers, finances or intellectual property in violation of security policies and regulatory requirements. Sometimes it's by mistake and sometimes the employee is looking to make a financial gain.

To combat data leakage, a growing number of vendors are pitching products designed to monitor sensitive information and block outgoing e-mails or instant messages containing it. This week alone, newcomer Fidelis Security Systems will debut, veteran player Vidiis will change its name and launch a product, and Tablus will reveal plans to deliver a product that combines network- and desktop-based monitoring.

Data-leakage prevention products typically work by being allowed access to databases to keep track of what an organization considers sensitive data and compare it with what goes out. But questions of false positives, missed leaks and its expense - \$100,000 is not an unusual price - have kept leakage detection in a niche reserved for a limited group of companies and government agencies.

**Inside jobs**

"It does stop e-mail with sensitive data," says Janet Behnke, IT manager at First Financial Credit Union in Los Angeles, which uses a gateway from Vidiis (now called PortAuthority Technologies) at its Internet access point. The product is used to watch for sensitive information, including customer account numbers, balances and ATM card numbers.

Most credit union employees whose e-mail is blocked by PortAuthority - the average is 20 to 25 unauthorized e-mails per day - are sending out sensitive data by mistake, Behnke says. But there have been instances where the bank caught employees forwarding customer information to brokers in order to make money.

"They did it because they were trying to get commissions," Behnke says, adding that these employees were terminated. PortAuthority "saved us from a lot of exposure," she says.

This insider-theft problem is similar to that facing Bank of America and Wachovia, which in late May acknowledged massive data leaks involving stolen account data on tens of thousands of customers sold by bank employees.

Bank of America, which says it has deployed the Vontu information-leakage product, declined to say where the content monitoring helped in uncovering the problem, which involved use of e-mail as well as simply printing out customer information.

A Bank of America spokeswoman says the bank could-

n't discuss the forensics while the investigation, which includes the Department of the Treasury as well as the Hackensack, N.J., police, continues.

While corporate users of information-leakage detection products say the offerings are effective in general, they acknowledge that the products aren't perfect.



**PortAuthority CEO Pete Foley says there is tremendous opportunity to thwart unauthorized disclosure of sensitive information.**

PortAuthority registers false positives every day, Behnke says. "It's pretty low, maybe 1%, but it happens," she adds.

"We do get false alerts often," says Jeff Karafa, CFO and head of operations at the Community Bank of Dearborn, Mich., which has deployed leakage-prevention products from another vendor, Reconnex. Nevertheless, the Reconnex iGuard monitoring and blocking product has proven its worth since being installed in February, he says.

"We had an employee who innocently sent out a list of customers but forgot to encrypt the file," he says. "It caught that."

In a rarer instance, the bank caught an employee copying and sending out confidential information deliberately for more nefarious purposes. "This person was dismissed," he says.

Strict regulatory requirements in the banking industry for data privacy is driving its adoption, Karafa says.

Both he and Behnke say the data-leakage prevention products they use are a help in supplying evidence when it's needed to confront suspicious behavior.

Advice From the Experts

<b>Plugging leaks</b>			
<b>A sampling of products designed to keep sensitive information from leaving companies.</b>			
<b>Company</b>	<b>Product</b>	<b>Price</b>	<b>Availability</b>
<b>Fidelis</b>	DataSafe	\$100,000	Now
<b>Reconnex</b>	iGuard 1300	starts at \$25,000	Now
<b>Tablus</b>	Content Alarm (combines network and desktop-based technology)	starts at \$75,000	August
<b>PortAuthority Technologies (formerly Vidius)</b>	PortAuthority (adds support for internal e-mail monitoring and blocking)	starts at \$20,000	Now
<b>Vontu</b>	Vontu 4.0 (adds blocking of outbound e-mail content)	starts at \$150,000	May

**Battling for customers**

Despite such praise, most of the network-based data-leakage prevention vendors don't count more than two dozen customers each, even though some of the companies have been around for a couple of years.

Fidelis, with its DataSafe product for monitoring e-mail, instant messaging and Web traffic, has four customers: the Washington, D.C., public school system; the city of Alexandria, Va.; the Pension Benefits Guaranty Association; and an Israeli telecom provider.

Fidelis founder and CEO Timothy Sullivan says he likes to call the \$100,000 DataSafe gateway an "extrusion prevention system," a phrase the company is copyrighting.

Most of the data-leakage prevention vendors - and some of the venture capital firms backing them - seem hopeful about the future despite a small customer base.

The newly renamed PortAuthority Technologies just gained \$13.4 million in funding from Greylock Partners, Sequoia Capital and Lexington Ventures with which to further develop its line and promote a new version of its software intended to monitor and block internal mail.

Although PortAuthority claims only 22 customers, new CEO Pete Foley is bullish. There's a "tremendous opportunity to address a significant enterprise challenge - unauthorized disclosure of sensitive information," he says.

However, some analysts say such vendors are having trouble breaking out of a niche. The expense of the products, plus competition from digital rights management companies, has kept network-based data leakage and prevention something of a luxury item.

"There's a bit of a shooting match between what we sometimes call 'egress information protection' and digi-

tal rights management, which involves enterprise use of encryption," says Trent Henry, an analyst at Burton Group. It's not clear whether one or the other will be widely adopted, but companies likely won't deploy both, he says.

However, with news about identity theft and data leaks making the front page almost every week, the data-leakage prevention vendors say awareness of the problem is becoming more acute all the time.

"There's a sense of urgency driven by the compliance issue," says Tablus CTO Jim Nesbit.

CEO Jim Ponte adds that solving the insider threat problem "is not only a network issue but one that needs to be addressed at the desktop, as well."

To that end, Tablus this week announced that by August it will have a version of its Content Alarm product that combines network- and desktop-based monitoring. The desktop content-monitoring technology was gained through the acquisition of Indigo Security in February. This would make Tablus the only network-based data-leakage prevention vendor to include a desktop monitoring component.

# Show me the money: How mandates are affecting IT budgets

## Regulatory requirements have IT jumping through hoops, although mandates also drive bigger security budgets

■ By Ellen Messmer

As challenging as the security demands imposed by some new regulatory requirements have been, they've also presented IT managers with a golden opportunity to make network improvements.

Of particular influence have been the Sarbanes-Oxley (SOX) Act's financial reporting standards for publicly traded companies and the Health Insurance Portability and Accountability Act (HIPAA), federal security rules for patient data that take effect next month for healthcare organizations.

For companies that spent several months striving to understand SOX or HIPAA, the requirements brought good news: For some IT departments, upper management generously opened purse strings to acquire new auditing and security protections.

"Sarbanes-Oxley has been a way to improve audits for compliance reasons," says Jim Flynn, systems manager for security policy and strategy at UPS in Atlanta.

"SOX was very much a driver for getting Configuresoft's Enterprise Configuration Manager and other tools," says Bill Randall, IT director at Red Robin Gourmet Burgers, a Greenwood Village, Colo., restaurant chain.

Configuresoft's ECM, which Red Robin added to 30 servers and about 200 workstations, documents and tracks operating system and application configurations and password changes, while ensuring compliance with a written policy.

According to Randall, that capability helps meet the SOX requirements that organizations document their systems for auditing purposes.

"When we knew SOX was coming down the pike, we

used it as an opportunity to better document our procedures because we know this will be part of the financial audit, which includes the SOX audit, that our auditor Deloitte will do later this year," Randall explains. "The IT audit is a big part of that review because IT is the gatekeeper for the financial controls."

Manual documentation and audit and policy-enforcement process would have taken Red Robin's IT department more than 12 hours, but automating the process through ECM reduced it to 10 minutes.

Red Robin also deployed the NetIQ Security Manager to centrally monitor and analyze network logs across the network, which included firewalls and intrusion-prevention systems.

"At the beginning of the year, we hadn't budgeted for all this," Randall says of the unexpected bonanza. But as the company examined its own practices, it became clear that SOX compliance would mean hiring more systems experts or implementing better automation - and Red Robin opted for the latter.

United Parcel Service (UPS), which has 360,000 employees, is choosing to approach SOX compliance by deploying security best practices across the board. UPS is giving everyone the handheld dynamic-password token SecurID from RSA Security for two-factor authentication to remotely access applications such as payroll benefits. The worldwide package delivery firm also is using IBM Tivoli's identity management software to automate user provisioning.

"Sarbanes-Oxley has been a way to improve audits for compliance reasons," says Jim Flynn, systems manager for security policy and strategy at UPS in Atlanta.

Regulations such as SOX and HIPAA don't exactly spell out what technologies must be used to stay on the safe side of the law. However, many IT managers appear convinced that regulatory compliance in the end will come down to the commonsense notion of best practices in management of identity, passwords, system logs and vulnerability assessment.

"For HIPAA, we needed to more robustly manage IDs," says Buddy Gillespie, CIO and vice president at WellSpan Health, a healthcare provider in Southeast Pennsylvania, which deployed Courion's user-provisioning software to centrally track how 6,000 users accessed applications.

"It cost us somewhere between \$75,000 and \$100,000, but it was reasonable enough to fit into our HIPAA budget," says Gillespie, adding upper management pays close attention to meeting HIPAA's security rules for protecting

## Advice From the Experts

unauthorized access to patient data.

Eben Berry, manager of IS at Network Health, a health-care provider in Cambridge, Mass., says senior management within his organization also has been highly focused over the last year on meeting HIPAA security regulations. Although he won't release specific financial figures, Berry says this focus helped the IT department get almost double the security budget it had before.

"HIPAA brought the visibility up to senior management, and we made five additional purchases for security purposes that probably wouldn't have been on the radar without it," Berry says. Network Health also conducted a HIPAA compliance check-up on itself using assessment tools from Askia and Mag Mutual's TurboCharge HIPAA Security.

Network Health also recently purchased WholeSecurity's host authentication, eEye Digital Security's Retina scanner and SurfControl's Web filter product to restrict access to the Web and lessen the chance of downloading viruses and spyware.

HIPAA is making it easier for Good Samaritan to get security funding, too, according to Chuck Christian, director of IS at the 1,000-employee hospital in Vincennes, Ind.

Good Samaritan girded for HIPAA security by getting together with other hospitals, state government regulators and attorneys under the umbrella of the Indiana HIPAA Task Force, which meets once a month.

To improve controls on access to applications, Good Samaritan decided to deploy Imprivata's single sign-on software and appliance, which cost about \$70,000. The hospital is also looking into the type of software that would monitor outbound e-mail and other communication to make sure confidential patient data isn't transmitted over the Internet without authorization. "This is all private and confidential information, and we need to keep it that way," Christian says.

**CHALLENGE**

Regulatory requirements such as SOX and HIPAA are placing tougher security and auditing demands on companies.

**RESPONSE**

Establishing a dialogue between IT and business leaders can further the deployment of needed security systems by defining them in terms of how they help achieve regulatory objectives rather than simply proposing them in complex technology terms.

**Regulatory requirements, mainly Sarbanes-Oxley, continue to squeeze IT budgets and staff**

■ *By Denise Dubie and Ann Bednarz*

The tab for regulatory compliance continues to climb - and along with it, demand for IT projects to bolster security, storage and reporting capabilities.

U.S. companies will spend \$15.5 billion on compliance-related activities this year, according to research published last week by AMR Research. A large chunk of the spending is designated for public companies' projects related to the Sarbanes-Oxley (SOX) Act of 2002. SOX spending will grow 11% from \$5.5 billion last year to \$6.1 billion this year, AMR says. Other budget-consuming initiatives include compliance with the Health Insurance Portability and Accountability Act (HIPAA), Food and Drug Administration regulations, and the Basel II international banking accord.

In particular, SOX has put a spotlight on compliance initiatives since it affects a broader swath of companies than some of the industry- or geographic-specific regulations, says John Hagerty, vice president of research at AMR Research. Additionally, it's getting budget priority over other regulatory projects because its deadlines are imminent. "Those with the shortest deadlines move to the top of the queue," he says.

Passed in the wake of accounting scandals at companies such as Enron and WorldCom, SOX is designed to deter fraud and add transparency to public companies' financial reporting procedures. Among the more onerous of the legislation's requirements is Section 404, which calls for companies and their auditors to formally attest to the existence and adequateness of internal controls over financial reporting systems.

Establishing, testing and documenting such controls is a time-consuming effort that not only has financial departments scrambling but involves nearly every aspect of IT.

The toughest part of SOX compliance is the scrutiny it places on the IT department, says James Olson, CIO at Waterbury Hospital in Connecticut. SOX has increased the number and comprehensiveness of IT-related audits, he says. "It used to be that a 100-watt bulb would be turned toward IS once a year. Now we have a searchlight looking at us."

Prior to the legislation, auditors examined the hospital's patient accounting system. Today, audits extend to multiple applications, including accounting, payroll, materials management and decision support systems.

Auditors today look not only at backup, data center security and password administration but also division of labor within the department, Olson says. "They have increased what they are auditing and [now look into]

Advice From the Experts

the formality of the policies, procedures and processes supporting the department," he says.

What makes SOX tough is that there's no one-size-fits-all checklist for compliance, adds James Kritcher, vice president of IT at White Electronic Designs. "From an IT perspective, the actions that a company will need to take depend on what is discovered in the internal controls inspection. IT leaders need to work closely with the Sarbanes-Oxley auditors to make sure that they know what their companies' weaknesses are."

When it comes to choosing technology to help with Section 404 compliance, purchases run the gamut from security and document management to collaboration and performance management products. There's no shortage of vendors offering SOX compliance assistance.

For example, OpenService this week is expected to release new versions of its flagship Security Threat Manager software, as well as Security Log Manager, an add-on monitoring application that alerts security managers to events that don't comply with pre-defined SOX policies.

Last week, SAP announced a deal with compliance specialist Virsa Systems to offer its Compliance Calibrator software to SAP users to help keep tabs on ERP system controls and avoid segregation-of-duties conflicts among end users.

**Getting help**

To automate manual processes, Waterbury Hospital has purchased configuration control software for patching its servers, password control software and other

technology, Olson says.

White Electronic Designs uses automated configuration management tools from Ecora and Tripwire to automate some of its SOX requirements, Kritcher says. The Phoenix company uses the tools to document baseline device configurations and detect unauthorized infrastructure changes, he says. "Without these types of tools, compliance would be much more difficult."

Even with the tools, the burden of SOX is palpable. "A great deal of IT time over the past year has been spent on Sarbanes-Oxley compliance activities," Kritcher says. "We had to defer a couple of planned, funded projects to divert staff resources to the compliance effort. The current year is looking much the same."

One of the aspects of SOX that has surprised companies is that it's an ongoing effort, Hagerty says. "People thought it would be a Y2K-like effort, but it's not. Companies have to deal with SOX requirements perpetually."

The ongoing nature of SOX compliance is disruptive and costly, Olson says. "The auditors will always find yet one more aspect that needs doing," he says.

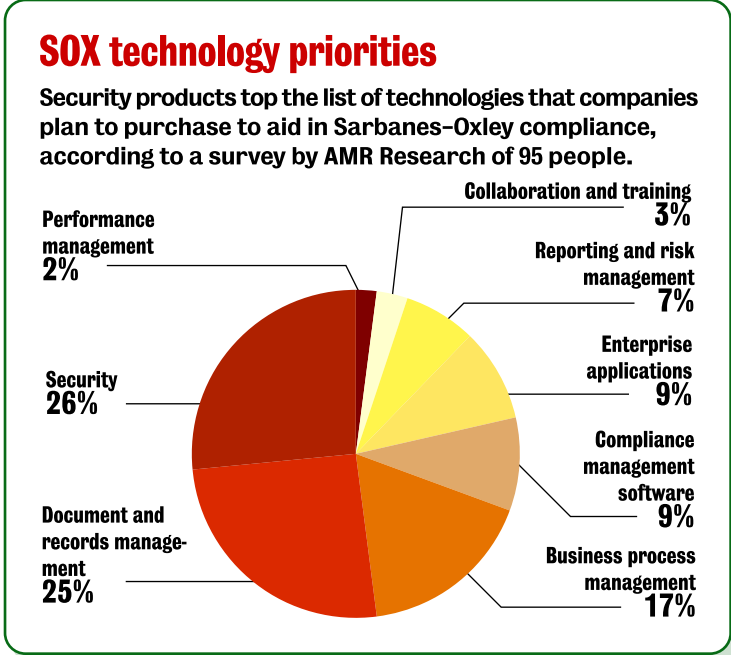
But there also are advantages for IT to SOX regulations, which can provide an impetus for companies to formalize their documentation and process controls. Many of the practices SOX has necessitated are good management practices, Olson says. "It is just we always gave them lower priority than our day-to-day stuff so implementation dragged," he says. "Now we have no alternative."

Mike Levinson, IT capacity planning and change manager at Hannaford Bros., a supermarket retailer in Portland, Maine, agrees. Levinson says SOX compliance helped him get management to approve the process-oriented approach he prefers to take. A former IBM systems administrator, Levinson always wanted to instill change management processes at the supermarket chain before SOX auditors hit the scene.

"Sarbanes-Oxley helped us get processes in place that probably should have been in place," he says.

Levinson says an audit of Hannaford's IT shop showed the company could improve its change management processes and its security controls such as defining separation of duties and establishing consistent policies across system platforms.

Levinson notes security policies on Windows, Unix, Linux and mainframe servers - all of which Hannaford has - differ and SOX will require the IT department to define consistent rules across the platforms. Also, SOX security policies, such as incident response,



## Advice From the Experts

need to be clearly stated to avoid any ad hoc firefighting when, say, a virus breaks out.

Levinson estimates that his IT team spends about 60% of its time fixing problems, which take priority over long-term IT projects. Now with SOX compliance on their list of things to do as well, he says he can't "accurately predict how many resources we will have for IT projects," which means they could potentially miss scheduled deadlines.

Because Hannaford is owned by the Belgium-based Delhaize Group, the company has another year to get compliant with Section 404. The Securities and Exchange Commission this month granted small and midsize public companies with a market capitalization less than \$75 million, as well as international companies, a one-year reprieve until July 15, 2006.

Large public companies with a market capitalization of at least \$75 million - with some exceptions - must begin including internal control reports required by Section 404 in annual reports filed for their first fiscal year ending on or after Nov. 15, 2004.

Looking ahead, AMR's Hagerty says companies will become more strategic about addressing SOX. Efforts this year will shift away from manual processes and toward

automating compliance, he says. "Fixes are heavily manual today, but that can't go on indefinitely or it would pose a real hindrance to business."

Kritcher says he sees an opportunity to shed some compliance costs and free up IT resources "by implementing systems and processes that simplify the compliance monitoring and audit process." As companies put compliance controls in place it makes sense to look for process re-engineering opportunities, he says.

Shifting SOX budgets from headcount-related costs to technology purchases reflect shifting mind-sets, Hagerty says.

Whereas companies spent about \$1.1 billion in 2004 on SOX-related technology, this year they will spend \$1.7 billion, he says. "People are spending more in '05 than '04 because they realize they have to automate a lot of the stuff they did by brute force last year."

Next up is finding ways to use technology to remediate any compliance shortcomings. By the end of 2005, companies will begin to deploy technology not only to automate processes and identify gaps, but also to help automatically close up any gaps that appear, Hagerty says.

# Hidden wrinkles in the compliance scenario

## How to SOC it to the Bad Guys

*A security operations center is becoming an enterprise must-have.*

■ By Joanne Cummings

Eamus Halpin's wake-up call was the Slammer worm. Until it hit, he had relied solely on port blocking to protect his enterprise network from hacks and intrusions. After he saw the network carnage Slammer wreaked around the globe, Halpin knew he had to revamp his company's approach to network security.

"I happened to be with Microsoft at the time at an NDA event in Seattle, and somebody scared me about what could happen to a port blocking-based network hit by Slammer," recalls Halpin, who is chief technical architect at iRevolution, a managed services provider in London. Although iRevolution's network was spared a direct hit by the worm, Halpin knew that had just been luck. "I spent three hours researching the implications of the worm, and my hair went white. We were as open as Swiss cheese," he says.

Although iRevolution had the basics in place - firewalls, anti-virus software, intrusion-detection systems (IDS) - it had no way to combine alerts from these various security tools to build a logical picture of the security health of the network.

"Everything was separately maintained and managed. They didn't speak to each other and didn't give us a business temperature for the enterprise as a whole," Halpin says. "So we could see occasionally that we were being attacked by a particular type of virus through e-mail, but we couldn't really determine how big an issue that was in the great scheme of things."

Halpin decided then and there to do a complete security overhaul. His goal was to build and maintain a world-class security operations center (SOC) for iRevolution's internal network, as well as to help support customers.

Just as network operations centers (NOC) continuously monitor networks to mitigate faults and ensure optimal performance, SOC's continuously monitor and manage a range of security devices and events to maintain and ensure overall network security. Experts say SOC's are becoming more common among companies for a variety of reasons, most notably because security has evolved from a discipline based on point solutions to something far more pervasive and critical to overall network health.

"It used to make sense to have security specialists



managing the various firewalls, IDS and so on because security was at a very specific location on your network and had a very specific function," explains Andreas Antonopoulos, senior vice president and founding partner at Nemertes Research. "But security no longer works that way. The perimeter is porous, and instead, security needs to be applied at the application level, at the network level and at the storage level. It's become a feature of your end-to-end application delivery, much like network performance."

Regulatory pressure brought on by the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act also drives enterprise SOC development.

"SOX is a good example of a proactive driver for SOC's," says Diana Kelley, executive security adviser at Computer Associates' eTrust division. "You've got to be ready for 404," she says, referring to the section of SOX that explains that executive management needs to take responsibility for establishing and maintaining an adequate internal control structure. "That means you need the correct and effective controls on your business reporting. And once you have them, you need to monitor and maintain them, and a SOC is an effective way to do that."

## Hidden wrinkles in the compliance scenario

According to preliminary research by Nemertes, the average U.S. organization plans this year to up its security budget 100%, from 2.4% of the IT budget to 4.8% - an increase Antonopoulos attributes almost entirely to regulatory compliance. "I can tell you that all those companies that are doubling their budget to do regulatory compliance are looking at either building a SOC or re-engineering a SOC to comply with the regulations," he says.

The trend to pull back security monitoring duties previously outsourced to managed security services providers (MSSP), especially in the financial services sector, adds fuel to the fire. An internal SOC allows better control and visibility into the enterprise network, and reduced costs overall, says Jim Tiller, chief security officer and vice president of security services at International Network Services, a network consulting firm.

"MSSPs are having difficulty responding in some cases," Tiller says. "With the regular occurrence of worms and denial-of-service attacks, especially in the financial industry, and the increase in our vulnerability and the sophistication of those threats, the ability to respond is strictly related to how much visibility you have in your network. By pulling the management in, you have more visibility and can facilitate the ability to respond."

Plus, "for large companies, the investment in managed security services is fairly significant and they're seeing long-term cost/benefit with regard to pulling

that in-house and managing it themselves," he says.

**The hurdles**

Although recognizing the need for a SOC is fairly easy, building one is not so straightforward. This is especially true when the security and network operations groups have grown up independently. Security monitoring might be robust, but if it is separate from network operations monitoring that can be a recipe for disaster, experts say.

"Security events don't always appear as security events," Antonopoulos says. For example, if a router stops responding and that's all the information you have, it's difficult to tell if it's a network problem, a systems problem or a security problem. If your network operations group is completely separate from your security operations group, one of two things will happen: "Either both groups will chase the problem separately, or worse, neither will chase it, concluding that it's the other group's problem," he says.

This confusion is exacerbated when it comes time for remediation. "If both organizations are implementing things on the network and monitoring it, you may come to the point where the network people are changing [access control lists], reducing your security, or your security people are applying ACLs that are impacting network performance," he says. "Since you're not integrating this and looking at it from an end-to-end perspective, you end up with problems."

A true SOC integrates security and network event

**Five SOC pitfalls to avoid**

**1. Technology tunnel vision.** Getting caught up in the latest and greatest tools is tempting, but the core of your security operations center (SOC) should be based on sound risk assessment and security policies. Once you've hammered those out, you can focus on the products and technologies that will best support them.

**2. Silo mentality.** Don't organize your SOC in a silo separate from your network operations. An efficient SOC depends on fully integrating security and network monitoring tools, as well as the staffing associated with them.

**3. Staffing mistakes.** Don't use your veteran security staff to do low-level monitoring, and make sure you have the proper checks and balances in place so that no one person holds all the keys to your network kingdom.

**4. Inflexible tools sets.** Choose tools that will support not only your current security devices, ticketing systems and network monitoring suites, but also those that are easy to customize and offer a variety of templates and wizards. Be aware that even the best tool sets require a good deal of customization and integration.

**5. Taking the cheap route.** A SOC is no place to skimp. On average, large organizations should plan to invest \$1 million or more to implement and maintain a truly enterprise-level SOC. And that investment will most likely grow over time.

— Joanne Cummings

## Hidden wrinkles in the compliance scenario

information so the security and operations staffs have an overall view of the event and the effect it's having on the network, and can make informed decisions about how best to react according to predefined security policies. But that's easier said than done.

**Where to start**

Many organizations first look to purchase a security event management system or alert correlation engine. But experts say that's a tactical mistake. An overall risk assessment, for determining the actual business importance of each network asset, must come first in the SOC project.

"You have to apply your resources to protect the things that are most important to you," says John Summers, global director of managed security services at Unisys. "Some IT execs have a very good handle on their infrastructures. They know what assets are out there and what's running at each IP address, but very few can tag a business priority to their infrastructure elements."

Knowing the business importance is key because the purpose of a SOC is to enable not only security event monitoring but also confident responses to those events. "So if this server went down, what would it mean to the business, and is this server more important than this other one? Once you know that, the technology part tends to fall into place," says Summers, who manages Unisys' three major SOC's.

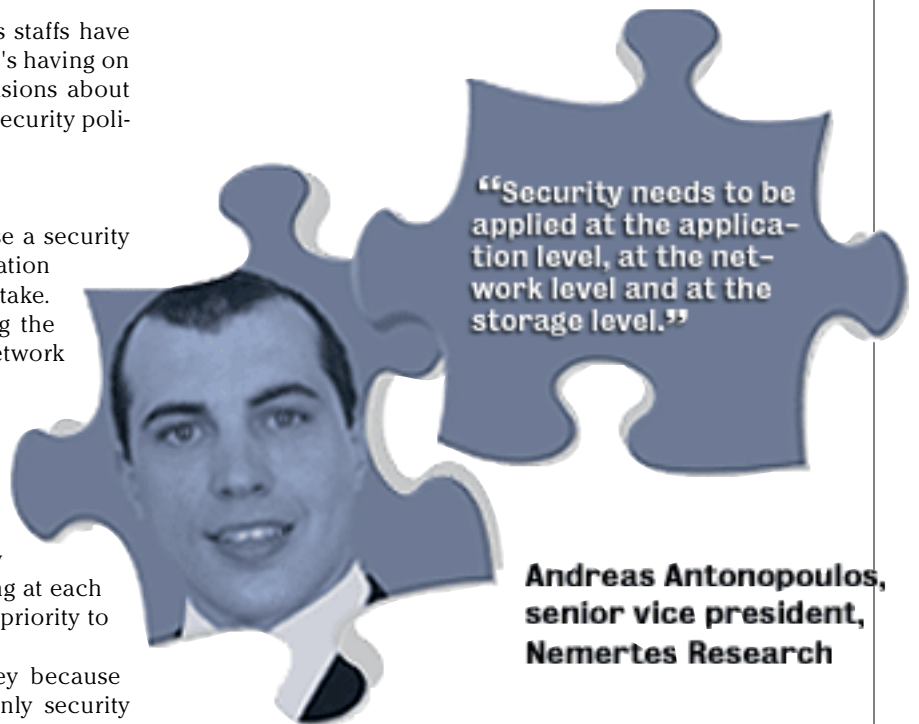
**Technology caveats**

Choosing a technology platform comes next. The goal is to find a security event management platform that can work with the variety of security devices you have in place, correlate their various alerts, and provide some form of integration with whatever you are using for trouble ticketing and network operations management. Organizations need this depth of visibility into the network to ferret out security breaches, experts say.

"A big financial services company we work with was seeing some poking at different areas of its network around the globe," CA's Kelley says. "Each of the pokes didn't look particularly bad individually, but they were all coming from the same IP address over a period of a couple of days. None of it was enough to trigger an alert on its own, but once the company pulled that information into a centralized console [within its SOC] and saw what this one IP address was doing to its network around the globe, things started to add up."

However, getting to the point where you can have such a global view within your SOC is time-consuming and expensive.

In addition to integrated security event managers from start-ups such as ArcSight, Intellitactics and



**Andreas Antonopoulos,**  
senior vice president,  
Nemertes Research

netForensics, most of the large network management companies - CA, HP and IBM - offer a security event monitoring capability integrated within their platforms. But they all come at a pretty hefty cost.

"In the security space, IDSs generally don't speak the same language to your management system that your firewall does," Nemertes' Antonopoulos says. "If you want to add a rule into your firewall to block something, you can't use the same language you would use to add a rule in a router. As a result, security event monitors require a large integration project to pull all that information, turn it into a common format and correlate it across all those domains."

The vendors pass on the cost of that large integration project to their customers. The hardware and software for these packages alone costs on average \$1.5 million to \$3 million, Antonopoulos says. "Add to that three shifts of people and the integration into a ticketing system, and it gets very expensive," he says.

IRevolution's Halpin says his SOC project, which is based on CA's Unicenter for network management integrated with CA's eTrust for security monitoring and event correlation, costs approximately \$1 million and took 18 months to implement. The SOC has been up and running for about six months, and Halpin says he's just now feeling like he's getting worthwhile and actionable information from it.

He negotiated a "fair" contract with CA, "but the majority of my costs are in people time," he says. That's because picking the tool is one thing but getting it tuned to

## Hidden wrinkles in the compliance scenario

your particular environment takes time and troubleshooting.

"Anybody who's up for this and wants to see a pretty center with blinking lights can get that in 10 minutes," Halpin says. "But building a real SOC takes time. And however long you think it will take, triple that, and then be prepared to maintain it. This isn't easy and it's never-ending."

He says one key to easing the process is to make sure the tool you choose is flexible. That means making sure that not only will it support the various firewalls, IDSs and network management platforms you have in place, but also is easy to customize and tune.

"It has to be easy to write rules," he says. "If you can write those rules quickly, and you have templates and good wizards for it, then that's going to make the whole process much easier."

But perhaps the biggest caveat for building a SOC is to realize that your initial million-dollar investment is just the beginning. Because technology is changing all the time, so will your security needs and strategies.

"Although I feel like our security and our SOC are very scalable now, I'm expecting that within three or four years' time, we'll have to throw the whole thing out and do something different because security will have moved on," Halpin says. "With the amount of processing power that is about to become available through dual-core and all of the other technologies, you can't stand still. Those things will have a significant effect on the technology and security marketplace, and we know here that security will always be an ongoing expenditure."

*Cummings is a freelance writer in North Andover, Mass. She can be reached at [jocummings@comcast.net](mailto:jocummings@comcast.net).*

## How to staff a SOC

**S**taffing a security operations center can be almost as challenging as building it or paying for it, users and experts say.

The 24/7 monitoring necessary in a SOC presents one of the biggest hurdles. "For companies used to having security personnel working eight hours a day, five days a week, that dramatically increases their overall staffing requirements, since one 24-by-7 seat is equal to roughly five full-time employees," says John Summers, global director of managed security services at Unisys. Faced with such a prospect, many organizations look to cut corners.

For example, some make the mistake of staffing their SOC solely with their best security personnel. "Companies take seasoned security professionals, stick them in front of a screen and ask them to do a six-hour monitoring shift," says Andreas Antonopoulos, senior vice president and founding partner at Nemertes Research. "You won't retain those people too long because they will very quickly become bored." Beyond boring and overworking a valued staffer, this tactic also could create a huge security vulnerability.

"If one person is writing your security policy, implementing your policy, monitoring it and then checking for compliance, that person is basically one huge risk," Antonopoulos says. "There's no separation of duties, and absolutely no checks and balances."

Instead, a good SOC, like a good, traditional network operations center, should be staffed in tiers, with Tier 1 personnel receiving alerts and doing low-level troubleshooting and Tier 2 and 3 people handling more complex alerts and problems. In the best of all worlds, Tier 1 personnel should provide the first line of response for both the security and network operations sides of the house. That way, your more veteran security professionals can handle the more complex risk-management and policy-writing tasks, while putting lower-level staffers into the SOC for the primary monitoring. Then, when alerts come up and the Tier 1 staffers are unsure how to proceed, they can kick up the problem to a Tier 2- or 3-level person. Only then does your more expert, and expensive, staff get involved.

— Joanne Cummings

## Hidden wrinkles in the compliance scenario

**Offsite security complicates compliance**■ *By Ann Bednarz*

Offsite security conditions are always a factor to consider when a company enters an outsourcing deal, but regulatory initiatives are raising the stakes.

IT executives need to ensure service providers have proper system controls in place before and after they enter into sourcing and hosting arrangements, analysts say. It's not only a good business practice, it's also increasingly required by law.

**IT executives need to ensure service providers have proper system controls in place before and after they enter into sourcing and hosting arrangements, analysts say. It's not only a good business practice, it's also increasingly required by law.**

One law putting a spotlight on outsourcing deals is the Sarbanes-Oxley (SOX) Act of 2002, which Congress passed in the wake of accounting scandals at firms such as Enron and WorldCom.

SOX has IT and finance departments working closely to review and modernize companies' financial reporting systems to comply with its regulations. Of particular concern is Section 404 of the legislation, which calls for company executives and third-party auditors to certify the effectiveness of internal controls - technologies and processes put in place to preserve the integrity of financial reports.

Doing due diligence to Section 404 means looking into conditions at outsourcing and hosting providers' sites, where sensitive corporate data might be accessible, processed or stored. That's where Statement on Auditing Standards (SAS) 70 comes in.

SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants for service organizations. It prescribes a method for an auditor to examine control activities at a service organization or outsourcing firm.

There are two types of SAS 70 audits. A Type 1 audit focuses on general controls at a single point in time and doesn't include testing by auditors. A Type 2 audit is more intensive - and more appropriate for SOX compliance. It looks at conditions over a prolonged period of time, and auditors perform testing to verify the effectiveness of controls at service organizations.

SOX compliance efforts have elevated interest in the auditing standard, which has been around since 1992. "We are doing a lot more SAS 70s lately," says Ed Byers, a principal at Deloitte & Touche.

Outsourcers agree that users are beginning to ask for SAS 70 audits. "It was something our customers were looking for," says John Engates, CTO at Rackspace Managed Hosting.

Ernst & Young recently concluded an SAS 70 Type 2 audit for the San Antonio managed hosting provider. The audit covered controls related to service delivery and operations, infrastructure maintenance, change management, back-up processes, and logical and physical data center access, Engates says.

Rackspace underwent the audit at the request of some of its largest customers, which are facing SOX Section 404 deadlines, Engates says. Section 404 says companies must prepare reports - to accompany their annual reports filed with the Securities and Exchange Commission - assessing the effectiveness of their internal control structures and financial reporting procedures. Section 404 deadlines are staggered and begin this spring.

"They really need some assurance that the controls that are in place outside of the walls of their companies are as effective as the controls inside their companies," he says.

At the same time, Rackspace benefits from having gone through a formal process to analyze and document its internal controls. "It put a spotlight on our documentation and the formalization of our policies and processes," Engates says.

Securing SAS 70 certification requires a commitment - of personnel and budgets - on the outsourcing providers' part. At Rackspace, the certification process took almost one year, from the early stages of defining the scope of the audit to the full-blown testing of controls.

Sierra Atlantic will spend about \$25,000 to achieve SAS 70 certification this year, says Marc Hebert, executive vice president at the Fremont, Calif., company, which offers a range of offshore application services. Sierra Atlantic is in the process of securing SAS 70 Type 2 certification.

Like Rackspace, Sierra Atlantic decided to pursue SAS 70 certification because of customer demand, Hebert says.

In general, there's a tendency for companies to secure more SAS 70 certifications from outsourcers than are needed, Byers says. "Companies are so scared about Sarbanes-Oxley they want to audit everything," he says.

There's confusion over when an SAS 70 audit is required and when it isn't - particularly when it comes to

## Hidden wrinkles in the compliance scenario

smaller service providers that might not have the necessary controls in place, Byers says.

The most common scenario that would require a company to secure an SAS 70 audit from its service provider is when the company outsources application processing such as payroll. "If you outsource a transaction process like payroll, then you probably want an SAS 70 - because the control is at the service provider," Byers says.

But not every outsourcing arrangement necessitates an SAS 70. For example, a company that uses contract employees from an IT service provider to help manage its applications probably doesn't need an SAS 70 from the service provider because control over the systems remains internal.

Likewise, if a company uses an outsourcer for certain application development activities but retains control over application testing and change control, an SAS 70 might not be required. "If management is providing all the control, you don't need to have an audit of the service provider," Byers says.

Some arrangements are particularly cloudy about SAS 70 requirements. In a hosting arrangement, it's important to determine who has control over updates to an application, Byers says. Additionally, even if a company retains control over application testing and updates, an SAS 70 audit might be required to assess physical and environmental controls at the service provider's site, Byers says.

Even if an SAS 70 audit has been completed, it might not be adequate for SOX compliance, Meta Group says. The SAS 70 standard was developed long before SOX regulations and doesn't necessarily focus on the type of controls that SOX requires, according to the research firm.

There's no standard prescription for what is covered in an SAS 70 audit, Byers agrees. A service provider typically defines the control objectives and activities covered in an SAS 70 audit of its operations. "An SAS 70 can include as much or as little as a service provider wants. It's not a standardized audit report," Byers says.

**There's no standard prescription for what is covered in an SAS 70 audit, Byers agrees. A service provider typically defines the control objectives and activities covered in an SAS 70 audit of its operations. "An SAS 70 can include as much or as little as a service provider wants. It's not a standardized audit report," Byers says.**

Because the comprehensiveness of SAS 70 audits varies, it's up to the contracting company and its auditors to assess a service provider's SAS 70 for completeness and adequacy.

"Since the SAS 70 isn't standardized, you need to assess its completeness," Byers says. "Does it cover all your general computer controls? Does it cover applicable business process controls via the application controls?" In theory, a service provider could exclude areas from an SAS 70 audit where it knows it's vulnerable. But that's not typical, Byers says. In general, SAS 70 audits have become more comprehensive in light of SOX, he says.