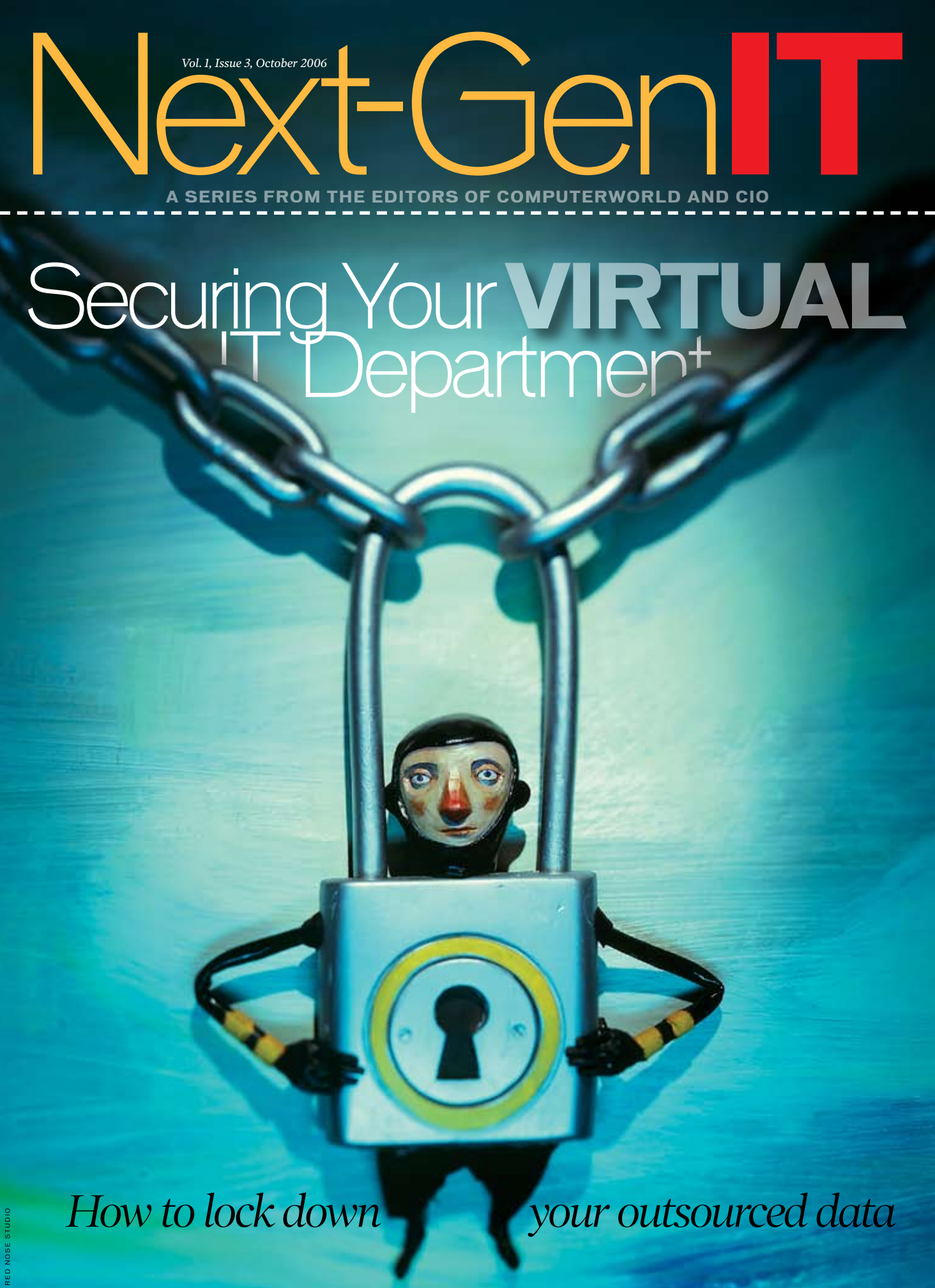
Vol. 1, Issue 3, October 2006

Next-Gen IT

A SERIES FROM THE EDITORS OF COMPUTERWORLD AND CIO

Securing Your VIRTUAL IT Department



How to lock down your outsourced data

RED NOSE STUDIO

EDITORS' NOTE

WEBB CHAPPELL

CIO Editor in Chief **Abbie Lundberg** and *Computerworld* Editor in Chief **Don Tennant**

Virtually Certain

THE CONUNDRUM is as old as the data center itself. Maximizing business efficiency may well require you to offload some portion of your IT operation to a third party, yet how can you be certain the third party will maintain the security of the data that's the lifeblood of your business?

It's a challenge that CIOs will increasingly confront, because the economic conditions that have created it are hardly abating. Forrester Research predicts that spending in the U.S. for IT outsourcing will grow from $68 billion in 2006 to $72 billion in 2007. And while its forecast is more modest, IDC projects that worldwide spending on IT outsourcing services will grow at an annual rate of nearly 5% to reach $112 billion by 2010.

Protecting that investment means protecting the corporate data that's entrusted to the outsourcer.

In this issue of Next-Gen IT, a series produced jointly by the editorial teams of *CIO* and *Computerworld*, we examine the issues involved in ensuring that your outsourced data is properly locked down. The examination is a crucial one: More than 90% of respondents to an International Association of Outsourcing Professionals survey said security breaches related to outsourcing would be "catastrophic" to their businesses.

If catastrophe strikes, moreover, the blame will rest not with the outsourcer, but with your company. And even if catastrophe is avoided, auditors and regulators will hold your company responsible if your outsourcer fails to comply with regulatory standards.

Fortunately, there's a lot you can do to minimize the chances of finding yourself in that unfortunate circumstance — and to minimize the fallout if you do. That's what this issue is all about. As Galen Gruman reports in "Security Can Never Leave" (page 3), M&T Bank, for example, gave its outsourcer an incentive to avoid problems by making it liable for the cost of notifying affected customers of data breaches. And in Robert L. Scheier's piece titled "Virtual Security: The Devil Is in the Details" (page 11), you'll read about how companies are taking tacks such as using dashboards to dynamically monitor their outsourcer's security performance.

We invite you to take full advantage of the information and pointers in this issue — and on our Web site (*ITNextGeneration.com*) — so you can be certain that your virtual IT department is as secure as the one you're sitting in. ◆

INSIDE

NEXT-GEN ONLINE

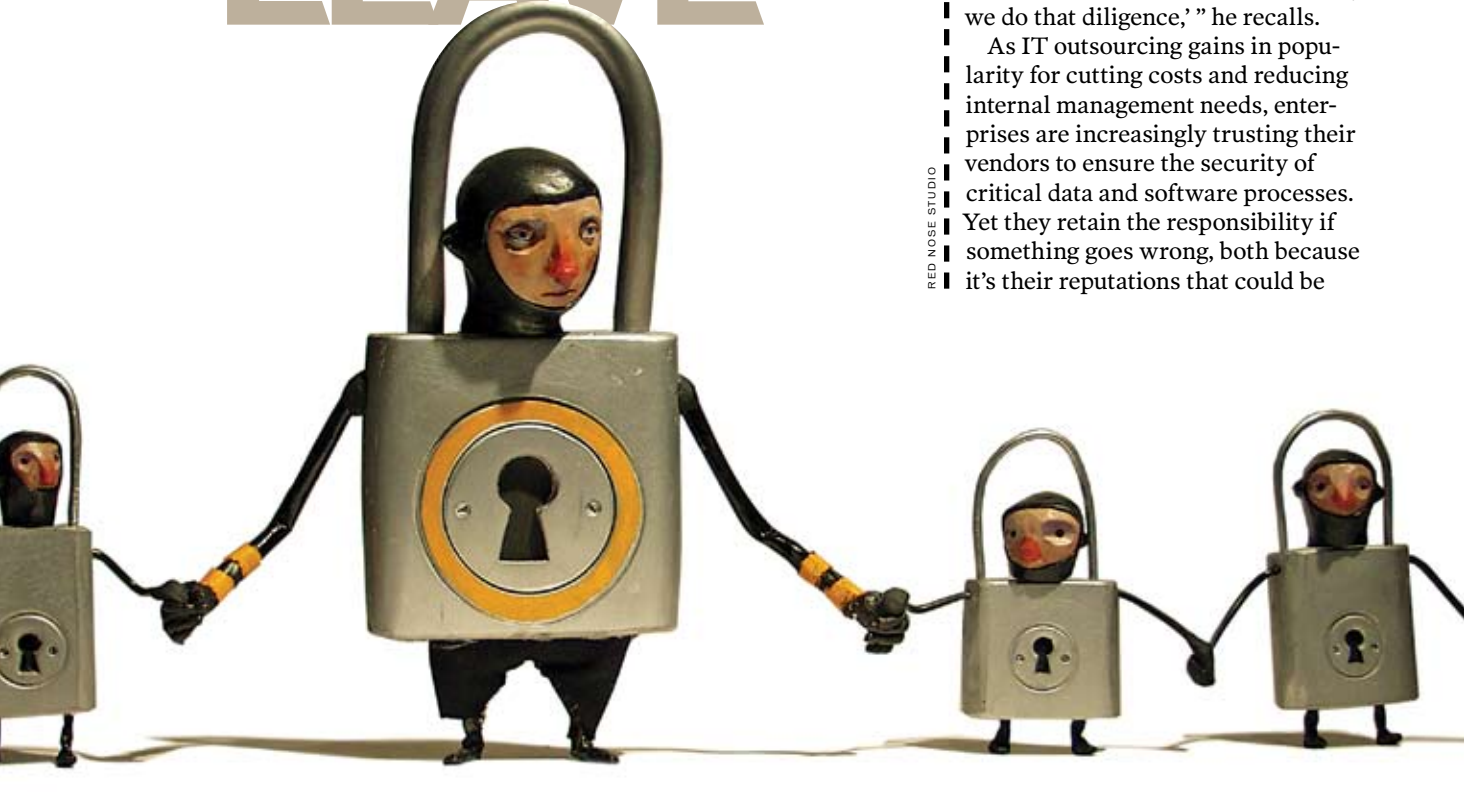
For the online edition of this publication plus relevant, related content from *CIO* and *Computerworld*, visit our Web site: **ITNextGeneration.com**

CIO COMPUTERWORLD THE VOICE OF IT MANAGEMENT

Computerworld editor in chief **Don Tennant** ■ CIO editor in chief **Abbie Lundberg** ■ Computerworld special projects editor **Ellen Fanning** ■ CIO executive editor **Christopher Koch** ■ Art director **April O'Connor** ■ Illustrator **Red Nose Studio** ■ Managing editor/production **Eugene Demaître** ■ Copy editor **Monica Sambataro** ■ Site architect **William Hall**

You can outsource your work to others, but the responsibility for security — and accountability for any problems that occur — will always be yours alone.

Security CAN Never LEAVE



RED NOSE STUDIO

BY GALEN GRUMAN

MATT SPEARE had to do something that's difficult for IT leaders (and their career prospects): He had to nix a deal that the business liked — a lot. The business people at Speare's company, M&T Bank Corp., wanted to sign on with an outsourcer to handle some of its data management. However, Speare, who is M&T's corporate information security officer, didn't like what he saw in his team's audit of the outsourcer's security procedures.

"It pointed out management issues in their control environment which they could not remediate," he says.

Despite some internal grumbling, M&T selected a different vendor. Speare says, "We had a lot of hand-wringing over this, as well as project delays." A few months later, the bypassed vendor, which Speare refuses to name, made headlines for allowing credit data for millions of people to be stolen. "As soon as the headlines hit, we told the business, 'This is why we do that diligence,' " he recalls.

As IT outsourcing gains in popularity for cutting costs and reducing internal management needs, enterprises are increasingly trusting their vendors to ensure the security of critical data and software processes. Yet they retain the responsibility if something goes wrong, both because it's their reputations that could be

A Second Pair Of Security Eyes

Not quite sure you can trust your outsourcer's security? Then don't. Instead, hire a managed security service provider (MSSP) to manage security for the outsourcer.

That's the strategy many Fortune 500 companies take, says Doug Howard, chief operating officer at Counterpane Internet Security Inc., an MSSP in Mountain View, Calif. Many traditional IT outsourcers, such as IBM, are better at ensuring system availability and uptime than at ensuring security, he says. Besides, hiring an MSSP along with the outsourcer means the two vendors are keeping an eye on each other's performance. While this setup results in two vendor relationships to manage, he says, it generally costs no more than securing the outsourcer yourself.

Such specialized help could be a nice addition to the IT skills of your core outsourcer – if you're willing to manage two outsourcers rather than one.

– ROBERT L. SCHEIER

ILLUSTRATIONS BY RED NOSE STUDIO

damaged and because regulators hold them accountable for the actions of their providers. "Outsourcing doesn't mean that the internal organization isn't responsible anymore," says Eric Litt, chief information security officer at General Motors Corp. "You still have the responsibility and the accountability to the business, so you have to define the policies."

Indeed, a company's security burden actually increases when it's considering outsourcing, because it's no longer just about being able to protect your own assets; it's about knowing whether the outsourcer knows how to protect itself, too.

"Outsourcing actually requires an even higher-performing [management] staff than if it's in-sourced," says Litt. "You need to know at least as much as the outsourcer does."

CIOs are ultimately responsible for making sure that their companies are protected, regardless of where the work resides. They need a strategy for building security competence in-house and monitoring it with their outsourcers. "You can't outsource your problems to fix them. You can't expect the service provider to do that," says Mark Lobel, a partner at accounting firm PricewaterhouseCoopers.

Ensuring the security of your outsourced IT operations doesn't start or stop with due diligence.

> **"You can't outsource your problems to fix them.** You can't expect the service provider to do that."
>
> **MARK LOBEL,** PARTNER, PRICEWATERHOUSECOOPERS

Instead, it requires the following multistep process:

1. Assess your risks and define your security needs.
2. Validate vendor ability through due diligence.
3. Spell out the requirements contractually.
4. Monitor performance after you've chosen the outsourcer.

Validating Potential Vendors

For most companies that outsource IT, validating vendors' processes and capabilities is the most important step to ensuring security. There are multiple elements in this strategy.

Continued on page 6

Continued from page 4

Southwest Airlines Co. starts with a detailed request for proposals (RFP) for all aspects of the outsourcing relationship, including security. "Asking a lot of questions upfront sets the expectations, so that tends to weed out those vendors who can't deliver," says Robert Schaffer, senior director of technology at the airline.

Likewise, when GM seeks outsourcing vendors, it first defines a statement of work that includes service-level agreements and metrics, Litt says.

"Savvy customers are asking questions earlier," notes Dave Bixler, chief information security officer at Siemens Business Systems, which provides outsourcing services.

In addition to details on processes and policies, CIOs should ask for details on staff turnover and credentials, which are indicators of how well the outsourcer can satisfy its promises, says Scott Crawford, an analyst at Enterprise Management Associates. "You don't want them to have mail-order diplomas," he says.


Scott Crawford

"You're not going to have all the questions and answers upfront," cautions Pawan Verma, managing director of the outsourcing advisory practice at PricewaterhouseCoopers. "What you need to achieve is a confidence that they can deal with issues. Look for a comfort level that you can work with the folks across the table."

Bixler says most customers deal with security by having a face-to-face meeting with him to assess whether he knows what he's doing. But Bixler cautions against relying too much on that personal evaluation. "What if I leave?" he asks. He encourages customers to do their homework first.


MICHELLE ANDONIAN

> "Outsourcing actually requires an even **higher-performing** [management] staff than if it's in-sourced."
>
> **ERIC LITT,** CHIEF INFORMATION SECURITY OFFICER, GENERAL MOTORS CORP.

Go Beyond the Usual Suspects

Evaluating RFP responses is just the first step in the vetting process. Corporate IT should also talk to vendors' customers and conduct Web and other searches to see if there have been publicized security failures, financial concerns or other indicators that a vendor might not be able to deliver.

"Google is your friend," says Andrew Jaquith, an analyst at Yankee Group Research Inc. It's particularly useful to ask reference customers why they did not choose another vendor; this helps build up pros and cons across the vendors you're considering, rather than just see the successes, he adds.

Also ask to see copies of third-party certifications, third-party audits and internal audits, recommends Jaquith. Even if you don't get everything you seek, you'll get a better sense of the vendor's responsiveness and openness, both of which are crucial to a successful relationship. "You're looking at the preponderance of evidence," he adds.

But be sure to know what audits the vendor has or should have by talking to other customers and auditors, advises Litt. "Otherwise, they'll just say it's not available," he says.

When you do get them, don't take all certificates and audits at face value. The Statement on Auditing Standards (SAS) 70 self-audit, for example, measures whether a vendor delivers on the processes it identifies — but it doesn't evaluate whether those are the right processes, notes PricewaterhouseCoopers' Lobel. Also watch out for "qualified" SAS 70 audits, which mean that the internal controls for the identified processes are not being applied consistently, calling into question actual performance, he says.

Take a Look at Yourself

That's why, at least for particularly critical IT functions, organizations should consider conducting their own audits, suggests Southwest's Schaffer.

Even smaller companies can do this, says Steve Withers, IT director at EaglePicher Technologies LLC, a manufacturer in Joplin, Mo. Withers says he visits his outsourced data center regularly "to see how seriously they take security in between audits."

Most industries have no mature auditing or certification standards that enterprises can rely on to assess potential vendors. "The standards are not as complete as they need to be," observes Litt, although there is some draft work under way. The financial industry is furthest ahead: The banking industry has the Payment Card Information data security standard and the Financial Institution Shared Assessments Program.


Andrew Jaquith

For Web-based applications, the Web Application Security Consortium has defined security standards. More broadly, the ISO 270001 standard for auditing security management is also emerging as a system for sharable audits, especially in India, explains Jaquith. And the American Institute of Certified Public Accountants Privacy Task Force has recently developed its Generally Accepted Privacy Principles to enable third-party audits whose conclusions cover the needs of many industries.

> "Even if vendors provide the **appropriate audits**, the legal controls [overseas] to enforce them don't exist, so you have **less leverage**. And it's harder to get **restitution**."
>
> **STEVE GORDON,** PROFESSOR OF IT MANAGEMENT, BABSON COLLEGE

Going Global Increases Risks


Steve Gordon

If you're outsourcing to other countries, there are additional concerns, says Steve Gordon, a professor of IT management at Babson College. "Even if vendors provide the appropriate audits, the legal controls to enforce them don't exist, so you have less leverage. And it's harder to get restitution," he notes.

Wanting to gain outsourcing business, some nations are emulating U.S. laws so the legal frameworks match. Generally, European countries are as strict as or stricter than the U.S., and Canada is fairly equivalent.

Prodded by India's National Association of Software and Service Companies, that country's government has begun aligning its laws to U.S. standards, says Rena Mears, privacy and data protection service director at accounting firm Deloitte & Touche USA LLP.

Japan has developed stricter requirements, mainly in response to demands from Japanese companies rather than to satisfy outsourcers that serve the U.S., she notes.

China is assessing its legal system, but for now, "there's little control over data protection and licensing," says PricewaterhouseCoopers' Verma.

Aligning the outsourcers' corporate presence with the countries where you need legal protection can also help. M&T Bank solves the dilemma by requiring any outsourcers it uses to have incorporated entities in the U.S. so they're subject to U.S. laws.

Similarly, companies often look to European outsourcers to handle European customers' data. The data protection laws there are stricter than in the U.S., and European outsourcers are generally better versed in the requirements, says Don DePalma, president of IT consultancy Common Sense Advisory Inc.

Get It in Writing

Once a CIO is satisfied with an outsourcer's ability to secure its data and applications, the next step is to codify the expectations, monitoring mechanisms and liability in case of failure.

Some CIOs say that rather than rely on the outsourcer's experience with other customers or a boilerplate contract, companies should develop codification from scratch.

"We think it is a horrible mistake to take the vendor's contract and modify it," says Speare. "You should have your own language." Of course, vendors would prefer not to have separate contracts with each customer.

Wherever a contract's language originates, CIOs should view them as dynamic documents, updating them as needs change. For example, M&T Bank changed the liability provisions in its outsourcing contracts last year after regulations arose that mandated the disclosure of privacy breaches to affected customers. As an incentive to avoid problems, M&T made the outsourcer liable for the cost of notifying affected customers of data breaches — $137 per customer, says Speare.

Keep Monitoring


Dave Bixler

It's nearly impossible to technologically monitor how outsourcers keep data secure on their own premises. Monitoring tools vary widely, and monitoring could unintentionally expose data from the outsourcer's other customers. That's why consultants and analysts recommend that businesses insist on a right-to-audit clause in their contracts, so they can do their own checking of the outsourcer's processes to ensure that the service levels are maintained.

But customers rarely follow through, says Bixler. The reason: "It's very resource-intensive, and most companies

Continued on page 10

Can You Trust SaaS Providers?

An emerging form of outsourcing is software as a service (SaaS), in which a vendor has a common application used by multiple customers. Unlike traditional outsourcing, there is no customization for each client, so the security policies are generally not negotiable beyond lower-level functions such as encryption standards or use of virtual private network connections.

"SaaS providers should make their security and privacy policies clear upfront," advises Steve Gordon, professor of IT management at Babson College.

SaaS providers can go a long way to gaining CIOs' trust if they get reputable independent audits that they share with customers, says Andrew Jaquith, an analyst at Yankee Group. "It doesn't need to be done for every customer," he says.

General Motors eyes SaaS providers cautiously, given its inability to impose its desired level of control on them. "If their contracts don't meet our security needs, we'll end discussions," says Eric Litt, the automaker's chief information security officer.

"We wouldn't use SaaS," says Matt Speare, corporate information security officer at M&T Bank. Speare is concerned about data management. "They intermix data, which contradicts financial services rules that require data segregation to ensure that data is truly destroyed" when it is no longer needed, he says. Both Litt and Speare say SaaS is better suited to smaller companies that have less risk or ability to manage risk.

Even if a company bars SaaS because of security concerns, such arrangements could still be a problem, Gordon notes, because departments may use a SaaS provider without IT's knowledge. IT has some recourse, including blacklisting unapproved SaaS providers' Web addresses from the network and using content filtering to detect leakage of corporate data to a Web site (which may indicate transfer to a SaaS system). But neither solution is perfect, so stubborn users may still use SaaS behind your back.

– GALEN GRUMAN

Continued from page 7

that hire outsourcers no longer have the resources to do the audit," he says.

Even if audits are rarely performed, requiring them is still a good idea. At Southwest, "it's rare to audit outsourcers, but it has been done," says Schaffer. "It's done based on risk, such as when something doesn't feel right." Southwest also gets a feel for outsourcers' performance by using information in audits for other purposes, such as Sarbanes-Oxley Act compliance, since these audits typically examine both Southwest and its outsourcers.

Another useful tool for low- or medium-risk data is to settle for a review of the outsourcer's support documentation, says Speare, because that will show whether the outsourcer is keeping its policies current and maintaining its operational rigor.

How to End The Relationship

An often-overlooked issue in securing an outsourcing relationship is how to handle its dissolution. For example, Withers is working with other customers of EaglePicher's manufacturing information systems outsourcer, Plexus Systems LLC, to create a trust arrangement for EaglePicher's data in case the young outsourcer goes out of business. And when you leave, "how can you ensure that all your data is wiped clean?" asks DePalma.

For him, the question is not academic: DePalma was shocked to discover that six months after Common Sense ended its relationship with Salesforce.com Inc., the company's data was still on the CRM provider's servers, even though Salesforce.com had promised to delete the data after a month. Common Sense learned of the retained data only when it began discussing a new relationship with Salesforce.com. (Salesforce.com declined to discuss its data management policies.)

> **"You don't have infinite resources, so you can't solve everything.** It comes down to what is the most critical thing to protect and how do you go about it."
>
> **RENA MEARS,** PRIVACY AND DATA PROTECTION SERVICE DIRECTOR, DELOITTE & TOUCHE USA LLP

It's All About Risk Assessment

Rena Mears

There's no way to absolutely ensure that your chosen vendor will secure your data and applications, regardless of the due diligence, contractual requirements and monitoring you apply. "You don't have infinite resources, so you can't solve everything," says Deloitte's Mears. "It comes down to what is the most critical thing to protect and how do you go about it."

"People are clearly thinking about security plenty," says Yankee Group's Jaquith. "But thinking and doing are two different things. You need to know what you're getting into."

Responsibility for security never leaves the CIO's desk, even when the work does. Without serious due diligence and a robust set of policies for handling security with IT providers, outsourcing can become a game of Russian roulette. ◆

Gruman, principal of The Zango Group and a regular contributor to CIO, *can be reached at ggruman@zangogroup.com.*

RED NOSE STUDIO

Virtual SECURITY: The Devil Is in the Details

From the initial contract to ongoing monitoring, it pays to get specific with your outsourcer about the security needs of your company.

BY ROBERT L. SCHEIER

HOPING TO save money and respond more nimbly to changing business conditions, companies are increasingly going "virtual" with their data centers, outsourcing the management of key applications and data.

But with new regulations and laws raising the penalties for security breaches, customers are becoming more and more concerned about whether their outsourcers can keep their systems and data safe.

In a survey conducted earlier this year by the International Association of Outsourcing Professionals, more than 90% of respondents said security breaches related to outsourcing would be "catastrophic" to their businesses, and 45% said they were more or much more concerned about data security than they were a year ago.

Watson Wyatt Worldwide Inc. in Arlington, Va., administers outsourced employee-benefit plans for its customers and outsources some of its

own IT functions to outside vendors. Five years ago, customers would leave it up to Watson Wyatt to perform vulnerability assessments of the Web applications that it manages for them, says Ryan Hunter, service delivery manager. Now, he says, there's a "huge uptick" in clients demanding to perform their own vulnerability scans to meet regulatory requirements.

Despite such worries, there's no stopping the headlong move to outsourcing. For the many companies that will hand over all or a piece of their IT systems this year to third parties, tricky tactical issues involving security come to the fore. And according to IT executives who have been there, it's all about keeping an eye on the details. Here's how to ensure that your outsourcer keeps your systems, applications and data in secure lockdown, and some information about the technologies that can help.

Get Specific With What You Need

Almost every organization has different security needs, based on the industry it is in, the type of systems it runs, the type of data it controls and the laws, regulations or industry standards it must follow. That's why effective management of an outsourcer's security must begin with an internal data assessment (see story, page 3). The customer can then use those internal requirements to build the processes and requirements their outsourcers must fulfill.

Some customers use off-the-shelf software to help assess the criticality of the IT services they have outsourced and what security measures they should demand of their outsourcers.

For example, Credit First National Association in Cleveland provides credit card services for Bridgestone/Firestone North American Tire LLC and relies on the parent company's internal IT department for services. To ensure that the IT group is complying with financial regulations, the credit card unit uses ControlPath Vendor Management software from ControlPath Inc. in Englewood, Colo., to identify the security requirements that its IT partner must meet.

As a result of this assessment, outsourcers "might have to answer how they handle the security of their employees, the security of their information systems or their contingency planning," says Peter Racco, manager of information and physical security and enterprise risk management at Credit First National. If a contract needs to be checked, for example, ControlPath fires off an e-mail to a lawyer advising him to be sure the contract is current. To do such work manually, Racco says, "I

SARA JORDE

> Despite the **number of tools and services** used to track security, it's still a major challenge to get **a single view** of all the vulnerabilities within all systems.
>
> **RYAN HUNTER,** SERVICE DELIVERY MANAGER, WATSON WYATT WORLDWIDE

would have had to hire five or six full-time employees."

It's also important to be very specific about your security needs, especially with an outsourcer that is more focused on meeting performance or efficiency goals than on security. In many cases, customers are hiring managed security service providers (see "A Second Pair of Eyes," page 4).

Sometimes a customer needs to drill down into details such as how an outsourcer staffs its data centers during vacations or other employee shortages. David Melnick, a senior manager at accounting and consulting firm Deloitte & Touche USA LLP, remembers one outsourcer that gave more than 100 employees administrative privileges on a customer's systems so they could fill in for other network, database or systems administrators who were out sick or on vacation. The customer considered this practice unacceptable and persuaded the outsourcer to instead give only limited-time access to such employees, reducing the number of people with unlimited rights to its sensitive systems.

Melnick also suggests detailing in contracts or service-level agreements (SLA) exactly what tests a customer can run on an outsourcer's security and which systems can be tested.

Keep a Close Watch On Performance

Outsourcers also need to ensure that the access rights of its customers' users are properly changed as their jobs change and that those rights end when a user leaves the organization.

It's hard enough to track down all the internal systems on which a user may have been granted a password, says Jon Watts, a principal at Booz Allen Hamilton Inc., a McLean, Va.-based consulting firm. "When you add in the component of an outsourcing relationship, it gets even more complex," he says. Auditors and regulators are "going to hold you responsible for ensuring the right access to your systems, whether you do it directly or if your outsourcer" does, Watts says.

Outsourcing customers should first clean up their internal processes for maintaining proper user-access rights and then build those same requirements into contracts or SLAs with outsourcers, says Watts. This includes, "performance monitoring to make sure these things are actually happening," he says.

Periodic audits are a vital and accepted part of the monitoring process. They are valuable because they are structured, evaluate the same criteria consistently and produce a detailed view of the outsourcer's actual performance over time.

However, they produce only a point-in-time snapshot that may overlook more critical and immediate problems. That's why a small but growing number of outsourcing customers are also using dashboards or other software to dynamically monitor an outsourcer's security performance.

See It All With Real-Time Monitoring

Dashboards gather and analyze information drawn from an outsourcer's security, identity management or access management systems and present it in a graphical, easy-to-understand form. Many security monitoring and control tools that internal systems administrators already use can present reports to a user outside the production network, such as a customer wanting to monitor the quality of an outsourcer's performance. Whether a specific dashboard

Road Map to Secure Outsourcing

1. Based on an internal assessment of critical data, **be very specific in contracts and service-level agreements** about which security processes you expect your outsourcer to perform and how.
2. **Use established standards where possible,** and even standard outside reports, to develop requirements or assess your outsourcer's performance.
3. Where necessary, **specify the proper access-control measures** the outsourcer must take, including which of its employees have privileged access to databases and networks.
4. **Consider supplementing audits** with real-time monitoring of systems or security logs.

> **[Auditors and regulators are] going to hold you responsible** for ensuring the right access to your systems, whether you do it directly or if your outsourcer [does].
>
> **JOHN WATTS,** PRINCIPAL, BOOZ ALLEN HAMILTON

SECURITY IS TOP OF MIND

When selecting an outsourcing partner, what are the most important evaluation factors?

1. Capabilities and quality of services
2. Pricing of service and cost savings to the company
3. Provider's security policies, capabilities and track record
4. Financial strength and business stability
5. Reputation, brand and references
6. Provider's regulatory and compliance history
7. Geographic factors

SOURCE: BOOZ ALLEN HAMILTON INC. SURVEY OF 158 EXECUTIVES, MARCH 2006

is right for the job depends on its ability to draw data from the various systems at the outsourcer, how well the dashboard can protect the information, and its ability to analyze and report on its findings.

One such tool is Consul InSight Security Manager from Consul Risk Management Inc. It monitors the actions of database administrators and other employees at the outsourcer, assesses whether the outsourcer's IT infrastructure complies with the customer's regulatory requirements, monitors database access, and manages logs for network and security devices.

One customer deploys the Consul software across a virtual private network to monitor an outsourcer that manages about 20,000 of its servers. Consul presents the results in the form of 20 to 30 custom reports. When an auditor asks for a report on change management violations at the outsourcer, for example, the customer can simply hit the print button on the product to generate the report, says Marc van Zadelhoff, Consul's vice president of marketing and business development.

Dashboards summarizing the data gathered by such tools should be created not just for executives, but also for various management levels within the customer, says Guillermo Kopp, a vice president at TowerGroup, a research and consulting firm in Needham, Mass. Executives might need "the very big summary saying all systems are go; the lights are green," he says, with only network and systems managers receiving information about specific transactions.


Guillermo Kopp

But like some other observers, Kopp suggests using dashboards "for a sense of if the outsourcer is doing well," and drilling down into specifics such as analyzing firewall or access logs only if there's evidence that the outsourcer is failing or during a periodic audit.

Ted Julian, vice president of marketing at Application Security Inc., a vulnerability scanning and monitoring vendor, says regular reports on how well the outsourcer is following the customer's contractual requirements for patch and password management "is probably more important than real-time reporting" from the outsourcer's security systems. Tracking the outsourcer's performance on criteria the customer set beforehand, such as how often user passwords must be changed and how quickly security patches are applied, are better indicators of whether the outsourcer's security performance is improving over time, he says.

WORRIED ABOUT CYBERSPACE

When evaluating or managing outsourcing relationships, how concerned are you about the following types of security threats?

CYBERTHREATS

Percentage of respondents who answered "very important":

64 % Theft, misuse or damage of company systems and data from **outside** the outsourcer (such as system hacking, viruses, spyware infiltration)

62 % Theft, misuse or damage of the company systems or data from **inside** the outsourcer

NON-CYBERTHREATS

Percentage of respondents who answered "very important":

35 % Theft or damage of data or assets via compromises of **physical security** (break-ins, vandalism)

35 % Compromise of operating continuity due to **external factors** (natural disasters, political instability)

SOURCE: BOOZ ALLEN HAMILTON INC. SURVEY OF 158 EXECUTIVES, MARCH 2006

BIGGEST CHALLENGES

Which factors present the biggest management challenges in evaluating and managing security in outsourcing relationships?

1. Establishing effective security management requirements in the contracts
2. Monitoring, auditing and evaluating vendor compliance with an established security policy
3. Evaluating and implementing security technology and process integration
4. Acquiring and maintaining the right skills and capabilities to manage security
5. Determining how much to invest in security in an outsourcing relationship
6. Delivering effective training in policies and procedures of outsourcing providers

SOURCE: BOOZ ALLEN HAMILTON INC. SURVEY OF 158 EXECUTIVES, MARCH 2006

Develop Your Own Security Policies

One reason many customers find it hard to trust their outsourcers' security claims is that different standards bodies promote different security standards and use different types of reports to monitor compliance with those standards. The lack of standards "makes it hard to compare vendors apples to apples," says Watson Wyatt's Hunter.

And while security management and monitoring tools are improving, some observers say it's still too hard to get an overall view of their own security situations — much less that of an outsourcer. Hunter uses multiple tools from different vendors and a third-party scanning service to monitor the security of his applications. But he says it's still a major challenge to get a single view of all the vulnerabilities within all systems and how changes to any of those applications and platforms will affect the security of other parts of the IT infrastructure.

All these complexities make it even more important for customers to develop effective security policies for themselves before they try to determine how good a job an outsourcer is doing. "You've got to look at your own security processes," says Watts, before deciding whom to outsource to and how to keep an eye on them. ◆

Scheier is a freelance writer based in Boylston, Mass. He can be reached at rscheier@charter.net. Additional reporting by Galen Gruman.

Back -to- Basics SECURITY

OPINION

Bart Perkins

UNDER THE Sarbanes-Oxley Act and the European Union's data-protection directives, you're responsible for any security breaches that occur — both yours and your outsourcer's. Fortunately, many security products are becoming more economically viable. Retina scans and voice recognition are now feasible identification tools. Cryptographic hashes used for data encryption (such as SHA-1 and Snefru) are growing stronger. Statistical anomaly techniques for intrusion detection are also improving. Researchers are working on systems to identify people by odor, ear shape, hand vein patterns and gait.

However, even the most advanced tools won't protect you if basic security procedures are not in place. The 2005 Computer Security Institute/FBI survey reports that only half of corporate security breaches fit the stereotype of cybercriminals using the latest James Bond tools or Defcon techniques. The other half originate inside your own organization through, for example, human error, poor procedures or employee theft.

Basic security controls will prevent most security breaches. **Make sure your outsourcer takes at least the following steps:**

- **Conducts background checks on all employees.** Insider attacks are the hardest to prevent.
- **Disables orphan accounts promptly.** Passwords and e-mail accounts should be disabled as soon as an employee leaves. Although this seems obvious, it can be difficult in organizations with decentralized security management systems or where many outsiders (contractors, researchers, etc.) are granted access.
- **Establishes a physically secure environment.** Many buildings require entry badges but can be easily entered by "tailgating" employees who hold doors open. Server centers are often in buildings subject to fires, floods, earthquakes — or roof leaks.
- **Secures the electronic environment.** Easy hacker access should be eliminated by disabling wireless networks and closing any open ports. Make sure passwords are complex enough to be secure and are changed regularly. (Many employees still leave their passwords taped to their monitors!) Servers and data should be virtualized. Software patches must be applied regularly, and backup files should be sent to a secure off-site location.
- **Develops security procedures.** Ensure that your outsourcer complies with regulations such as the Gramm-Leach-Bliley Act and HIPAA or industry standards such as PCI-DSS for credit card handling.
- **Establishes an intrusion-detection group.** The Internet Engineering Task Force is developing a common format for tracking electronic intrusions. Monitor its progress, and make sure the eventual standards are adopted.

Expect your outsourcer to provide basic security; consult industry associations such as BITS or universities such as Rutgers for checklists. Make sure security controls are specified clearly in your contract. Large outsourcers can provide additional levels of security — at additional cost. Carefully analyze your need for extra security, since all data is not equally sensitive. Balance the cost of additional security against the probability and cost of potential loss, then factor in your company's tolerance for risk.

Security considerations are critical to successful outsourcing efforts. Before you sign the contract, make sure your outsourcer can provide security levels that match your organization's needs. Prevent predators from leveraging small security mistakes into enormous and costly losses. ◆

Perkins is managing partner at Louisville, Ky.-based Leverage Partners Inc., which helps organizations invest well in IT. He was previously CIO at Tricon Global Restaurants Inc. and Dole Food Co. Contact him at BartPerkins@LeveragePartners.com.