INFORMATION SECURITY®
DECEMBER 2010/JANUARY 2011

Game Changer

The DATA ACCOUNTABILITY AND TRUST ACT would supercede state data protection laws. Here's what you need to know.

also

SECURITY'S ROLE IN DISASTER RECOVERY

HOW ARE YOU AT VENDOR MANAGEMENT?

TechTarget
INFOSECURITYMAG.COM

FROM OUR SPONSORS

contents

DECEMBER 2010/JANUARY 2011
VOLUME 12 NUMBER 10

FEATURES

DEPARTMENTS

ALSO

Waging an endless war against security threats? We can help you prepare for battle.

Security threats like viruses, worms and hackers are toxic to your infrastructure. Fighting them off can burn through your time, and your budget. Not to worry. At CDW, we have your back. We have the people, products and plan to help keep your systems and sensitive data safe. Our security specialists can assess your infrastructure as well as design and implement a solution tailored to your needs. We know the latest threats and are well-versed in combating them. It's why we're the best allies in the business.

For free Symantec trialware, how-to videos or more information, visit CDW.com/protectionsuite

Symantec. + CDW

Symantec and CDW. Partners and problem-solvers.

Don't Get Left Behind

Cloud computing presents a lot of security issues but security professionals need to accept the challenge. BY MARCIA SAVAGE

UNLESS YOU'VE BEEN living under a rock, you know that cloud computing is all the rage these days. Cash-strapped businesses are eagerly looking to move IT operations and applications to the cloud in order to cut costs. For enterprise security managers, this trend is nerve-wracking to say the least. Already battered by constantly evolving Internet threats and compliance demands, the last thing you want to do is lose control of your corporate data to a cloud service provider.

But you better figure out a way to deal with this cloud phenomenon. As several industry experts pointed out at the Cloud Security Alliance Congress 2010 in November, cloud computing is a trend that's here to stay.

More than one speaker at the conference described cloud computing as a train ride and security professionals should make sure they aren't left behind. Symantec Chairman John Thompson drew a particularly colorful analogy, comparing cloud computing to Mother Nature, against which it's futile for IT professionals to fight. He and other speakers urged security pros to embrace the trend as an opportunity for improvement.

More than one speaker at the conference described cloud computing as a train ride and security professionals should make sure they aren't left behind.

What's to embrace from a security perspective, though? Cloud computing raises all sorts of issues. Depending on the model, there's a loss of control. There's the lack of visibility; some cloud providers are far from forthcoming about how they protect data. How do you maintain compliance with regulatory requirements and industry standards when working with a cloud provider?

And as Scott Charney, Microsoft's corporate vice president for Trustworthy Computing, pointed out in a conference keynote, while there are a lot of reasons to move to the cloud, aggregating data creates rich targets for bad guys. Breach investigations can become problematic in multi-tenant environments, he noted. "Information aggregation will put pressure on identity," and the traditional user name and password method won't cut it anymore, he added.

However, there is a lot of work underway to tackle cloud security issues. Born two years ago, the nonprofit CSA is a broad coalition of security practitioners, industry experts, and vendors. The group, which has more than 13,000 members, has published security guidance on the critical areas of focus for cloud computing, a paper on top cloud computing threats, and recently unveiled the CSA Governance, Risk Management and Compliance Stack. The

GRC stack is a set of three free tools designed to help companies, cloud providers and others to assess both private and public clouds against industry standards, best practices and compliance requirements.

To be sure, moving IT operations and applications to a cloud environment will require a shift in security thinking. Some, like Thompson, say it will mean a transition from focusing on securing devices and infrastructure to an information-centric approach. Focusing on protecting the truly sensitive data in an enterprise makes sense as traditional network perimeters continue to crumble with mushrooming numbers of remote workers and smart phones.

Certainly, there's a lot of hard work ahead for security professionals as companies forge ahead into the cloud, but be assured that there are a lot of smart people working to get ahead of the issues.

Certainly, there's a lot of hard work ahead for security professionals as companies forge ahead into the cloud, but be assured that there are a lot of smart people working to get ahead of the issues. There are tools and knowledge available that can help, and security pros should take advantage of them.

Thompson told CSA Congress attendees not to fear the cloud; the security industry will adapt and solutions will be found, he said. Speaking from 40 years of experience in the technology industry and having seen a lot of changes, Thompson's words carry weight.

Security is often criticized as reactive, but with cloud computing, security professionals have a chance to be proactive. At the risk of overusing the phrase, don't let the train pass you by.›

Marcia Savage is editor of Information Security. *Send comments on this column to feedback@infosecuritymag.com.*

Find the cybercriminal.

(Never mind. ArcSight Logger already did.)

Stop cybercriminals, enforce compliance and protect your company's data with ArcSight Logger.

ArcSight™

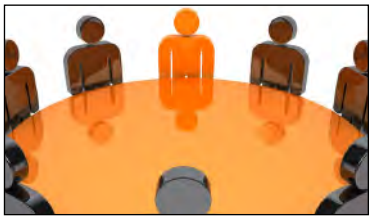
Learn more at www.arcsight.com/logger.

COMING IN FEBRUARY

ENDPOINT INTEGRITY

Endpoint integrity is an important security control, especially for organizations with large and productive on-the-go workforces. Laptops, netbooks, tablets, and smartphones seeking access to centralized data and applications are often out of policy or even compromised. Integrity checks can be used to determine whether endpoints are non-compliant, infected with malware, or running risky applications. In this Supercast, you'll learn about the many endpoint integrity enforcement options at your disposal, from directory-based group policies to network access controls. Discover how to select and deploy endpoint integrity technologies, craft policies, and quarantine problem endpoints.

PRIORITIES 2011



Want to compare your strategic initiatives and budget plans with what your peers are doing? Our annual Priorities survey provides a view into what's ahead for the security industry. More than 600 readers participated and shared their technology and process priorities for 2011. This year, our survey also looks at the changing roles of security professionals in the enteprise. You'll want to know what your peers are doing to protect corporate assets and how enterprise security jobs are evolving.

SCADA SECURITY

The Stuxnet Trojan put the spotlight on critical infrastructure protection and the inherent security vulnerabilities in SCADA control systems. More than ever, there is increased attention on critical infrastructure protection because of state-sponsored espionage and the emergence of the advanced persistent threat into the security lexicon.This feature will look at critical infrastructure protection in context of the Stuxnet threat, and examine the regulatory and technology efforts being undertaken to improve the state of CIP security.

In every issue: *Information Security* magazine is the insider's publication for security professionals. In every issue, we tackle the trends and technologies that most impact your day-to-day responsibilities. We complement that coverage with opinion from our editors, the industry's leading practitioners and experts such as Bruce Schneier and Marcus Ranum.

MUST READ!

websense®

ESSENTIAL INFORMATION PROTECTION™

The Fast Path to Industry-Leading Security

The right Security-as-a-Service solution can perform reliably and effectively and deliver the flexibility and control associated with on-premise solutions — at a significantly lower cost — without compromising privacy and security.

When choosing a SaaS provider, consider the market-leading capabilities provided by Websense solutions.

To learn more, visit www.websense.com

Open Season on Internet Privacy

In the 112th Congress, enterprises can expect a heavy focus on Internet privacy issues on Capitol Hill.

BY JUDITH HARRIS, CHRISTOPHER CWALINA AND AMY MUSHAHWAR

WITH THE OBAMA Administration's reported "watchdog" plan for online privacy and U.S. Rep. Joe Barton's November statement that Internet privacy policies will be in the crosshairs in the next Congress, privacy remains one of many bull's eyes for the 2011-2012 policy agenda. Adding to this renewed fervor toward privacy issues, the Department of Commerce and the Federal Trade Commission are poised to release comprehensive reports regarding the collection, use and security of personally identifiable information. Even the Federal Communication Commission is getting into the mix with its public notice and hearing regarding the regulation of cybersecurity and its recent probe into the information collected by Google Street View.

So, here's what enterprises will want to keep an eye on in Washington D.C. for the upcoming year:

- **Cybersecurity Legislation**, which we expect to be along the lines of the pending bill proposed by Senator Joseph Lieberman in the 111th Congress, S. 3480, that would address both public and private sector cybersecurity;
- **Do-Not-Track Registry for Web Activities**, given the popularity of the National Do-Not-Call Registry, this is a tangible concept for consumers no matter how difficult it would be for industry to implement (and there have been recent statements by the FTC that such a registry could be created unilaterally by the agency);
- **Privacy by Design**, given recent statements by FTC Commissioners that privacy by design—or privacy contemplated in the R&D process—is paramount to staying ahead of the technological curve (and is in line with efforts abroad);
- **Greater Breach Notification Uniformity**, in recognition of the angst that private industry is feeling over the current patchwork of sector-specific federal breach notification laws and breach laws in nearly all 50 states;
- **Harm Standard**, given FTC consumer protection chief David Vladeck's numerous statements that focusing solely on tangible harm—current protections against financial harm (identity theft), physical harm (stalking) and intrusions (spam and malware)—leaves gaps in the life cycle of online information collection, we expect the FTC to discuss whether privacy protection should move from a harm-based standard to something closer to the European individual right model;
- **Sensitive Information**, we expect a statement regarding the categories of personally iden-

tifiable information that should not be collected at all (such as health data and sexual orientation) in keeping with the FTC's preliminary statement about this topic in its Behavioral Advertising Guidelines;

- **Customer PII Access and Correction Mechanisms**, which would be in line with EU privacy law and some US laws;
- **Further Privacy Policy Simplification**, given increasing frustration with some private sector privacy policies and recent government efforts to address this issue, such as forms creating standardized privacy policy models in the financial sector;
- **Behavioral Advertising**, we expect continued discussions regarding Internet advertising issues before Congress or the FTC and whether this activity is best addressed under regulatory mandates or voluntary self regulatory principles;
- **Increased International Transborder Data Flow Cooperation**, especially given the EU's differing approach to transborder transfers of data and the continued dialogue regarding revisions to the U.S. Safe Harbor Program.

Finite definitional points (such as the meaning of first-party collection or personally identifiable information), jurisdictional issues, and whether any new guidance would apply to off- and online data will be important, heavily debated issues.

As we are all aware, the devil will be in the details as to how each of these issues will be addressed. Finite definitional points (such as the meaning of first-party collection or personally identifiable information), jurisdictional issues, and whether any new guidance would apply to off- and online data will be important, heavily-debated issues. And with the Republicans now in charge of the House of Representatives, there is still ample support for privacy in principle. But, in the months ahead, we can expect a change in tone of the debate. Republicans will be more suspect of any proposed government enforcement mechanism that has the potential to stifle innovation.›

Judith L. Harris, Christopher G. Cwalina and Amy S. Mushahwar are attorneys in the Data Privacy, Security and Management practice in the Washington D.C. law offices of Reed Smith LLP. Send comments on this column to feedback@infosecuritymag.com.

Did I just *send* that **file** to the ***wrong person?***

Check Point **DLP** prevents data breaches before they occur

Have you ever accidentally sent an email to the wrong person or attached a document that wasn't meant to be shared?

Check Point makes DLP work by combining technology and processes to move businesses from passive detection to prevention, before data breaches occur.

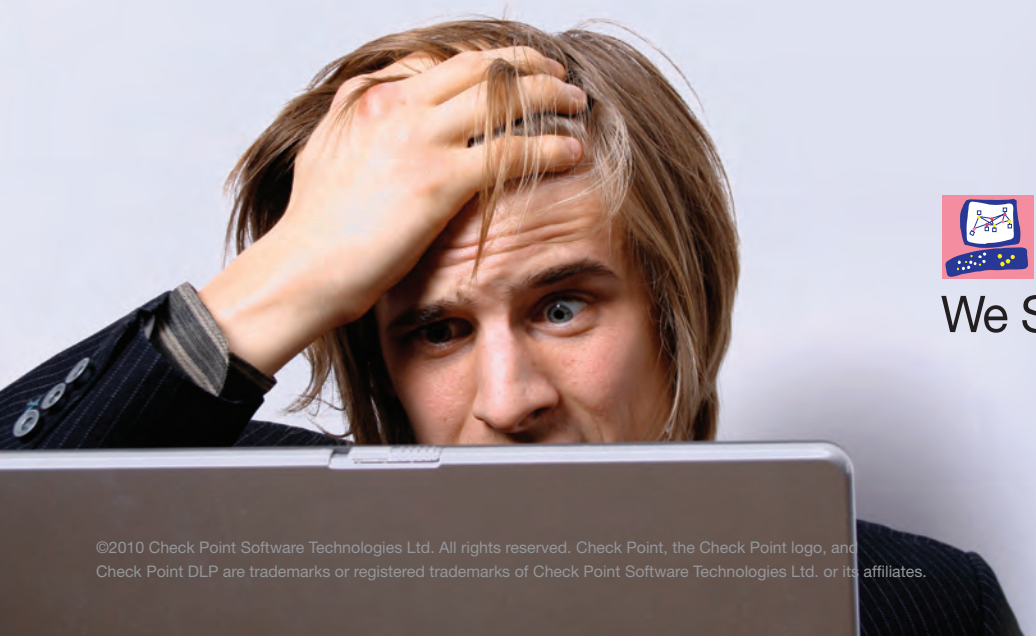
PREVENT data loss

EDUCATE users

ENFORCE data policies

Get the **FREE** Frost & Sullivan white paper now and learn how Check Point DLP can help you prevent data loss at:

www.checkpoint.com/dlp_whitepaper



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

ANALYSIS | MALWARE

Experts Advocate New Response to Customized Malware

Cybercriminals are targeting weak network configurations and taking advantage of poorly deployed security software with customized malware. BY ROBERT WESTERVELT

WHEN INVESTIGATORS at Trustwave's SpiderLabs forensics team responded to a breach at an international VoIP provider earlier this year, the conditions they found at the provider's data center were appalling to say the least. Servers containing data on 80,000 customers were located in a run-down barn. To make matters worse, the investigators had to endure the odor from about 20 farm cats living among the equipment.

The third-party hosting service looked professional; its website boasted of hundreds of customers and even included pictures of a hardened data center. The VoIP provider was the target of customized malware—a rootkit—which took advantage of the hosting service's weaknesses. The VoIP provider realized it had a problem only after customer complaints came pouring in—months after the malware did what it was designed to do. The cybercriminals were long gone, says Jibran Ilyas, a senior security consultant for Spiderlabs.

Customized malware is a growing problem, he says. Poor network configurations, shoddily deployed security software, and an over-reliance on traditional, signature-based antivirus is resulting in some very costly data breaches, he says.

"We always tend to over-estimate the big environments; we think they're going to be really secure," Ilyas says. "It's only until we get there that we realize there's a major gap between the skill level of IT administrators and security folks who do the job."

Ilyas says companies such as the VoIP provider have no chance against cybercriminals wielding customized malware. For example, typically ports are open to enable outsourced IT operations to gain remote access to the network. "If those ports are open for integrators, they're also open for the hackers," he says.

Companies that fail to properly evaluate their outsourced operations are also likely relying

on poor or even misconfigured security software to protect their network. In addition to keystroke loggers and network sniffers, malware with memory parsing capabilities are almost no match for antivirus software, says Greg Hoglund, a malware expert and founder of HBGary.

He has been railing against the effectiveness of antivirus, warning that many companies rely too much on traditional signature-based approach to detecting and eradicating malware.

"Most organizations in the commercial space rely entirely on their AV vendor to do all of the end-node security for the network," Hoglund says. "This model doesn't work very well because the AV vendor has no idea about the threats targeting an individual site."

Hogland says organizations need to improve incident response procedures. Many organizations eliminate the malware and reimage an infected machine. Hoglund says incident responders need to conduct a basic level of forensics, examining the company logs and DNS records. Looking at the malware's characteristics could reveal information used to detect other infections on the network. Malware fingerprinting and attribution techniques are going to be needed because traditional signature-based methods can't keep up, he says.

Paul Laudanski, who headed more than a hundred volunteers who investigated spam and phishing attacks and malware for his website CastleCops.com, couldn't agree more. For several years, Laudanski and his wife Robin made headway capturing IP addresses and foiling cybercriminal operations. Fed up with unrelenting denial-of-service attacks against his site and strapped financially, they shuttered the operation at the end of 2008.

"Malware is always going to be a big component," says Laudanski, who now works for antivirus vendor ESET. "The fundamental attacks continue because hackers are always going to look for vulnerabilities they can exploit, but we're also seeing more targeted attacks cause problems."

"The bad guys are creating forums, they're providing support services and even have development teams to create targeted malware designed to penetrate networks and remain undetectable."

–JAMES LYNE, senior technologist, Sophos

Some experts are also identifying a shift in the way cybercriminals are conducting their operations. James Lyne, a senior technologist at UK-based security vendor Sophos, says cybercriminals are moving from randomly stealing credit card numbers and personal information to far more structured, organized criminal activity. Sophos engineers were detecting 5,000 pieces of malicious code a day at the end of 2009, Lyne says. Today on average, the same engineers are looking at more than 60,000 malware samples a day.

"The bad guys are creating forums, they're providing support services and even have development teams to create targeted malware designed to penetrate networks and remain undetectable," Lyne says. "You've got to be secure on all fronts, not just with your security technology if you expect to keep your systems safe."

Robert Westervelt is news director of the Security Media Group at TechTarget. Send comments on this article to feedback@infosecuritymag.com.

Keep Productivity High and Security Threats Low

Social Media and Web 2.0 platforms like Facebook, Twitter and YouTube are everywhere. Even at work. That means more viruses, more malware and less productivity. It is a triple threat to your business.

Smart IT managers recognize these productivity and performance damage losses from Web 2.0 and are taking steps to address them. Steps like installing NETGEAR® ProSecure® content security appliances.

ProSecure security appliances keep productivity high and security threats low by blocking the Web 2.0 applications you don't want while allowing access to the ones you do.

NETGEAR ProSecure-handling the triple threat that is Web 2.0. Isn't it time you looked into a reliable, affordable and simple solution?

Learn more at **www.prosecure.netgear.com**

NETGEAR®
PROSECURE®

Bug Bounty Bandwagon

by *Information Security* staff

When Barracuda Networks launched its bug bounty program in November, it joined a growing number of companies offering rewards to researchers who uncover security flaws. Barracuda, a maker of antispam, antivirus, firewall and Web filtering appliances, is offering between $500 and $3,133.70 to bug hunters who find serious vulnerabilities in its products. Other vendors offering similar programs include:

Google: The search giant launched its bug bounty program earlier this year to reward security researchers who reported Chrome browser flaws. Google has said it would reward as much as $3,133.70 for significant flaw finds. The number refers to "eleet," sometimes identified as 31337, an alternative alphabet used by coders on the Internet. In November, Google extended the program by adding rewards to researchers who find serious Web application flaws in its Web properties Blogger, Orkut, and YouTube.

Mozilla: The maker of the Firefox browser and other programs launched its Security Bug Bounty Program in 2004, funded by Linux distributor Linspire (now owned by Xandros) and Mark Shuttleworth, founder of the Ubuntu Project. Researchers who report of valid, critical security bugs receive a $3,000 cash reward and a Mozilla T-shirt. In July, Mozilla increased the maximum cash reward from $500.

TippingPoint: Launched five years ago, Tipping Point's Zero-Day Initiative (ZDI) buys vulnerabilities from researchers, offering various levels of payment depending on the severity of the exposed flaw, the value of the vulnerable product, and other criteria. The company provides an IPS signature to protect its customers from the vulnerability and sends a report to the affected vendor. TippingPoint, which is owned by Hewlett-Packard, announced in August that ZDI would begin enforcing a six-month deadline on vulnerabilities that it submits to vendors.

VeriSign: iDefense launched its reward program for software flaws way back in 2002, and VeriSign kept up the program when it bought the company in 2005. The iDefense Labs Vulnerability Contribution Program claims to pay more for high-quality research than anyone.

overheard

"Don't fight Mother Nature. It's inevitable that applications will move to the cloud, it's just a matter of which ones. Embrace the change and manage the change in a way that's effective for your business."

–SYMANTEC CHAIRMAN JOHN THOMPSON

Protect Your Customers' Confidential Data

If you are looking for a complete data loss prevention (DLP) solution (network, endpoint, and discovery) with a scalable architecture that is fast-to-deploy and easy-to-manage, then you need consider Code Green Networks TrueDLP®. Unlike other complex data loss prevention solutions (McAfee, RSA, Symantec, Websense), Code Green Networks enables organizations to cost effectively solve their data leakage problems in days not months.

Key Benefits of Code Green Networks TrueDLP Data Loss Prevention Solution

- Fast-to-deploy and easy-to-manage
- Complete DLP (network, endpoint, and discovery) without the complexity
- Ensure regulatory compliance by automatically encrypting sensitive data (HIPAA, PCI, etc.)
- Lowest total cost of ownership (TCO) and no dedicated resources required
- Detects sensitive content, monitors network use, and enforces policies to ensure protection
- Complete visibility into file and device activity on endpoints
- Approximately 1/3 the cost of the more traditional DLP providers

SC MAGAZINE BEST BUY

"Overall, we were impressed with the scalable and flexible performance of the tool and the all-inclusive nature of the [dlp] solution." ***SC Magazine, May 2010***

SEE A DEMO
www.codegreennetworks.com/demo

CODE GREEN NETWORKS

Invest in Yourself

Choose wisely when pursuing industry certifications and advanced degrees to gain the best competitive advantage.

BY LEE KUSHNER AND MIKE MURRAY

INFORMATION SECURITY PROFESSIONALS have been conditioned to invest in their careers. Whether through traditional methods such as security certification courses or advanced degrees, you have expectations that by achieving these credentials, you will accelerate your career. By investing in yourself, you're on the right track; any investment that helps develop skills, expand knowledge and provide additional education is a good one. However, the expectation that a single common career investment will provide you a competitive advantage over others is unrealistic.

The CISSP certification is a prime example of this. When the information security industry was in its formative years, Certified Information Systems Security Professionals (CISSPs), were rare. Holding the CISSP certification provided a much greater advantage over peers who did not. Employers placed a higher value on this designation, and rewarded professionals with advanced compensation and accelerated career paths. Today, the CISSP is much more commonplace and does not serve as the talent differentiator it once did; (ISC)², which governs the CISSP, reports on its website there are more than 60,000 certified professionals worldwide. Instead, CISSP certification training has become more of a requirement and the absence of this particular career investment could negatively separate you from peers.

Annually allocate and budget time and money to invest in your career.

When determining a career investment strategy, it is paramount to refer to your career plan and map your investments toward your intended result. Annually allocate and budget time and money to invest in your career. This should be akin to contributing to your 401K or insurance programs. Considering that your professional skills are the keys to generating current and future income, allocating money for your professional development provides you with better control over your future than any other investment that you can make.

Next, you need to figure out the best way to achieve maximum value for your investments; these costs vary greatly and can come in the form of a

Lee Kushner's and Mike Murray's blog can be found at www.infosecleaders.com where they answer your career questions every Tuesday, or you can contact them via email.

Lee Kushner is the president of LJ Kushner and Associates, an information security recruitment firm, and co-founder of InfoSecLeaders.com, an information security career content website.

Mike Murray has spent his entire career in information security and currently leads the delivery arm of MAD Security. He is co-founder of InfoSecLeaders.com, where he writes and talks about the skills and strategies for building a long-term career in information security.

weeklong training course, a personal coach, or a conference to help you address a deficient skill. These environments generally will enable you to pinpoint specific needs and give you the opportunity to address them in a condensed time frame, under guidance from a recognized authority. Some examples are management seminars, sales training, or time management courses. Although these may be viewed as minor investments of time and money, they can provide a significant impact on your long-term professional development.

Another key component of a career investment strategy is the branding associated with the career investment. Considering the achievement will be on your resume and discussed during an interview or promotion process, you should feel comfortable with the external image it enforces and impression it portrays to others. One of the best examples of this could pertain to the perceived quality of an advanced degree, such as an MBA. The fact is: You can receive an MBA from many different schools, but top-tiered MBA programs carry a better brand than MBAs from distance-learning programs. If your career goal is to become a CISO of a Fortune 500 firm, chances are that someone on the interview team will hold an MBA from a top-rated school. By carrying a similar brand into the interview process, you should give yourself a competitive advantage over others vying for the same role. In addition, if you have an MBA from a school that is not viewed upon favorably, the career investment could have an opposite effect, and could possibly eliminate you from consideration.

Probably one of the most overlooked factors in selecting a career investment is the value of knowledge and personal growth. Generally speaking, if you select to pursue a career investment for personal satisfaction, you are able to do so at your direction and without advanced expectation. Making yourself smarter, more effective and more complete has benefits in the workplace and beyond. As security professionals working in diverse environments, dealing with global issues and multicultural workforces, gaining a broader understanding of relevant topics that have a personal interest can only be helpful. Although nothing is for certain, if you decide to let this principle guide the direction of some of your career investments, you may be pleasantly surprised by the future impact it may have on your career development.

As security professionals working in diverse environments, dealing with global issues and multicultural workforces, gaining a broader understanding of relevant topics that have a personal interest can only be helpful.

As the information security profession continues to mature and competition for information security leadership roles increases, it will become more important for information security pros to differentiate themselves from their peers. Developing a consistent pattern of logical career investments is one of the better ways to accomplish this. Information security professionals who are able to effectively map their personal career investments to their long-term career goals should have a much better chance of achieving them.›

Send comments on this column to feedback@infosecuritymag.com.

Database protection and compliance made simple.

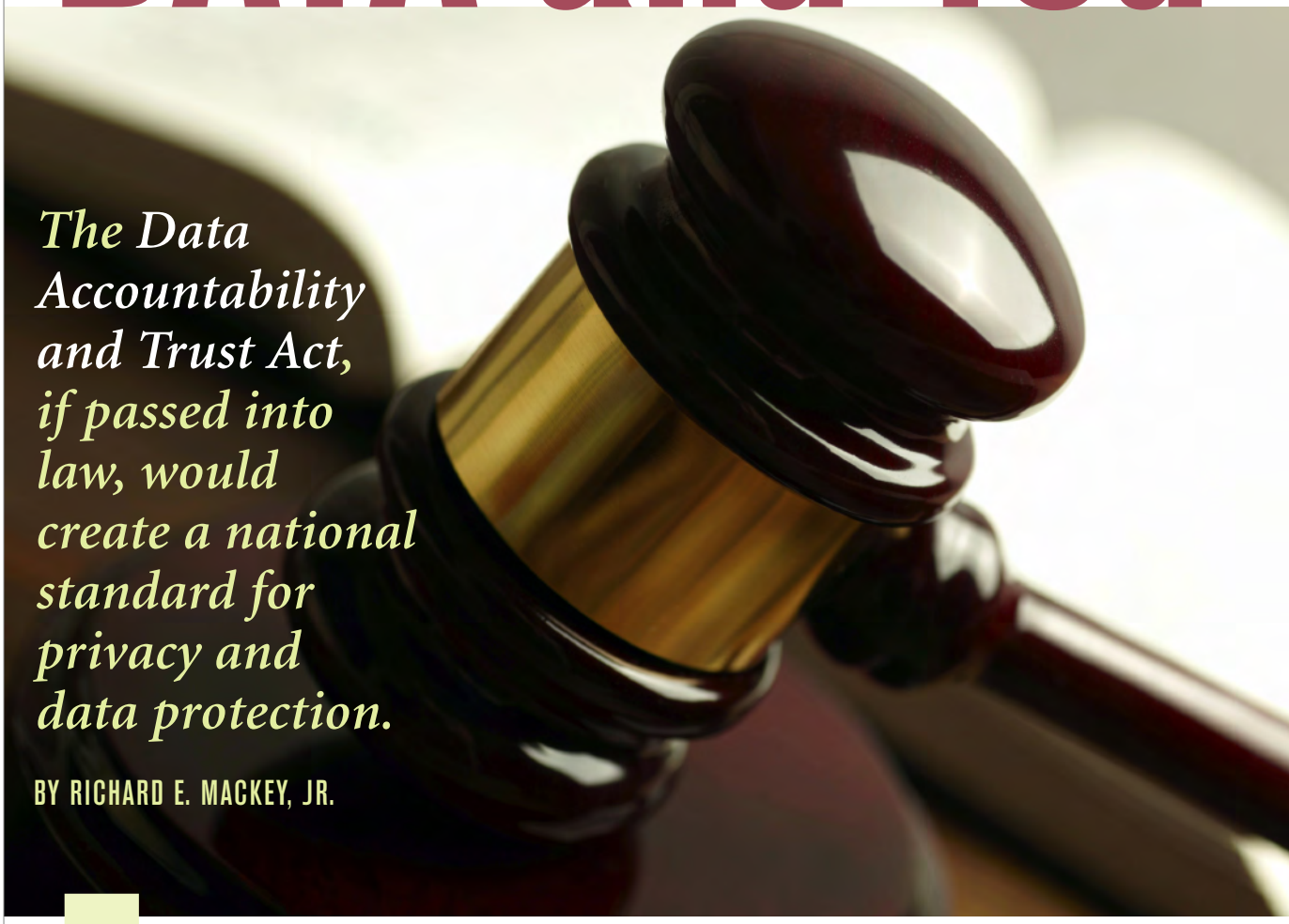
Guardium, an IBM Company, provides the simplest, most robust solution for continuously monitoring access to high-value databases and automating compliance controls for heterogeneous environments – assuring the integrity of trusted information and enabling enterprises to drive smarter business outcomes.

- Gain 100% visibility and control over your entire DBMS infrastructure.
- Reduce complexity with a single set of cross-DBMS auditing and access control policies.
- Enforce separation of duties and eliminate overhead of native DBMS logs.
- Monitor privileged users, detect insider fraud and prevent cyberattacks.
- Automate vulnerability assessment, data discovery, compliance reporting and sign-offs.

For more information, visit
www.guardium.com/SearchSecurityUK

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

DATA and You



The Data Accountability and Trust Act, if passed into law, would create a national standard for privacy and data protection.

BY RICHARD E. MACKEY, JR.

THERE ARE CURRENTLY more than 40 different state and territorial laws that require organizations entrusted with personally identifiable information to notify individuals when their information has been exposed to unauthorized parties. These laws range from those only requiring notification to those that mandate full security programs designed to prevent breaches in the first place. They define personally identifiable information differently, require different notification processes and force organizations to deal not only with the victims of the breach, but also the attorneys general of all the states where victims reside. The complexity and cost of notification, let alone the difficulty of ensuring compliance with security program requirements, is daunting.

Still, breaches that lead to identity theft happen regularly and people expect organizations to be held accountable for the security of their personal information. Politicians have heard the public outcry and have recognized that there is a need for more uniform protection of

personal data and more manageable and predictable notification processes. Consequently, every year there seem to be a handful of new proposed federal laws to address the growing problem of sloppy handling of personal information and breaches.

At the end of 2009, the U.S. House of Representatives passed the Data Accountability and Trust Act of 2009 (DATA). If passed by the Senate and signed into law, DATA would supersede existing state laws and thereby eliminate the complex array of notification procedures and the myriad protection mechanisms required by the states. The proposed law would also provide a universal definition of personally identifiable information, appoint the Federal Trade Commission to specify regulations and enforce compliance, and require organizations to implement formal security programs to prevent unauthorized access to personally identifiable information. Compared to other data protection legislative efforts, DATA's passage in the House makes it the only bill to gather the necessary support in either chamber. Its impact is potentially far reaching, and organizations should understand how it might affect them.

If passed by the Senate and signed into law, DATA would supersede existing state laws and thereby eliminate the complex array of notification procedures and the myriad protection mechanisms required by the states.

PERSONAL INFORMATION DEFINED

At the heart of DATA, or any data protection law, is the definition of personally identifiable information. The definition is critical because it not only spells out what types of information need to be protected, but also helps organizations strip out elements of data sets to avoid having to protect them. This practice, known as scrubbing, is commonly used to protect credit card numbers and Social Security numbers by masking all but the last four digits.

DATA defines personal information as an individual's first name or initial and last name, or address, or phone number, in combination with any one or more of the following data elements for that person:

- Social Security number;
- Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

This definition is similar to most state breach laws with some notable differences: It does not consider a financial account number alone (without a PIN or password) sensitive. In addition, unlike another proposed federal law—S. 1490, the Personal Data Privacy and Security Act—DATA makes no mention of mother's maiden name as sensitive (even though it is often used to authenticate an individual's identity).

The law would provide room for the FTC to modify the definition of personal information

Security Innovation®
THE SOFTWARE SECURITY COMPANY

Reducing IT Risk
By Securing Your Applications

Application Security TRAINING | CONSULTING | E-LEARNING

Security Innovation focuses on the most difficult problems of IT security, and the root cause of most data breaches – those at the application layer.

The company's world-class application security eLearning and consulting solutions provide IT and Development Teams with the knowledge and programs needed to build internal expertise, create secure software applications and reduce overall information risk.

TRY our application security eLearning FREE at elearning.securityinnovation.com

getsecure@securityinnovation.com

www.securityinnovation.com

+1.978.694.1008

as necessary to accomplish the goals of the act as long as these changes do not unreasonably impede interstate commerce.

APPLICATION AND ENFORCEMENT

As proposed, DATA will be regulated and enforced by the FTC. Consequently, the legislation applies only to those entities over which the FTC has jurisdiction. Even though DATA states that it applies to persons, partnerships, or corporations engaged in interstate commerce, it does not apply to all organizations. One of the most significant repercussions of the appointment of the FTC is the limit of the legislation's jurisdiction; the FTC does not regulate banks, savings and loans, or common carriers such as airlines and railroads.

One of the most significant repercussions of the appointment of the FTC is the limit of the legislation's jurisdiction; the FTC does not regulate banks, savings and loans, or common carriers such as airlines and railroads.

However, the FTC is not the only enforcer of the law. DATA also carves out room for state attorneys general to take action against violators. They are empowered to enjoin further violation, compel compliance, or obtain civil penalties. In other words, state attorneys general have about the same power they have under the current state laws. The FTC or U.S. Attorney General, though, could intervene and limit state prosecution while federal actions are pending.

PREVENTATIVE CONTROLS

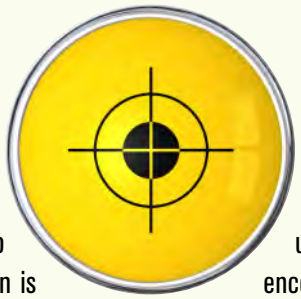
One of the ways DATA distinguishes itself from state laws that simply deal with breach notification is that it requires organizations to implement a security program designed to prevent compromise of the information. Organizations need to:

- Appoint a person as a point of contact who is responsible for overseeing the program;
- Document a security policy for the collection, use, sale, dissemination, and maintenance of personal information;
- Establish contracts with third parties with access to the information to establish controls meeting the requirements of the act;
- Establish a process to identify risks and vulnerabilities and implement administrative and technical controls to mitigate the risk of compromise of the information;
- Define and implement a process for securely disposing of both digital and paper records including personal information.

The security controls required by DATA are similar to those required by state regulations such as Massachusetts 201 CMR 17; they include a risk assessment, a vulnerability assessment, testing, remediation, and secure destruction and disposal of personal information. One notable exception is that DATA only requires organizations to establish contracts with third parties to protect personal information; it does not require definition of the policy and procedure for vetting the security prac-

Information Brokers in the Crosshairs

Companies that collect personal data face extra requirements under DATA.



A MAJOR DIFFERENCE between state laws and DATA is the set of special requirements for information brokers. DATA requires information brokers to implement additional controls and program elements to those required by data owners. This provision is likely an attempt to avoid another breach like the one involving Choice Point in 2005 by making data brokers accountable to the information they collect and sell.

The legislation defines information brokers as a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers. Information brokers collect such data in order to sell it or provide third party access to it for a fee; they may either collect information themselves or contract others to collect and maintain the information. The definition specifically excludes entities that maintain information about employees, customers, or former customers.

Under DATA, information brokers must establish "reasonable procedures" to assure the accuracy of personal information they collect, assemble, or maintain. In addition to striving to maintain accuracy, they must support a program to respond to individuals' written requests to provide information assembled about them once per year. These responses must be provided at no cost to the individual and the method for submitting requests must be conspicuously advertised on the organization's website. Individuals must also be able to use this method for expressing a preference as to how their information might be used for marketing purposes.

If someone finds inaccuracies, the information broker must provide a mechanism for the individual to request changes to correct the inaccuracies. If the broker is not the source of the information (e.g., the data was harvested from public records), the brokers must provide the person the source of the information and a method for correcting the inaccuracy at the source organization. The individual may provide proof that the public record has been corrected and require the information broker to correct its version of the information. Someone may also require a broker to mark the information as disputed if it hasn't been corrected.

As proposed by DATA, when an information broker has a breach, it must follow the same reporting procedures as other businesses. However, these organizations must also submit the policies governing their personal data protection program to the FTC as part of the notification and may be required to undergo an FTC security audit. The FTC has the right to request an information broker's policy at any time.

–RICHARD E. MACKEY, JR.

tices of these organizations. Some state and federal regulations, most notably 201 CMR 17 and HIPAA, provide more in-depth requirements for dealing with business associates and service providers. This may be an area that the FTC will spell out more clearly if DATA becomes law.

The legislation also does not provide requirements for where encryption is required. State laws and regulations from Massachusetts and Nevada require encryption of personal information when it is transmitted over public networks or stored on removable devices. This may also be an area eventually addressed by FTC regulations or guidance.

BREACH NOTIFICATION RULES

Any organization that has gone through the process of breach notification according to multiple state laws would likely welcome the single set of rules that would come from a federal law.

DATA defines "breach of security" as the unauthorized access to or acquisition of data in

electronic form containing personal information. However, the legislation allows the data owner to avoid the process of notification if the data owner determines that there is a no reasonable risk of identity theft, fraud, or unlawful activity. While this is a rather broad statement, it means, at a minimum, that information that was encrypted and exposed to unauthorized parties would not be considered breached.

In the event of a breach, DATA requires data owners to notify the FTC and directly notify each individual throughout the U.S. whose data has been exposed. This notification must take place within 60 days of discovery of the breach.

The data owner may send notice in writing or electronically. However, electronic notification is only acceptable if the individual has consented to receiving official communications in that manner. In cases where the data owner does not have complete contact information for all individuals, the data owner may use email to the full extent possible, publish a notice on its website, and issue notification in print and broadcast media for areas where the victims reside.

The notification must include a description of the information breached and a toll-free number to inquire about the breach. The letter must also include an offer to receive free quarterly credit reports for two years or a credit monitoring service. The individual must also be given toll-free numbers for credit reporting agencies and contact information for the FTC to learn about identity theft.

PENALTIES

DATA sets out steep penalties for violations, which come in two types: failure to comply with security program requirements, and failure to follow the breach notification rules.

The two types of penalties are calculated differently. The amount for security program penalties is based on the number of days the organization is found to be noncompliant multiplied by a maximum of $11,000 per day. Notification penalties are calculated by multiplying the number of violations—individuals they failed to notify—by an $11,000 maximum. Each failure to send notification is considered a separate violation. The Act sets the maximum civil penalty for violations of each type to $5 million, making it possible for a single organization to pay up to $10 million for a combination of security program and notification violations.

The Act sets the maximum civil penalty for violations of each type to $5 million, making it possible for a single organization to pay up to $10 million for a combination of security program and notification violations.

LOOKING AHEAD

The biggest difference between existing state laws and the proposed federal laws (both DATA and other similar bills) is the inclusion of special requirements for information brokers *(see p. 25)*. This special treatment will not be taken well by the large organizations in the information broker business as it increases cost substantially.

It will be interesting to see how information brokers and businesses in general react to these

bills as they are debated in the Senate. Maplight.org, a nonprofit, nonpartisan research organization that tracks money and influence in the U. S. Congress, shows that the backers of the bill receive campaign contributions from finance companies and credit agencies. This makes sense as both these groups would benefit from stronger identity controls. Maplight.org shows no money associated with opposition to the bill–at least not as yet.

DATA clearly has benefits for the general population and, whether they want to admit it or not, businesses that will need to notify people when breaches occur. The overall approach of ensuring that organizations formally protect information, implement sound technical controls that include risk assessment and treatment, and follow a uniform set of notification and support procedures promises to reduce the incidence of identity compromise and create incentives to improve overall security.›

Richard E. Mackey, Jr. is vice president of consulting at SystemExperts, an information security-services firm. Send comments on this article to feedback@infosecuritymag.com.

YOUR COMMERCIAL BANKING CUSTOMERS ARE AT RISK

Online Fraud is a Billion Dollar Problem

The financial services industry is faced with a significant threat to profits posed by criminals armed with an array of malicious software. Financial malware like ZeuS is stealing millions from commercial banking customers by taking over accounts and transactions.

Stop Online Fraud Before it Happens

IronKey Trusted Access for Banking provides banking clients a secure connection isolated within a tamper-proof, portable and virtualized environment – it's the only available solution that allows institutions to meet NACHA and FBI guidelines for safe online banking.

Find out more about IronKey Trusted Access: www.ironkey.com/TA

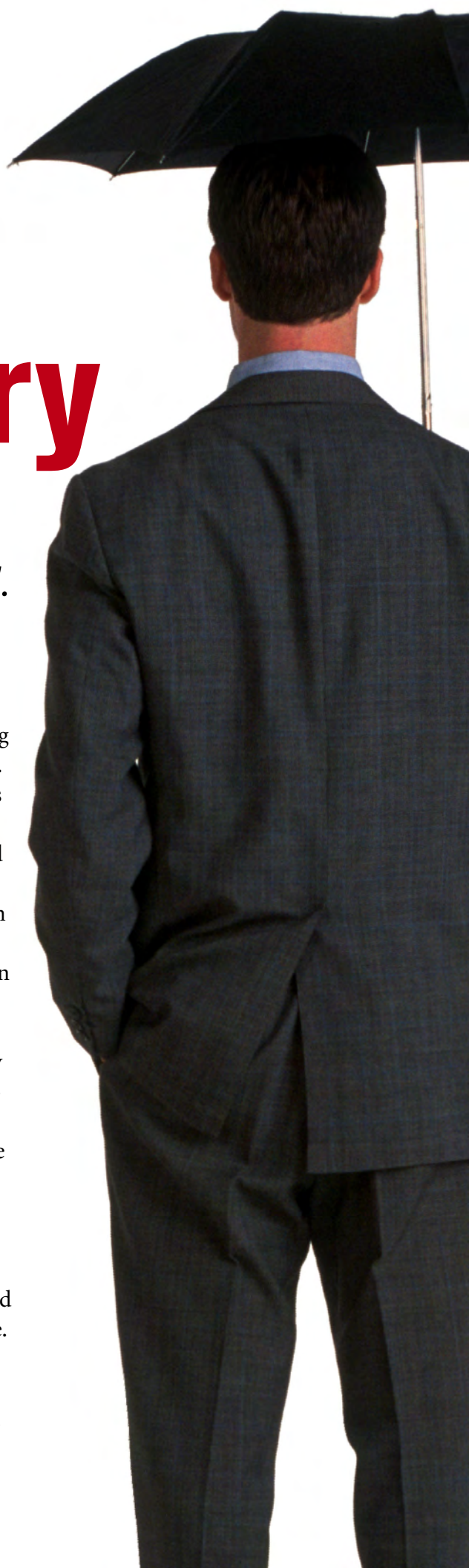
IRONKEY™

IronKey Headquarters
600 W. California Avenue
Sunnyvale, CA 94086 USA
sales@ironkey.com | 866.645.9847

Safe Recovery

Security must be included in disaster recovery planning to ensure sensitive data is protected.

BY MARCIA SAVAGE



IN A DISASTER, all focus is—naturally—on getting critical business processes back up and running. Whether the disaster is natural or manmade, it's all about recovering business operations as fast as possible, getting employees back to work, and avoiding costly downtime.

In this scenario, information security is often far down on the list of considerations, experts say. But companies that overlook data protection provisions in their disaster recovery/business continuity plans risk winding up with a double whammy: a security breach on top of a recovery situation. Imagine having to issue breach notification letters in the midst of recovering from a hurricane or other disaster. After all, compliance requirements aren't lifted in an emergency.

"You need to get folks access to the data if they need it, but you also need to prevent unauthorized access," says Ed Moyle, a manager with CTG's information security solutions practice and a founding partner of consultancy SecurityCurve. "That's where a lot of organizations fall down."

Disaster recovery/business continuity plans must ensure that an organization's information security policies are maintained in a recovery

situation, security practitioners and others say. That means making sure the recovery site has proper security, including updated antivirus and firewall protection. It also means conducting proper due diligence of any disaster recovery provider and taking proper precautions in a shared recovery facility. Transmission of data for backup purposes must also be secured.

"What you're doing to secure a disaster recovery site has to be every bit as good as what you're doing in your primary site," says Brian Engle, director of information security at Temple-Inland, a manufacturing firm based in Austin, Texas. "If you end up in a disaster recovery situation, it could be long term, maybe six months…Can you be comfortable with the decisions you make in choosing the facilities and the protections for that length of time?"

SECURITY LEFT OUT

Organizations often don't think about how the security controls they have during routine operation might fare in the event of downtime, Moyle says.

"For example, if you have a security program built around the idea of keeping physical access to things like servers locked down, you may not be able to enforce that to the same degree in an emergency scenario as you could during normal business," he says. "You want to make sure security controls continue to function during a downtime scenario."

Some companies assign disaster recovery planning responsibilities to their security groups, but others focus on databases, servers and networks rather than security reviews in their planning, says William Hughes, director, consulting services BC/DR Center of Excellence at SunGard Availability Services. "They're not as involved as they should be," he says of security teams.

> "Security teams have insights into how data is protected and how access works. They need to be included."
>
> –RANDALL GAMBY, enterprise security architect for a Fortune 500 insurance and finance company

Organizations typically consider disaster recovery a business problem and often leave security out because they view security as an IT function that puts up barriers to business, says Randall Gamby, an enterprise security architect for a Fortune 500 insurance and finance company.

"Security teams have insights into how data is protected and how access works," he says. "They need to be included."

Security technologies are often considered overhead infrastructure, but if left out of disaster recovery/business continuity planning, could mean users can't access the business resources they need in a recovery situation, he says. For instance, if the organization uses single sign-on in its routine business operations but SSO isn't supported in the disaster recovery plan, then users may not be given proper log-in prompts or be able to access certain back-end applications.

Some companies, however, make security a priority in their disaster recovery planning. An information security officer at a financial institution, who requests anonymity, says his organization is in a highly regulated industry and cannot afford to overlook data security.

"Purely from the standpoint of being compliant with the regulatory bodies, it [security] has to be at the top of the list when we look at disaster recovery," he says.

COMPLIANCE CONSIDERATIONS

Indeed, companies—particularly those in highly regulated industries such as financial and health care—need to be aware that data security mandates aren't waived in a disaster.

"We have tremendous compliance requirements from a variety of regulators," says the financial information security officer. "The requirements for information security don't make a distinction between whether you're in a disaster recovery mode or not."

In fact, the HIPAA Security Rule specifically calls out the need for maintaining security in an outage situation, Moyle notes. Section 164.308(a)(7)(ii)(C) requires the implementation, as needed, of procedures to enable continuation of processes for "protection of the security of electronic protected health information while operating in emergency mode."

One disaster scenario to consider is the possibility of guard staff reductions and loss of monitoring capability to prevent theft, Moyle says. If servers or laptops are stolen with regulated data on them, a company would still have to meet breach disclosure requirements.

"You could incur regulatory penalties over and above what it costs you from a downtime standpoint," he says.

Organizations don't tend to get audited during a recovery operation but they need to be prepared down the road, SunGard's Hughes says. "Now I'm getting an audit six months later. How do I reconstruct the chain of custody for the data and how it was protected in the time frame, if the auditor wants that?" he asks.

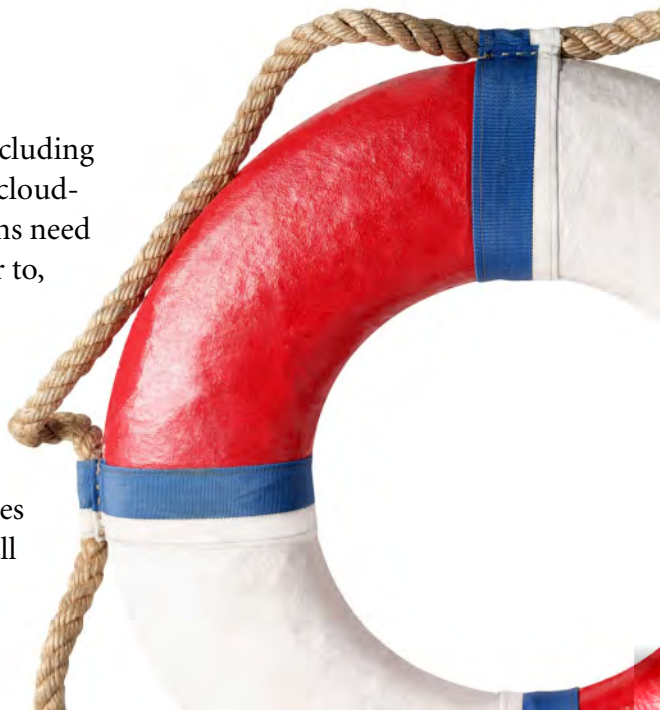
Temple-Inland's Engle says he can't imagine a company that has PCI Data Security Standard compliance requirements deciding to operate for two months without protecting cardholder data after an outage. "You will get driven out of business if you go for an extended amount of time without all the same protections you had originally," he says.

> "We have tremendous compliance requirements from a variety of regulators. The requirements for information security don't make a distinction between whether you're in a disaster recovery mode or not."
>
> –An information security officer at a financial institution

RECOVERY SECURITY

There are a variety of disaster recovery methods including hot sites, cold sites, managed service provider and cloud-based services. No matter the method, organizations need to ensure the security of the site they're failing over to, experts say.

"You're trying to replicate normal operations at a backup site… Make sure you have all the security in place when you get there," says Beau Woods, solutions architect for security and risk consulting services at Atlanta-based security services firm SecureWorks. That means making sure firewall



Get recognized—our members do.

In a sea of IT professionals, ISACA members get noticed.

Many IT and information systems professionals worldwide consider membership in ISACA® essential to their career advancement. As a nonprofit, global association, ISACA connects exceptional people with exceptional knowledge to provide members with a robust offering of professional resources.

ISACA®

Trust in, and value from, information systems

www.isaca.org/benefits-infosecmagazine

protection, intrusion detection and antivirus are in place and updated, and if a company has a security operations center, making sure there's a place for those employees to sit, he says.

"You need to make sure that when people arrive to activate the site, that the controls in place are at least as strong as the controls that would be operating in a normal scenario," Moyle says. "The policy doesn't change in an emergency."

Gamby says companies often take it for granted that users have access to systems and forget about the access management layer—such as virtual directory services, federated technologies, and containment zones—that must be in place at the recovery site in order for business to continue.

"A lot of controls around data protection are based on a user's profile and that profile may get down to identifying the particular IP or MAC address for the system he or she uses," he says. "At a remote facility, you need to make sure those profiles are put in for those individuals so they can access the data from their desktops."

Organizations also need to consider encrypting the shared communication lines used for data transmission when switching over to a recovery site, Gamby says. After an incident, companies typically switch from their dedicated lines to a service provider's shared pipe to reroute traffic to the backup site. While the shared links won't mean cross contamination of data, someone managing the switching environment could look at the traffic crossing the lines, he says.

For BioWare, an electronic game developer, uptime and availability are critical—as is data security, says Craig Miller, senior team leader of infrastructure. The company uses a virtual tape library for disaster recovery; the digitally replicated tapes are sent over an encrypted VPN tunnel to another site. Every couple months, physical backup tapes are encrypted and sent to Iron Mountain.

"Being in game development, all we have is our data…If the assets aren't available or recoverable, we don't have anything," Miller says.

BioWare uses two storage arrays from Compellent and plans next year to move one array offsite and double the disk size at each site for full cross replication; if one array goes down, the other could be active in seconds, he says.

"Being in game development, all we have is our data…If the assets aren't available or recoverable, we don't have anything."

–CRAIG MILLER,
senior team leader of infrastructure, BioWare

VENDOR MANAGEMENT

If contracting with a fixed-site disaster recovery provider, managed service provider, or cloud-based service, companies need to vet them as they would any third party, says Rachel Dines, an analyst at Forrester Research.

"You need to know where they are storing the data, what are their encryption, access control and authentication policies, and whether they can provide documentation for all that," she says.

Organizations usually will ask vendors if they use encryption but neglect to ask important questions about the type of encryption, where the keys are stored and who has access to the keys, Dines says, adding, "Vendors shouldn't have access to your encryption keys."

Third-party recovery sites raise the issue of multi-tenancy, which bring additional security

Missing Backup Tapes

A sample of breach reports involving backup tapes over the past two years.

October 2010

San Diego Regional Center, which serves people with developmental disabilities, notified some clients that a backup tape created for the purpose of disaster recovery testing was lost by UPS in shipping, according to a breach noticed obtained by PHIprivacy.net. The tape contained some current and former customers' names, Social Security numbers, addresses and medical diagnostic information.

September 2010

Pediatric and Adult Allergy, P.C., in Iowa reported losing a backup tape with patient personal information in July. Information on the backup tape included names, Social Security numbers and health plan data. The loss affected 19,222 individuals, according to the U.S. Department of Health and Human Services.

June 2010

Insurance broker Marsh and Mercer reported the loss of a backup tape that was being transported by a third-party courier, according to records obtained by DataBreaches.net. The tape contained employee benefits information; the data was maintained by Marsh's Association business, which operates through Seabury & Smith and Mercer Health & Benefits. The number of records exposed totaled 378,000, according to Privacy Rights Clearinghouse.

February & April 2008

Third-party couriers lose unencrypted backup storage tapes belonging to the Bank of New York Mellon in two separate incidents. The lost tapes potentially exposed the data of approximately 4.5 million people.

January 2008

GE Money, the firm hired by JC Penney to run its credit card operations, said it lost a backup tape containing the personal information of about 650,000 shoppers of JC Penney and other merchants. The tape was discovered missing in October 2007 by a worker at Iron Mountain.

–MARCIA SAVAGE

concerns, Dines says. "I'm not sure if people think through all the full implications of that—there are other companies' employees walking around there if they declare [an emergency] at the same time. You need to make sure the access controls to your infrastructure and data is strictly controlled."

SunGard's Hughes says customers in a shared recovery site need to step up their vigilance but acknowledged that can be a challenge. "That's tough in a recovery because that's not your first focus," he says. "The first is to get out of the situation you're in."

Cloud-based disaster recovery is relatively new but comes with a set of security concerns that organizations need to pay attention to, says George Ferguson, product marketing manager of security, compliance and continuity services at HP. The cloud-based option offers flexibility, cost savings and the ability to reduce recovery times, but companies need to step back and evaluate the cloud vendor's security controls, he says.

Ferguson cites the Cloud Security Alliance's guidance regarding the 13 critical areas of focus for cloud computing. Among the 13 areas is business continuity and disaster recovery, and the CSA recommends inspecting a cloud provider's recovery and continuity plans.

BACKUP DATA TRANSMISSION

Disaster recovery has traditionally relied on tape-based backup to off-site storage, but the transfer of those tapes doesn't always go as smoothly as organizations expect. In recent years, there have been numerous reports of backup tapes missing in transit, resulting in breach disclosures *(see above)*.

Backup tapes are at risk in transit, but unlike BioWare, many companies still fail to secure them with encryption, experts say.

"We've come a long way in starting to secure devices like laptops, CDs and thumb drives, but when you look at the backup tape generated on a daily basis in a lot of organizations across the world…rarely is someone encrypting that," says Moyle.

SunGard's Hughes says companies tend to focus on the process of maintaining backup tapes and having a third party transfer them rather than securing them. He's seen a shift away from tape backups, not necessarily for security reasons but because of concerns with recovery times. At the same time, the cost of replication is going down, he said.

HP's Ferguson says the security risks of lost or stolen backup tapes—along with the need to improve recovery times—has driven a move toward electronic vaulting services, also called cloud-based backup and replication, as a means of avoiding the physical transfer of tapes.

Overall, cloud computing has the potential to ease disaster recovery and business continuity by making it easier for organizations to have a mobile workforce, says Dean Ocampo, solutions strategy director at security supplier SafeNet.

"The benefit of moving to a cloud infrastructure is that you can access it from anywhere," he

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
DATA ACT
DISASTER RECOVERY
VENDOR MANAGEMENT
SPONSOR RESOURCES

Common Mistakes

Companies err in throwing disaster recovery planning onto IT and forgetting to test.

LEAVING SECURITY OUT is one of the mistakes organizations can make in disaster recovery/business continuity planning, but experts cite a couple other common mistakes: Leaving the planning to IT and not doing enough testing.

Companies often throw disaster recovery onto the IT team without prioritizing what business functions are the most critical to recover and setting recovery deadlines, says Beau Woods, solutions architect for security and risk consulting services at Atlanta-based security services firm SecureWorks.

"IT has to make decisions on its own and it ends up not being in line with the business," he says. "You need to have a cross-functional group make those high-level decisions before going down the road of how you'll recover from a disaster and continue business."

Another frequent mistake organizations make is not conducting enough test of their recovery plans, Woods says: "You need to make sure the way you've designed it is the way it operates in real life, both on the technology and people/process side."

William Hughes, director, consulting services BC/DR Center of Excellence at SunGard Availability Services, also says testing is critical.

"People tend to build a solution and think that's the end state, but that's really just the beginning," he says. "The end state is about four tests later, after you work through the bugs."

–MARCIA SAVAGE

says. However, companies are reluctant to move their IT processes to the cloud until protections such as encryption and authentication are in place, he adds.

BUILT-IN SECURITY

Designing a disaster recovery site has to be similar to anything else—with security built in, says Temple-Inland's Engle.

For example, companies need to identify ahead of time potential areas where security controls constrain application functions or implementations and plan accordingly. If you know you had difficulties installing something in your primary environment then you should anticipate that it will be even more problematic in a recovery scenario. An organization doesn't want to find itself in a situation where it's trying to recover an application and has to shut down security controls to make it work, and then is unable to turn them back on, he says

"If you develop a disaster recovery plan and try to secure it on the back end, it's not going to work," he says.

"If you develop a disaster recovery plan and try to secure it on the back end, it's not going to work."

–BRIAN ENGLE, Temple-Inland

The information security officer at the financial institution agrees that security must be integrated from the beginning.

"Our attitude is that we don't bolt on security—it's baked in across the board, not just for day-to-day operations but for that disaster recovery situation, which is potentially a day-to-day operation," he says.

Marcia Savage is editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

Start Your Adventure and Save!

Secure your place at RSA® Conference 2011, and stay one step ahead of the challenges that face the information security industry.

- **Expand your knowledge** with 200+ key industry-focused sessions, including network security, identity management, cloud computing, Web 2.0 security and more
- **Learn how new regulations** and constantly evolving compliance rules affect both the industry and your job
- **Demo the best technologies** and discover what's new and upcoming from over 350 exhibiting security companies
- **Benefit from a variety of opportunities** to network with thousands of peers, industry leaders and security luminaries

the adventures of alice & bob

SAVE $400

Register by January 14 to secure your discount!

Follow the Adventures of Alice & Bob at
www.rsaconference.com/aliceandbob2011

RSA® CONFERENCE 2011

20 YEARS

FEBRUARY 14-18 | MOSCONE CENTER | SAN FRANCISCO

www.rsaconference.com/techtarg

5 ways security can influence VENDOR MANAGEMENT

BY ERIC HOLMQUIST

EVERY BUSINESS TODAY depends to some extent on third parties—it's a reality that's becoming even more pronounced as companies move to more cloud-based services. And in order to effectively provide a product or service, a certain percentage of those third parties will require access to confidential corporate and/or customer information. Obviously, it is incumbent on management to ensure that not only is the third party capable, but also in the course of its operations can ensure that the data entrusted to it remains secure. Traditional vendor management programs have tended to focus to a

THE CISO HAS A KEY ROLE IN REDUCING THE RISK OF SHARING SENSITIVE CORPORATE DATA WITH THIRD PARTIES.

large degree on "ability to deliver" with data security being an almost secondary consideration. What managers often fail to fully appreciate, especially for large or very visible companies, is that while a third party's failure to deliver would in all likelihood be operationally disruptive, a massive data breach could be devastating.

The challenge for companies is how to ensure protection when they often have little ability to monitor day-to-day operations, evaluate the third party's strength of internal controls or have meaningful input into the third party's risk management systems. While we often talk in terms of keeping the data "secure," the grim reality is that, simply because people need to use it, the data is not secure. Adding an external entity into the equation just makes it that much less secure.

The challenge for companies is how to ensure protection when they often have little ability to monitor day-to-day operations, evaluate the third party's strength of internal controls or have meaningful input into the third party's risk management systems.

Companies tend to approach vendor management in many different ways. Some split contract and vendor management between the legal department and other operating units, respectively. Some have large procurement groups that cover all aspects. Still others may use a decentralized model, distributing different pieces throughout the company. Regardless of which model is used (each having its own merits and drawbacks), the governance aspects related to data security really don't change. We'll explore five key risk management principles relative to information security within vendor management, and describe some basic strategies for reducing the risk associated with sharing confidential information. The CISO plays a key role by ensuring that the critical governance elements for data sharing with third parties are in place.

#1 *ownership*

The first and possibly most critical governance aspect is ownership. Regardless of how the contract and related due diligence is facilitated, one absolutely and irrefutably truth remains: There must be one specific person responsible for the relationship—not a department, committee, or a vendor group—a person. In all likelihood, that person will be in the business or operating unit that directly oversees the product or service that the third party provides, be that IT, a line unit, back office, etc. This person, perhaps assisted by others, is specifically and directly responsible, and accountable, for management of that third party. This includes any damages caused by a failure of that third party to adequately protect the data provided to them.

Therefore, the first responsibility of the CISO is to make certain that the company has a process in place to ensure that each third party will have an associated third party relationship manager (TPRM) who is actively involved in the process of managing the relationship. The CISO will likely

end up being consulted in the due diligence process where appropriate, but he cannot be the one responsible for managing the third party.

While assigning a TPRM is essential, we need to understand that there is a dilemma here. Even though having TPRMs assigned to all third parties is critical to good governance, there is an unfortunate conflict of interest that exists here. The fact is, assuming that the business wants to use a given third party, the TPRM is somewhat less than motivated to find problems with them. In fact, quite the opposite; they may find themselves looking for reasons to trust the third party, perhaps ignoring subtle, or not so subtle, signs that could be an indication of something suspicious. This is why accountability is so critical—if TPRMs are responsible for the misdeeds of their third party, they become significantly less incented to turn a blind eye. Therefore, it is also the CISO's role to ensure that TPRMs are taking the contract, due diligence, management and monitoring process seriously and proactively.

#2 contractual provisions

Assuming clear ownership has been established, the next area covers a set of questions and provisions that the CISO must ensure are being addressed before any contracts are signed and data exchanged.

The first and most logical question is, why? Why does the third party need this data? Is it required for them to provide their product or service? Do they need all of the data or just some of it? Is the business area just being lazy and suggesting it all be sent, rather than taking the time to create more discrete, or sanitized, sub-sets? Ultimately, the related business area must be able to clearly rationalize why the data is imperative to the third party's product or service. This is an area where the CISO may be consulted as a subject matter expert, perhaps facilitating a discussion around what options exist that could reduce the type and quantity of data provided. It is a sad fact that well meaning people often view data (even highly confidential data) as an operational necessity, like bricks to the builder, and not the highly valuable, highly sensitive, corporate asset that it is.

It is a sad fact that well meaning people often view data (even highly confidential data) as an operational necessity, like bricks to the builder, and not the highly valuable, highly sensitive, corporate asset that it is.

In terms of contractual provisions there are a number of things the CISO needs to ensure are included any time confidential data will be exchanged. These include:

- Standard confidentiality language commensurate with the degree of information shared
- A "right to audit" provision against the third party's system of internal controls
- Clear service-level agreements for notification requirements in the event of a data breach
- Financial liability for any expense associated with a data breach

In the end, however, a company needs to remember that while these provisions exist (at least in theory) to prevent an incident, the reality is that they largely exist for recourse. Real prevention will be accomplished through comprehensive due diligence, actively setting and managing expectations and effective monitoring.

#3 due diligence

All enterprises have skeletons they prefer not to disclose, so there's no reason to assume your vendors don't also have something they'd prefer to keep quiet. Consequently, the third major area that the CISO needs to be actively engaged in is the design of the overall due diligence process. The fact is that companies need to be very deliberate about how they assess and manage their third parties when it comes to data sharing.

When performing third party due diligence, how the information is gathered isn't nearly as important as what is done with that information. (As far as forms go, you can't really beat the BITS Shared Assessment templates, and many major companies have already completed these forms anyway.) Generally speaking, the information provided by a third party relative to its information security practices should be viewed just like a resume. While it is a form of attestation on the part of the third party, it is not designed to verify adequacy; it's just a tool to start the conversation. The job of the organization, with the CISO's direction and/or assistance, is to get behind all of the wonderfully crafted language and carefully constructed responses. What is the truth about how the third party stores, manages, protects and ultimately destroys the confidential data that you are, or will be, sharing? Where will it reside? Who exactly will have access? How is access granted and revoked? What are their change management practices? What technology is the third party using and does it contain known vulnerabilities? Is it current or obsolete? What independent reviews of the third party's environment are conducted and by who? What were the past results?

Generally speaking, the information provided by a third party relative to its information security practices should be viewed just like a resume.

This is not a check-off exercise—it's a gauntlet, and one that should be very difficult to navigate. If the business isn't asking really hard questions, it's not doing its job. It's the CISO's job to make sure that this process is happening, both at contract origination, and throughout the life of the contract.

Another part of the due diligence process should be a mechanism for classifying the data that will be shared. What type of information will be included? What is its level of sensitivity? How much information will be shared and how often, etc.? This provides a baseline for the business so that if the nature of the relationship changes, particularly one which requires a change to what data is shared, the company can reassess the risk based on the new data

requirements. The CISO should be able to help develop an agreed upon classification schema that can be used consistently throughout the organization.

An area that is often overlooked is data destruction. When and how will the data be destroyed? How will the third party attest to its destruction and what are the consequences if it is not destroyed? This is a difficult area to manage because, let's face it, proving that data has been completely eliminated is difficult to impossible. Nevertheless, this area must be subject to clear expectations, which the CISO needs to ensure has been documented.

Ultimately, when going through the third party due diligence process, a company should develop a risk profile for all of its third parties that includes a risk rating based on the type and amount of the data being shared. This allows the company to focus its energy and resources on those third parties that represent the most risk, and provides a baseline to reference when either the third party or the nature of the contract changes.

#4 monitoring

Monitoring and incident response are the most challenging and precarious areas of vendor management. This is simply because monitoring is difficult if not impossible, and recovery from an event is extremely tough.

Nevertheless, despite the limited ability to monitor third parties, there are some areas that the CISO should ensure are addressed. The first represents internal changes. This would typically be a change to the scope of the contract which requires a change to the type, sensitivity, quantity or frequency of the data that is being exchanged. In this case, there must be a process to revisit the risk profile based on the new data requirements, and if a material change is going to take place, then a new due diligence and risk assessment analysis needs to be completed. Otherwise you're applying old rules to a new game.

Monitoring and incident response are the most challenging and precarious areas of vendor management.

The other area obviously involves changes with the third party themselves. This would include facility moves, corporate restructuring, business acquisitions, new business lines, etc. Each of these can have an impact on the internal controls related to data protection, and it is the CISO's responsibility to ensure that systems are in place to monitor these third parties for material changes. Changes such as these should prompt, at minimum, a conversation between the TPRM and the third party to understand what impact, if any, these changes will have on the company's data usage and internal controls.

The other, and fairly intuitive, area of monitoring involves media coverage. Should the third party become subject to any degree of regulatory or other third party criticism or, worse, be the victim of some sort of data compromise, then the entire due diligence and risk assessment process must start from scratch. All prior attestations and assumptions are null and discarded.

The CISO will have to manage this area because this is where the TPRMs will often try to take

Teaching you security...one video at a time.

Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a firehose'.

The Academy Pro allows information security professionals to learn about today's most important technologies on demand and at their own pace.

Check out The Academy Pro at
www.theacademypro.com

the academy pro

Sponsored by:

www.theacademypro.com

the easy way out for fear of having to switch vendors. Often their response is "Yes, they had a breach, but they say that they have taken care of the vulnerability." O.K., prove it.

#5 incident response

Incident response is possibly the most treacherous part of vendor governance. Ideally, there will never be a scenario where data is compromised and somebody needs to clean up the mess. However, we know that it as a statistical certainty that it will happen and, when it does, the company needs to have the processes in place to respond quickly and decisively. The fact is that if you looked at every data breach since the beginning of time, they all share one common attribute—and that is that time is not on your side.

Certainly, at a minimum, every third-party contract must have a provision for notification requirement in the event of a data breach. This should be numbered in hours, if not minutes. On the heels of a data exposure, the initial hours can be critical, particularly where customer information is involved. CISOs need to ensure that both companies—their own and the third party—have a clear escalation and notification strategy so that all parties involved know exactly who needs to be notified and who will take charge in developing and implementing a resolution plan.

On the heels of a data exposure, the initial hours can be critical, particularly where customer information is involved.

These are not details that can be made up at the time of a breach—they must be clearly established, and tested, well in advance of any live event. And, again, a data incident of any kind should prompt a revisit to the third party's due diligence and risk assessment. If the incident was very minor, very localized and easily corrected, fine. But at a bare minimum, a discussion needs to take place that asks whether the potential vulnerability was previously disclosed and how it has been addressed.

NO SMALL FEAT

Experience has shown that the majority of companies collect only basic information about the third parties with which they will exchange confidential data, tend to do only cursory analysis of that information, take minimal due diligence steps, implement limited monitoring and haven't really thought through their incident response procedures in the event of a major data breach. And yet every single one knows without a shadow of a doubt that it should be doing more and is probably accepting too much risk. Simply put, this is just not acceptable.

The CISO has a substantial task to ensure that all of the systems and controls are in place to ensure third party compliance with information security policies and practices. To quote Ronald Reagan, this is definitely an exercise in "trust but verify" and it is no small task. This further reinforces why the CISO must be in a very senior role with total management access. He or she must work very closely with internal vendor management groups to provide subject matter expertise,

program design assistance and direct oversight when necessary. We all like to believe that people will always do the right thing, but this is simply not the case. There are criminals everywhere, and they can disguise themselves as hard working employees just looking for an opportunity to strike. But through strong contractual provisions, comprehensive due diligence, detailed documentation, active management, dynamic monitoring and ability to respond quickly, companies can go a long way towards managing their third-party risk.›

Eric Holmquist is president of Holmquist Advisory, LLC, which provides consulting to the financial services industry in risk management, operations, information technology, information security and business continuity planning. Send comments on this article to feedback@infosecuritymag.com.

what drives *your* approach to IT security?

Balancing business priorities and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our **ISO 17799/27002 Compliance Program** helps you to focus resources on your most important business risks and comply with regulations such as **Sarbanes-Oxley, FFIEC, HIPAA, PCI,** and **Gramm-Leach-Bliley.** Best of all, our approach works equally well for "Main Street" businesses and the Fortune 500 clients we've proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

INFORMATION SECURITY®

EDITORIAL DIRECTOR Michael S. Mimoso

EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum, Bruce Schneier, Lee Kushner, Mike Murray

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

USER ADVISORY BOARD
Edward Amoroso, AT&T
Anish Bhimani, JPMorgan Chase
Larry L. Brock, DuPont
Dave Dittrich
Ernie Hayden
Patrick Heim, Kaiser Permanente
Dan Houser, Cardinal Health
Patricia Myers, Williams-Sonoma
Ron Woerner

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS DIRECTOR Robert Westervelt

SITE EDITOR Jane Wright

ASSISTANT EDITOR Maggie Sullivan

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Greg Smith

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

VICE PRESIDENT/GROUP PUBLISHER Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT Susan Shaver

DIRECTOR OF MARKETING Nick Dowd

SALES DIRECTOR Tom Click

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER Elizabeth Lareau

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Andrew McHugh, Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Leah Paikin lpaikin@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Jeff Wakely

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

ARE YOUR NETWORK DEVICES HOLDING YOUR LOGS HOSTAGE?
WHAT YOU DON'T KNOW CAN HURT YOU.

OPTICS FOR SECURITY INFORMATION MANAGEMENT IS AN AFFORDABLE AUTOMATED LOG MANAGEMENT SERVICE THAT CENTRALIZES, ANALYZES AND RETAINS LOG DATA AND HELPS YOU USE IT TO SUPPORT BUSINESS FUNCTIONS. SCALABLE TO100% OF YOUR LOG DATA, SO YOU CAN REST EASY, GLASSHOUSE HAS GOT YOU COVERED.

FOR MORE INFORMATION CONTACT: SECURITY@GLASSHOUSE.COM

WWW.GLASSHOUSE.COM

GLASSHOUSE

CDW

See ad page 4

- Are You Getting the Best Security for Your Money
- Getting from Point A to Point DLP

ArcSight, Inc.

See ad page 7

- First Annual Cost of Cyber Crime Study: Benchmark Study of US Companies
- Universal Log Management Solution

Websense

See ad page 9

- 2010 Threat Report: The only constant is change
- Seven Criteria for Evaluating Security as-a-Service (SaaS) Solutions
- Websense Hosted Web Security Datasheet

Check Point

See ad page 12

- Check PointClamps Down on Data Loss
- Check Point IPS - Secure What's Yours

NETGEAR, Inc.

See ad page 15

- Accounting Firm Improves Security and Reclaims Employee Productivity With NETGEAR® ProSecure® UTM50
- The Role of the Internet in the Propagation of Malware

Code Green

See ad page 17

- A radically different approach to data loss protection
- We are solely focused on protecting your confidential data

Guardium

See ad page 20

- Oracle Account Security: Chapter from "HOW TO Secure and Audit Oracle 10g and 11g"
- Essential Steps to Implementing Database Security and Auditing
- IBM InfoSphere Guardium: Managing the Entire Database Security and Compliance Lifecycle

Security Innovation

See ad page 23

- Ensure you applications are in compliance. eLearning for secure application design, coding, & testing
- Out-of-the-Box Secure Coding Standards for PCI-DSS, NIST, OWASP, ISO, etc.
- High-Performance, Standards-Based Crypto - ideal for constrained devices & high-transaction volume

IronKey

See ad page 28

- Stop commercial banking account takeovers
- Manage Portable Data Security – Protect data with IronKey portable encryption solutions

ISACA

See ad page 32

RSA Conference 2011

See ad page 37

- Register early and save
- 20th anniversary

The Academy Pro

See ad page 44

- Free infosec videos for the information security community.

SystemExperts

See ad page 47

Glasshouse Technologies

See ad page 49