Best Security, Privacy, and Data Protection Articles of 2007

A collection of ITCi's most popular analysis and advice from the past year.

Series Editor: Huan Do, Esq.

www.ITCinstitute.com

ITCi
IT Compliance Institute™

Contents

Best Security, Privacy, and Data Protection Articles of 2007

www.itcinstitute.com

EDITORIAL AND RESEARCH DIRECTOR Cass Brewer
SERIES EDITOR Huan Do, Esq.
ART DIRECTOR Deirdre Hoffman
GRAPHIC DESIGNER Bill Grimmer

IT Compliance Institute
GENERAL MANAGER Geoff Bridges
DIRECTOR OF MARKETING Michelle Johnson
DIRECTOR OF EDUCATION John Rapp, Esq.

1105 MEDIA

PRESIDENT & CHIEF EXECUTIVE OFFICER Neal Vitale
CHIEF FINANCIAL OFFICER & SENIOR VICE PRESIDENT Richard Vitale
EXECUTIVE VICE PRESIDENT Michael J. Valenti
MANAGING DIRECTOR Dick Blouin

VICE PRESIDENT, FINANCIAL PLANNING & ANALYSIS
William H. Burgin
VICE PRESIDENT, FINANCE & ADMINISTRATION
Christopher M. Coates
VICE PRESIDENT, AUDIENCE MARKETING & WEB OPERATIONS
Abraham M. Langer
VICE PRESIDENT, INFORMATION TECHNOLOGY Erik A. Lindgren
VICE PRESIDENT, PRINT & ONLINE PRODUCTION Mary Ann Paniccia

CHAIRMAN OF THE BOARD Jeffrey S. Klein

REACHING THE STAFF

Staff may be reached via e-mail, telephone, fax, or mail.

E-mail: To e-mail any member of the staff, please use the following form: FirstinitialLastname@1105media.com.

Renton office (weekdays 8:30 a.m. to 5:00 p.m. PT)
Telephone: 425.226.9126; Fax 425.687.2842
1201 Monster Road SW, Suite 250, Renton, WA 98057

Corporate office (weekdays, 8:30 a.m. – 5:30 p.m. PT)
Telephone 818.834.1520; Fax 818.734.1528
9121 Oakdale Avenue, Suite 101, Chatsworth, CA 91311

ADVERTISING SALES Lesley Schwartz
lschwartz@1105media.com, 425.277.9196

List Rentals: 1105 Media, Inc., offers numerous e-mail, postal, and telemarketing lists targeting business intelligence and data warehousing professionals, as well as other high-tech markets. For more information, please contact our list manager, Merit Direct at 914.368.1000 or www.meritdirect.com.

ITCi
IT Compliance Institute™

OUR MISSION

The IT Compliance Institute (ITCi) strives to be a global authority on the role of IT management in corporate compliance, risk management, and governance. ITCi helps organizations navigate today's complex regulatory environment, turning compliance responses into capital opportunities.

Providing extensive research, news, tools, and education for the IT compliance community, ITCi is a useful and trusted resource for compliance professionals. We are one of the few independent compliance analysts who provide a cross-industry, cross-regulatory, and global perspective on topics ranging from anti-fraud controls to technical security, privacy, records management, compliance unification, technology frameworks, and effective IT auditing. To serve our diverse member community, ITCi covers these topics through an array of publications and programs, including a worldwide membership program, publications, compliance reference databases, live and online educational events, the Compliance Convergence Initiative, and more.

OUR MEMBERS

ITCi supports a diverse member community composed of CIOs, CTOs, IT leaders, auditors, risk management and business executives, consultants, and compliance specialists from around the globe. Our members gain unrestricted access to most ITCi resources, as well as discounts on ITCi-hosted events and interactive tools.

LEGAL DISCLAIMER

When assessing any legal matter, do not rely solely on materials published by third parties, including the content in this publication, without additionally seeking legal counsel familiar with your situation and requirements. The information contained in the **Best of ITCi Series** is provided for informational and educational purposes and does not constitute legal or other professional advice. Furthermore, any applicability of any legal principles discussed in this paper will depend on factors specific to your company, situation, and location. Consult your corporate legal staff or other appropriate professionals for specific questions or concerns related to your corporate governance and compliance obligations.

ITCi makes every effort to ensure the correctness of the information we provide, to continually update our publications, and to emend errors and outdated facts as they come to our attention. We cannot, however, guarantee the accuracy of the content in this publication, since laws change rapidly and applicability varies by reader.

The information in this publication is provided on an "as is" basis without warranties of any kind, either expressed or implied. The ITCi disclaims any and all liability that could arise directly or indirectly from the reference, use, or application of information contained in this publication. ITCi disclaims any liability, whether based in contract, tort, strict liability, or otherwise, for any direct, indirect, incidental, consequential, punitive, or special damages arising out of or in any way connected with access to or use of the information in this publication.

ITCi does not undertake continuous reviews of the Web sites and other resources referenced in this publication. We are not responsible for the content published by other organizations. Such references are for your convenience only.

Access Control: 10 Best Practices

Properly implemented, access controls only give employees access to the applications and databases they need to do their jobs. At many regulated organizations, such controls are too often manual, outdated, and largely ineffective. Here's how to overhaul your access control program.

By Mathew Schwartz

Published online March 27, 2007

What is the importance of automated IT access controls in regulated environments?

Consider the case of DuPont: Between August and December 2005, a research scientist about to leave for a new company admitted he downloaded more than 22,000 sensitive abstracts from DuPont's electronic data library. He was also able to access an additional 16,700 files, most of which didn't relate to his job function. This access was 15 times greater than the next library user, and reportedly involved $400 million in trade secrets, yet DuPont didn't discover the inappropriate access until December 2005, after the employee gave notice. Furthermore, he had already uploaded some of the documents to his new work laptop in February 2006 before federal authorities finally caught up with him.

When it comes to insiders abusing their access rights, DuPont isn't alone. According to a Forrester survey of 28 companies who experienced a data breach in 2005, the leading cause—contributing to 39 percent of all incidents—was "authorized users exploiting their privileged access rights."

The moral is that just restricting access isn't enough to stop a malicious insider from misbehaving. With that in mind, how can companies better administer user accounts, control access, and watch for signs of inappropriate access behavior?

Start with these 10 best practices:

1. Create an Access Baseline

Begin by having your IT department record and generate a baseline of current access levels and controls in place. By doing this, "you'll see the holes in your current processes" and quickly nab any gross offenders, such as "someone who's running a business out of their cube," says Ellen Libenson, vice president of product management at Symark Software. "Then you just go through people's roles in the company, and based on need-to-

know access, you define who really does need to have access" to specific functionality.

2. Automate User Provisioning

Organizations must watch for signs of inappropriate access activity. Yet according to a new survey of 600 organizations' identity and access management practices conducted by the Ponemon Institute, 58 percent of companies use "mostly manual monitoring and testing" to monitor access policy compliance; cue the DuPont breach. Indeed, using manual processes makes detecting unusual behavior difficult.

Look to user provisioning software—defined by Forrester Research analyst Jonathan Penn as "the administration and audit of users' accounts and privileges"—to help. User provisioning has six components, he says: a framework for managing access control policies, usually by role; interconnections with IT systems; workflows to guide sign-offs; delegated administration; password management; and auditing. By automating these processes, organizations ensure employees only get access to the information they need to do their jobs. If their job role changes, so will their access levels.

3. Find the Business Case

Experts says most access control programs today are driven by regulatory compliance concerns, but companies should also identify a business case, to ensure they get the most from their investment. For example, automating account provisioning, de-provisioning, and password management means companies require fewer IT people to handle account administration, and will also save in help desk costs.

Access controls can also boost overall employee productivity. "Compliance requires you restrict access to information only to the people who are authorized to read it, but by doing so, and restricting it appropriately, you actually get the right information to the right people more quickly," notes Sumner Blount, director of solutions marketing at CA.

4. Tie Access Controls to Your Environment

The precise access controls that your company needs depends on your IT environment, and the regulations you face. "Is an eight-character password always better than a six-character password and worse than 10 characters? Is strong two-factor authentication—often defined as a best practice—required to log into the lunch cafeteria menu Web site?" asks Forrester Michael Rasmussen. "Ultimately, a best practice in your control environment is what works best for you."

When determining which access controls to enforce, check your applicable regulations. "For Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley, the control is being able to audit, review, and declare who has access to what," says Rajiv Gupta, CEO of Securent. Meanwhile, HIPAA mandates need-to-know access to people's personal health information, and the Payment Card Industry Data Security Standard restricts access to people's personal financial information. Basel II, Canada's Personal Information Protection and Electronic Documents Act, and the EU Data Directive, among others, also mandate access restrictions. Finally, states' data disclosure laws take a different tack: companies who suspect people's personal data has been inappropriately accessed must notify every affected state resident.

5. Segregate Access Using Roles

SOX, among other regulations, demands segregation of duties: developers shouldn't have direct access to the production systems touching corporate financial data, and someone who can approve a transaction shouldn't be allowed to given access to the accounts payable application. Most companies approach this problem by continually refining role-based access controls. For example, perhaps the "sales executive" role can approve transactions but never access the accounts payable application; no one can access the developer environment except developers and their direct managers; and only application managers can touch production systems.

6. Apply the Doctrine of Least Access

No matter the regulation, auditors increasingly want to see the doctrine of "least privilege" applied. Namely, "if

you don't need to work with it, you shouldn't have access to it," says Libenson. This is a good starting point for setting access controls.

Another good starting point: immediately restricting access for IT personnel , and especially for the employees who administer the access controls, since they typically have the necessary access levels and knowledge to do maximum damage should they turn into a malicious insider. Furthermore, many IT staff already take a questionable approach to data privacy. According to one poll of almost 650 IT professionals conducted last year, 10 percent admit to regularly abusing their security privileges and inappropriately accessing corporate data.

7. Channel Big Brother

As the revelation of inappropriate access by IT employees suggests, employees are more apt to test access restrictions if no one is watching. Hence companies should audit all access, and remind employees their access is being watched. "If people know their activity is being tracked, they're less likely to do something," says Libenson.

8. Terminate Orphaned Accounts with Extreme Prejudice

Do your former employees' access rights expire when they give notice, or last step out of the building? Given the threat posed by disgruntled ex-employees, immediately suspending their access should be a no-brainer. Yet the de-provisioning process at many companies is still manual. "The typical complaint we hear is, we have over 10,000 employees, and one employee could, over the course of their career, have been given access to 10 servers and 20 applications, and we have to go to each server and pull them out of each access control list," says Libenson.

Until those credentials get pulled from the access list, the former employee still has insider access levels, and thus poses a security risk. "It's not a case of having to create a back door to get access," she says. "We hear of people's e-mail working for a year after they've been terminated." In short, companies in regulated environments must implement automated user provisioning, which notably includes automated de-provisioning.

9. Proactively Monitor for Unusual Activity

While an effective security program includes passwords or possibly two-factor authentication, passwords and key fobs can also be lost, stolen, or access rights abused. That's why experts recommend companies monitor access patterns to watch for unusual activity, such as a large spike in a user's access to an electronic library containing sensitive information.

According to Ponemon Institute, only 14 percent of organizations today "are proactive and use preventive approaches" to manage access. Yet unusual access patterns—based on the time of day, week, or job role—can be one of the best signs a malicious insider is at work, or an outside attacker managed to steal someone's access credentials.

10. Control Remote Access, plus Applications and Databases

Apply access controls and auditing to all remote access too. Indeed, as an organization's perimeter expands, it must also define fine-grained roles for consultants, business partners, and supply chain members, to quickly give them appropriate access. Access levels for applications and databases need to be controlled, starting with anything that touches a Web application, since these are highly vulnerable to attack.

Today, applying such controls can require manual integrations or ad hoc security add-ons. In the future, however, organizations will increasingly be able to "externalize the access control from the applications themselves," says Gupta, thanks to XACML (OASIS eXtensible Access Control Markup Language), which he dubs "the de facto standard for entitlements." While XACML-compatible applications are not yet widespread, he says XACML will eventually make access control easier to extend across applications, between business partners, and via Web services. ■

Mathew Schwartz is a contributing editor for the IT Compliance Institute. You can contact him about this and other articles at Mat@PenandCamera.com.

Beyond SOX and Endpoint Security: Six Emerging Trends in Compliance

Spending on SOX, Vista apathy, and endpoint security dominated our 2006 predictions for compliance. Learn how the landscape is shifting for 2007.

By Mathew Schwartz

Published online March 20, 2007

Last year, Sarbanes-Oxley (SOX) dominated companies' compliance efforts, organizations increasingly adopted endpoint security, data breaches grew epidemic, and experts warned companies Microsoft's operating system Vista would be no silver bullet for compliance or security efforts.

Here's what's changed from 2006, and what experts predict for the coming year:

1. Targeted Attacks Escape Detection

For some time, attackers have been using malware to exploit PCs, turn them into zombie computers, and create large, distributed bot networks, especially for distributing spam and malware. Phishing attacks have also become so prevalent and sophisticated that some financial institutions report their losses related to online fraud increased five-fold from 2005 to 2006.

Increasingly, however, attackers are launching more targeted, stealthy attacks aimed at stealing people's lucrative personal information. The emerging, frightening truth is that the scarcity of targeted attacks means the intrusions often go undetected by security researchers or vendors. The result is companies are left wide open to attack, which of course is the attackers' ultimate goal. "More bad guys are learning, let's not be overly greedy, it's easy to do this and get away with it if we don't try to do too much at once. If we just do it slow and steady, we'll make off with a lot more and have a better chance of getting away with it," notes Michael Gavin, security strategist at Security Innovation.

2. Breached Data: 100 Million Records and Counting

Driven by such targeted attacks, data breaches have reached epic proportions over the past few years. Indeed, the Privacy Rights Clearinghouse now estimates, since it started tracking data breach disclosures in February 2005, that the total number of potentially breached records surpassed 100 million by the end of 2006. Perhaps the most high-profile recent example is the TJX Companies' disclosure that its network was hacked

sometime in 2003, and the attack was not discovered until 2006.

Such a disclosure, of course, is only the result of laws on the books in over 30 states—inaugurated by California SB 1386 in 2002—requiring any organization to disclose a data breach which affects their residents. Meanwhile, efforts to pass a national data breach and consumer protection law of at least equal strength to the states' laws has so far failed.

Even so, current data breach repercussions can be extensive. Due to clean-up efforts, consumer notification services, legal fees, and customer defections, a single breach can result in millions of dollars of direct costs and lost revenue for an organization. As a result, companies are increasingly doing everything possible to safeguard all sensitive consumer or employee data, to avoid ever having to make the reputation crushing data breach notification.

3. Revisiting Compliance Controls

The first several years of SOX involved a mad dash to get needed IT controls in place to ensure compliance. Firms typically first instituted manual controls, and have been steadily replacing those controls with automated ones, to create more easily repeatable, demonstrable, and cost-effective compliance.

Unfortunately, many of these controls are actually ineffective, claims Forrester Research analyst Michael Rasmussen in a recent report. The problem: "In a rush to avoid being fitted for orange jumpsuits, firms don't devote nearly enough consideration to the adequacy of the controls that compliance teams are implementing." Rather, many companies rely on one-size-fits-all checklists of controls—"because firms all want a 'get out of jail free' card that assures their executives that if they do these three things in order, litigators and regulators will leave their companies alone."

As a result, he says, "many compliance teams have implemented controls that may not make sense for their businesses." Thus controls are either overblown, which siphons off valuable IT time and resources; or more often insufficient, which leaves organizations vulnerable to attack, as well as potentially noncompliant with regulations. Hence as regulations mature, expect auditors to take a much closer look at whether in-place controls actually do the job.

4. Better Compliance through Improved Security

On that note, experts have long argued that compliance efforts don't automatically result in improved security. Many companies, however, didn't seem to listen. According to new research by Forrester Research analyst Khalid Kark, "most organizations increased their regulatory spending while decreasing their security budgets and postponing security initiatives, thinking that regulatory compliance would lead to better security." Yet "in a lot of cases," he says, "this assumption was not true." Furthermore by forsaking sufficient information security investments, many firms are now at increased risk from today's more virulent and targeted attacks.

Expect firms to now play catch-up. Forrester predicts security spending in North America—as a percentage of the overall IT budget—will increase by 7.5 percent in 2007, after declining from 8.5 percent of the IT budget in 2004, to 6.9 percent in 2006.

5. PCI Overshadows SOX

Increased security spending will also be needed to comply with the Payment Card Industry Data Security Standard (PCI DSS) version 1.1, which was released in September 2006. The PCI DSS is a security standard that was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help mitigate emerging payment security risks, while facilitating the broad adoption of payment account data security. Simply put, PCI specifies minimum policies, procedures, data security, network architecture, and more for any merchant handling credit card data.

Unlike SOX, which many deride as being so vague that many auditors aren't even sure what it requires, experts say PCI is a model of clarity, clearly spelling out what companies must do. For example, "PCI really addresses all the system components that are involved in the network, whether a firewall, router, or anything connected to the network. Anything that comes in contact with cardholder data has to be secured," notes Ellen Libenson, vice president of product management at Symark Software.

Noncompliance with PCI can lead to fines and a revocation of credit card processing capabilities, which can have substantial business repercussions. Visa has established monetary rewards for compliance. Visa's PCI Compliance Acceleration Program (CAP), announced December 12, 2006, promises banks financial rewards and lower processing fees if they can ensure merchant compliance with major PCI requirements. In addition to cash incentives, the program offers lower interchange rates, transaction processing fees that banks pay for credit card transactions. Visa expects banks to pass these incentives on to merchants. Other card companies are expected to follow the path set by Visa. As a result, many companies are now making a concerted push to become PCI-compliant.

"PCI to me has become the new SOX," says Chris Farrow, director for Configuresoft's Center for Policy and Compliance. "SOX has really toned down in terms of its appearance in the media and priority for a lot of organizations. After the first Enron, WorldCom, and Tyco guys, how many people have gone to jail? Not many. It doesn't have the teeth it used to. Lobbyists continue to push to get SOX toned down. Small businesses keep getting extension after extension, and people are complaining SOX costs too much money to comply."

6. Insider Threat Drives Access Controls

So what do Medco, DuPont, and Compulinx have in common? All suffered security breaches due to insiders. At Medco, for example, an IT administrator attempted to launch a logic bomb to delete internal information; it failed. Meanwhile at Compulinx, the CEO reportedly—and fraudulently—used employees' personal information for credit purposes.

Of course insider breaches are not new, with some studies estimating insiders account for up to 85 percent of all security breaches. The threat is straightforward and typically pervasive: the average employee has access to too much information. Indeed, employees rarely lose access to databases, servers, or applications, and often just acquire more as new systems appear, and their job responsibilities evolve.

To comply with regulations, and especially laws which mandate need-to-know access to sensitive information—including HIPAA, SOX, and PCI—companies now have a clear mandate, says Forrester's Kark: "CISOs must be able to identify the sensitive information and ensure that it has the appropriate amount of protection to prevent against data disclosure and security breaches." Expect companies to expend significant energy this year trying to learn where their sensitive data lives, so they can restrict and audit access accordingly. ■

Mathew Schwartz is a contributing editor for the IT Compliance Institute. You can contact him about this and other articles at Mat@PenandCamera.com.

Top 10 Employee Security Gaps to Plug Right Now

If it seems that companies aren't learning anything from the front-page security mistakes of competitors, take heart: Consultants and security experts are. Based on their experience and observations, here are 10 security gaps the experts have observed over and over, along with advice for addressing them.

By Linda L. Briggs

Published online October 16, 2007

If there's good news about the often-abysmal state of information security at most companies, perhaps it's this: We're all making the same mistakes, and we're making them over and over again. "When I go into an organization, I don't care what size or type… I will generally find [the same] five general overall problems" with employees and security, according to Chris Apgar, a CISSP and president of Apgar and Associates, a compliance and information privacy consulting firm that focuses on the health care and financial sectors. Those five areas: Training, policies and procedures, disaster recovery and business continuity planning, audits, and risk analysis.

Here are suggestions from Apgar and two other security experts on addressing some of the most common employee security problems they see.

1. Review policies and procedures

It sounds basic, but when it comes to security policies and procedures, Apgar is brutally blunt in summing up what he sees out there: "They are generally incomplete, inaccurate, not enforceable, and not reviewed periodically." Good policies and procedures go hand-in-hand with training, since one depends on the other. In general, security policies and procedures should be looked at yearly—more often if a significant change occurs in the company.

The reverse is also true: some companies are handling security exactly as they should be, but the procedures themselves aren't well-documented. Poor or missing written procedures can be a red flag for external auditors of all stripes, Apgar points out. "Auditors love documentation; they're going to ask for it," he says. "The quality of your documentation is going to govern how long that auditor sticks around." Whether true or not, good documentation signals to auditors that a company is doing the right things around security.

2. Define your trusted insiders

If your company is like most, you need to realign your thinking around the term "employee." With firms opening up to more and more third-party access via

outsourcing, partnerships and other arrangements, you're expanding your perimeters, often unthinkingly. Sometimes that sort of quasi-insider access is thought through and locked down; sometimes it isn't.

"Many times, networks are set up in such a way that those people have the same access as regular employees," according to Michael Gavin, security strategist at Security Innovation, a company that provides application security and risk assessment, risk mitigation and training services. "Before you decide that someone is a trusted partner," Gavin says, "put controls in place to limit their access."

As an extension to that, make sure your next threat assessment includes a broad look at exactly who has access to what parts of the company, who defines and controls that access, and evaluating what level of risk that introduces.

3. Crack down on physical security

It's been said plenty before, but it evidently bears repeating, since laptops continue to be lost or stolen apace. Take yet another hard look at whether your company could be a very public victim of a physical theft of a laptop, or of backup tapes or a memory stick mysteriously gone missing, or one of the myriad other ways that huge batches of customer data have disappeared lately.

Like so many employee security issues, it's an education issue in great part, so make a vow to step up employee training that focuses on this particular issue. And don't forget those trusted outsiders mentioned earlier; they need training as well, either by you or by their employer. IT also needs to do its part by properly encrypting data and limiting worker access to it, but there's plenty of work to go around here, and educating employees is crucial.

It's not just laptops, but any mobile device, since more and more can carry significant amounts of data these days. Also, Gavin says he's seen cases where corporate access policies are less stringent when it comes to network access via mobile devices. That might be because higher-ups are often the users of those devices, and it can be hard to say no to the CFO. Again, take a hard look at your policies: Are they up to date and do they delve into enough detail in terms of the latest devices? At your next risk assessment, ask whether the convenience of C-level access is worth the risk.

4. Plug the browser gap

Malware. Viruses. Root kits. Key loggers. It's all bad, and it's all out there waiting for an employee inadvertently running amuck on the Internet. (Root kits take over the operating system; key loggers record and report back on a user's keystrokes.)

By running ActiveX controls and other executables, Gavin says, users can pick up all sorts of malware. The best defense: companies can blacklist known bad sites, using software designed for that purpose. Or whitelist sites, allowing employees to use their work systems only on allowed sites. In either case, the product should have a client agent, so that if users aren't on the corporate network but are elsewhere on a company laptop, they're still protected.

5. Watch the Web surfing

Although big firms get most of the media attention when a breach occurs, small companies face at least as many challenges in keeping employees in line and out of trouble. MIS Alliance is an IT solution provider that focuses on small and mid-size companies. In companies with a few hundred employees or less, according to VP of IT Brad Dinerman, the biggest problems come from the Internet. Despite warnings, Dinerman says, employees "continue to go to the Web and download whatever is of interest to them at the moment." That might be a freeware screen saver, a new toolbar, or a piece of pornography. Any download, of course, can carry a variety of malware along with it.

6. Push password rules

Another problem Dinerman sees regularly: A failure by employees to change passwords regularly, and when they do change them, to choose appropriately complex words. Company training to address both Web surfing and poor password policies should include pointed, direct infor-

mation about how a security breech affects the entire company. After all, at a small company, a single training session might need to reach an audience ranging from the office manager to the night guy in shipping who just wants to surf the Web when things are slow.

7. Create an "acceptable use" policy

Another good tool for reining in employees: Dinerman highly recommends that employees be asked to sign an "acceptable use" policy. "Those are important; we make all of our employees here sign one," he says. The document basically functions as a stern warning, in which employees agree that, for example, anything they do on a company computer is legally discoverable; that the company can repossess computers at any time, and that employees won't conduct personal business using the company email system. Basic rules, but putting them in writing helps to show employees that you're serious.

Because new security challenges arise regularly, Dinerman also suggests that IT staff at small companies, who often wear many hats, consider joining a security organization for networking and information-sharing, and for sample documents such as an acceptable use policy. He formed such a group five years ago, the National Information Security Group, which meets monthly in Boston to discuss security issues. Its technical tips mailing list is free, as are meetings; sign up at http://www.naisg.org.

8. Monitor phishing threats

One reason for regularly repeating employee security training is the constant stream of new and fresh ways attackers come up with to elicit information from the unwary. Spear phishing is a clever term for phishing taken to another level by targeting a specific set of users about which attackers have some piece of information. The attack might look like it's coming from HR, or from a friend. Those tactics can make the phishing e-mail seem very real—it might address a user by name, reference a specific account, include an address, and so forth. That boosts the success rate of such attacks, Gavin says, and can also help such email fly under the radar of spam software and other perimeter defenses.

Again, users need to be warned regularly through very immediate examples of the sort of threat this poses, and reminded again to never ever respond to email requests for personal information, and to never click through on email links requesting that information. Also, Gavin says, the latest round of browsers have some anti-phishing capabilities, by which they can sometimes identify a suspicious Web site and which are updated regularly with known phishing sites. Those may not work for spear-phishing, though, so be aware. IT administrators can join the Anti-Phishing Working Group, or APWG for more information.

9. Watch your wireless network

The proliferation of wireless has created a whole new set of issues, among them the ability of an ordinary employee to create an onsite wireless access point, or WAP, on the company's wireless network. The problem with that, according to Security Innovation's Gavin: "If you set up a WAP and are not authorized to do that, you're managing it yourself." For that reason, it's much more likely to be successfully broken into. "They have to be taught that they need to be willing to let it be managed by someone else," Gavin says.

Again, the best remedy here is increasing employee awareness. Although such rules are seldom popular, make it known that rogue devices are a security breach, and users who want to set up a laptop as a wireless access point need to understand the ramifications, and talk with IT first.

Another strategy to control unauthorized wireless access points, Gavin says: "Do what the attackers are going to do. Occasionally walk around and look for things. Put together the old Pringles can and go 'war driving' in your own environment. I really don't know a better solution than to occasionally do that." (The Pringles can reference is to a much-discussed method of building a wireless antennae device on the cheap.)

10. Train, train, and train some more

If there's a common thread the experts all agree on in addressing each of these issues, it's the importance of education and training. Poor training and unaware employees lie at the root of many if not most employee security breaches. All three of the interviewed security experts emphasized one point: Use real-life examples from today's headlines to shake employees out of security complacency and to help make your points. Unfortunately, there's no lack of those stories into the foreseeable future. ■

Linda Briggs is the founding editor of Microsoft Certified Professional Magazine and a former senior editorial director at 101communications. Based in San Diego, she writes about technology in corporate, education, and government markets. You can contact her about this and other articles at lbriggs@lindabriggs.com.

Data Breach Kit: Five Steps to Help You Survive the Inevitable

Fact: Information systems are porous. Most companies will, despite their best efforts, allow some level of data exposure during the next year. Are you ready? Learn the tools and processes you need in place now to control data-breach damage, perform digital forensics, and gather the evidence required to recover and reduce risk.

By Mathew Schwartz

Published online June 19, 2007

Data breaches are inevitable, and

most companies will—despite their best efforts—suffer a breach in the coming year. Such breaches may compromise people's confidential or personal information and thus put an organization in noncompliance with various regulations, including HIPAA, the Payment Card Industry Data Security Standard, Visa member rules, or privacy laws with notification requirements now in effect in many states and countries.

Yet many organizations do not detect a breach until extensive damage has been done, or know how to proceed when they do suspect a breach. Accordingly, all companies—and especially those in regulated industries—need a data breach response plan, including a strategy for utilizing digital forensics to investigate breaches.

By planning ahead, organizations can spot breaches and react more quickly to contain the damage, gather evidence, and know who to notify. "With any kind of regulation, the faster you react, the more you can limit your exposure," says Michael Gavin, security strategist at Security Innovation. "If someone has broken into your database and it's HIPAA information, the more time they have to download records, the more the organization is at risk."

Five Steps to Contain Data Breaches

To control data-breach damage, pursue forensic investigations that hold up in court, and help prevent breaches from happening in the first place, experts recommend companies follow these five steps:

1. Spot the Breach

To stop data breaches, first know there's a breach. Otherwise, your company may end up like the TJX Companies, which didn't discover an ongoing breach resulting in the theft of 45.7 million credit card numbers until several years after it began. Cue regulatory actions, public outcry, and class-action lawsuits.

To detect breaches, IT departments must monitor network and system performance, disk usage, Internet

activity, and any unusual access. Related tools include intrusion detection/prevention systems (IDS/IPS), network security monitoring tools, plus security event and log correlation and analysis tools. "Look to anything that has some sort of alerting mechanism on things that happen in your environment—anything suspicious or unusual," says Gavin.

Of course, many organizations already have such tools. "People say, we have IDS systems in place, and you say, great, when was the last time you actually looked at them? And you get the blank stare. When did you look at the logs on your Active Directory servers? Are you deleting users who are no longer with the company? Things of that nature," says Brian Gawne, who heads the forensics practice at CTG Information Security Solutions, which is a certified assessor for Visa.

In other words, to spot breaches, IT must now pay attention to "all the stuff that IT shops don't have a lot of time to do," he says.

2. Build Response Plans

Next, study the top information security threats facing your organization, and begin creating an incident response plan for each one, beginning with the greatest risks first. Each plan should detail who at the company can request a forensic investigation of a suspected security breach, and how that investigation should proceed.

In particular, each plan should address how you will:

Respond. Specify how to respond to the threat in question. For example, a credit card processor might block a denial of service attack yet keep all systems online. If a healthcare database storing HIPAA information is under attack, however, the plan may be to take it offline, pending an investigation.

Investigate. When defining goals for an investigation, companies typically want "to identify early on what's been exposed, what's the damage, how broad is it, how extensive, and what types of data did they actually get access to," says Gavin. Often, this involves rapid triage, and then testing assumptions based on initial research. "Things that you find, you need to just drill down and see how deep they go."

Notify. For each type of incident, know who to notify. Requirements vary based on regulations and business partners. For example, if a Visa member company suffers a security incident—defined by Visa as "deliberate electronic attacks" on "communications or information processing systems"—then it "must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings," all within 10 days. Yet determining whether or not you will need to notify law enforcement agents of a breach or attack can be unclear. Thus, experts recommend getting to know agents at your local FBI and Secret Service branches now, so you'll know who to ask.

Also update your security policies so investigators can access any data or devices they need during an investigation. Gawne says related security policies typically specify that employees "have no right to privacy if using corporate-owned assets or … private ones in the enterprise," such as iPods.

3. Train Response Teams

For each security incident response plan, identify who's on the response team. While the exact mix will vary by plan, such teams often draw from human resources, legal counsel, financial managers, technical specialists, company leaders, and even public relations. Indeed, "if it's a breach, you may want them to be able to spin this," notes Gawne.

Train the teams—including executives—on the plans, and then regularly test and refine them. "Practice the plan," says Gavin. "Find out where it's weak and where it needs improvement."

Also train in-house IT personnel about how to respond to a suspected incident, and to always document changes they make to the IT environment, whether in response to a breach or not. "That's the biggest problem I come across—there were no notes taken," says Gawne. Such

notes will dramatically speed an investigation, since they tell an investigator which changes to the IT environment were authorized and made purposefully, to help them then identify suspect activity.

4. Find Digital Forensics Experts

Digital investigations require forensic specialists who know proper techniques for seizing devices, properly imaging and analyzing them, as well as how to correctly document their efforts and transfer custody of evidence. In addition, they are typically certified to use the two primary tools for performing digital forensics: Guidance Software's Encase, and Access Data's Ultimate Forensics Toolkit (FTK).

Frequently attacked companies—especially high-technology companies and financial institutions—often have on-staff forensic investigators. Most other companies will look to consulting companies for help on an as-needed basis, and thus should plan ahead: identify digital forensic specialists you can call in an emergency, and consider working with them now to refine your security incident response plans.

Avoid making existing IT staff into amateur forensic investigators, simply because of the amount of knowledge needed to successfully extract and analyze data from a variety of devices—from PCs and Apple laptops to the latest smart phones and USB keys—while also maintaining its integrity.

5. React Quickly but Meticulously

With proper planning, a response team can and should react quickly to any suspected attack. "When you're dealing with a security breach, time is of the essence, because people will do some unintelligent things when everybody is scrambling to patch a hole in a system," says Gawne. "So the sooner we can get in, help control the problem, while maintaining the environment and controlling evidence, the better we're going to triage everything—figure out what's going on, forensically look at systems that may have been the point of access, and as you're doing this, help the client secure the network, get things under control, and stabilize the systems. We're not just going in there to catch the bad guy."

Once you've launched an investigation, be meticulous. "Conduct every investigation as if it will go to court," says Gavin. That way, investigators won't mishandle evidence if the investigation—or a counter-suit—does end up in court. Remember, minor breaches sometimes end up revealing major disasters.

Closure Not Guaranteed

By following the above steps, organizations can create fast-reaction plans to contain data breach damage. Yet what about going a step further, and catching the bad guys?

Unfortunately, closure is often an abstract concept. Even in cases of blatant security policy violation or fraud, many cases settle out of court. Others may be dismissed for lack of evidence or jurisdiction, or take years to resolve. Indeed, about five years ago and in a previous job, Gawne says he investigated the theft of 8 million credit card numbers and ultimately worked with both Visa and the Secret Service, which considered the crime a felony and began investigating. As of recently, he heard it's still an active investigation. ■

Mathew Schwartz is a contributing editor for the IT Compliance Institute. You can contact him about this and other articles at Mat@PenandCamera.com.

Threats, Compliance, and the Human Condition

Blame human psychology: when it comes to information security, we're simply not built to intuitively rank actual risks. Learn how building threat models can help companies rationalize the biggest security and compliance risks they face.

By Mathew Schwartz

Published online April 10, 2007

Human psychology: can't live with it, can't live without it.

When it comes to judging security risks, we humans do great—provided we're responding to an obvious and immediate threat. Thousands of years of evolution have prepared us for the moment we get charged by a rhinoceros: the adrenaline kicks in, and without a second thought we literally run for our lives.

Information security threats, of course, are not two-ton, plant-eating mammals with horns; they're rarely so obvious and frequently much less imminent. As a result, we typically overreact to less risky threats while ignoring bigger, quieter, more long-term hazards. Thus we obsess about laptop encryption, try to automatically monitor for information leaks, while ignoring the threat of insiders or social engineering attacks, and wait for some impending governance, risk, and compliance platform silver bullet to solve all future problems.

Lack of information is frequently not the cause of our inability to identify our biggest information security and compliance-related threats. Rather, it's a more fundamental problem. "We are not adept at making rational security trade-offs, especially in the context of a lot of ancillary information designed to persuade us one way or another," alleges BT Counterpane chief technology officer Bruce Schneier in a recent essay titled "The Psychology of Security." In particular, he identifies five areas "where perception can diverge from reality" when it comes to evaluating security trade-offs: risk severity, risk probability, cost magnitude, countermeasure effectiveness, and the actual trade-off itself.

The causes are simple: evolution isn't done yet. "Our ability to duck that which is not yet coming is one of the brain's most stunning innovations, and we wouldn't have dental floss or 401(k) plans without it," noted Harvard psychology professor Daniel Gilbert last year in a Los Angeles Times op-ed. "But this innovation is in the early stages of development. The application that allows us to respond to visible baseballs is ancient and reliable, but

the add-on utility that allows us to respond to threats that loom in an unseen future is still in beta testing."

So how can security and compliance managers overcome these basic human-condition stumbling blocks and better rationalize actual threats? The answer: compliance officer, know thyself. Perhaps by understanding our psychological predispositions, suggests Schneier, "we can learn how to override our natural tendencies and make better security trade-offs."

Beyond Darwin: Security Survival in the Information Age

What you don't know can kill you—or at least seriously damage the business, as you apply resources to mitigating one risk, while potentially missing or ignoring an even greater one. Accordingly, many organizations are adopting risk management frameworks to help executives build a complete picture of all risks to the business, whether they relate to business models, competitors, compliance, outsourcing, or technology.

Yet as noted, human psychology and objective risk assessment have an imperfect relationship. One predominant psychological predisposition—affecting everyone from executives down to IT managers—is what Ed Adams, president and CEO of Security Innovation, and author of the forthcoming Information Security Management: Survival Guide, calls the "recency" trap. "That trap is reacting and often overreacting to a recent or current event that causes you to make security investments—usually in the wrong place, and for the wrong threat."

One example: the trend to encrypt all data stored on a laptop, especially since organizations including Boeing, Ernst & Young, ING, and the Veteran's Administration lost laptops storing people's personal information. "The reaction is, all of a sudden we must encrypt all data on any machine that could possibly leave the building, and that's a reaction that's going to be very costly in terms of time and productivity," says Adams, and possibly not all that useful a security countermeasure at many organizations.

Indeed, encryption is notoriously difficult to implement; many organizations try but don't get it right. Thus laptop encryption may create the feeling of security, while actually leaving organizations less secure—a double-whammy. "You only have a certain amount of resources, and time, and attention, and when you mandate something like 'all data on laptops must be encrypted,' you're taking your eye off of other problems that are much more real and much more risky," he says.

Toward Rationality: Threat Modeling

Instead of just reacting to current events, Adams recommends a different approach: threat modeling. Namely, identify the most likely threats to high-value applications, development processes, business logic, or just the business itself. Then see whether these threats are currently mitigated. If not, then organizations can create an action plan to prioritize risks and assign resources appropriately, starting with "low-hanging fruit, areas prone to attack, or at high risk," he says.

How can organizations build threat models? Useful starting points vary by domain, but include the National Institute of Standards and Technology's Special Publication 800-30 ("Risk Management Guide for Information Technology Systems"), the Microsoft Threat Modeling Process, and the forthcoming, version 3 of the Information Technology Infrastructure Library (ITIL), which advocates threat modeling as part of best practices for IT service delivery. "All ITIL is saying is, as a good IT department, you're delivering high-quality service, and this is one of the activities you should be conducting so you can best prioritize how to spend your time when a new threat becomes apparent," says Adams.

Threat models, once generated, also persist, and this speeds ongoing risk assessment. "When a new risk is produced, you can pump it into that model and see if you've already mitigated against it, or if you need to address it," he says, as opposed to having to conduct penetration

testing on every potentially affected application or business process.

Threat Modeling for Beginners

If you are just starting out with threat modeling, model high-value applications and business processes first, since they're most at risk, and also because small mistakes can mean big problems. For example, Adams says his company recently tested the security of a Georgia bank's online consumer banking application, which the financial institution rated as extremely secure. Yet when the security team opened several bank accounts in a short period of time at different branch locations, they quickly noticed a pattern: new bank accounts appeared to be numbered sequentially. So researchers created a list of 1,000 likely account numbers, then looked for a way to guess the four-digit PIN required to gain online access without tripping the "three strikes and you're out" safety check, which then requires a call to customer service to reset your password.

Accordingly, the security researchers tested two common PIN numbers for all 1,000 accounts: "1234," with 29 percent success; and "0000," with 14 percent success. In short, "using just two PINs, and counting on the psychology of users, we were able to get access to over 40 percent of accounts," says Adams. This, obviously, was a large risk to the business, especially because such access wouldn't appear abnormal. Thanks to the threat model, however, the bank was able to quickly address the previously unidentified problems.

From Reactions to Rationality

Building a threat model helps security and compliance managers identify the actual risks their organization faces. Thus threat modeling allows an organization to know: "Do I invest time, money, or resources in this area, or do I invest those resources somewhere else?" says Adams. "That's hard to do in the absence of a threat model, because you're prone to fear, uncertainty, and doubt." These psychological predispositions, however natural, unfortunately don't make for optimum security investments or IT compliance success. ■

Mathew Schwartz is a contributing editor for the IT Compliance Institute. You can contact him about this and other articles at Mat@PenandCamera.com.