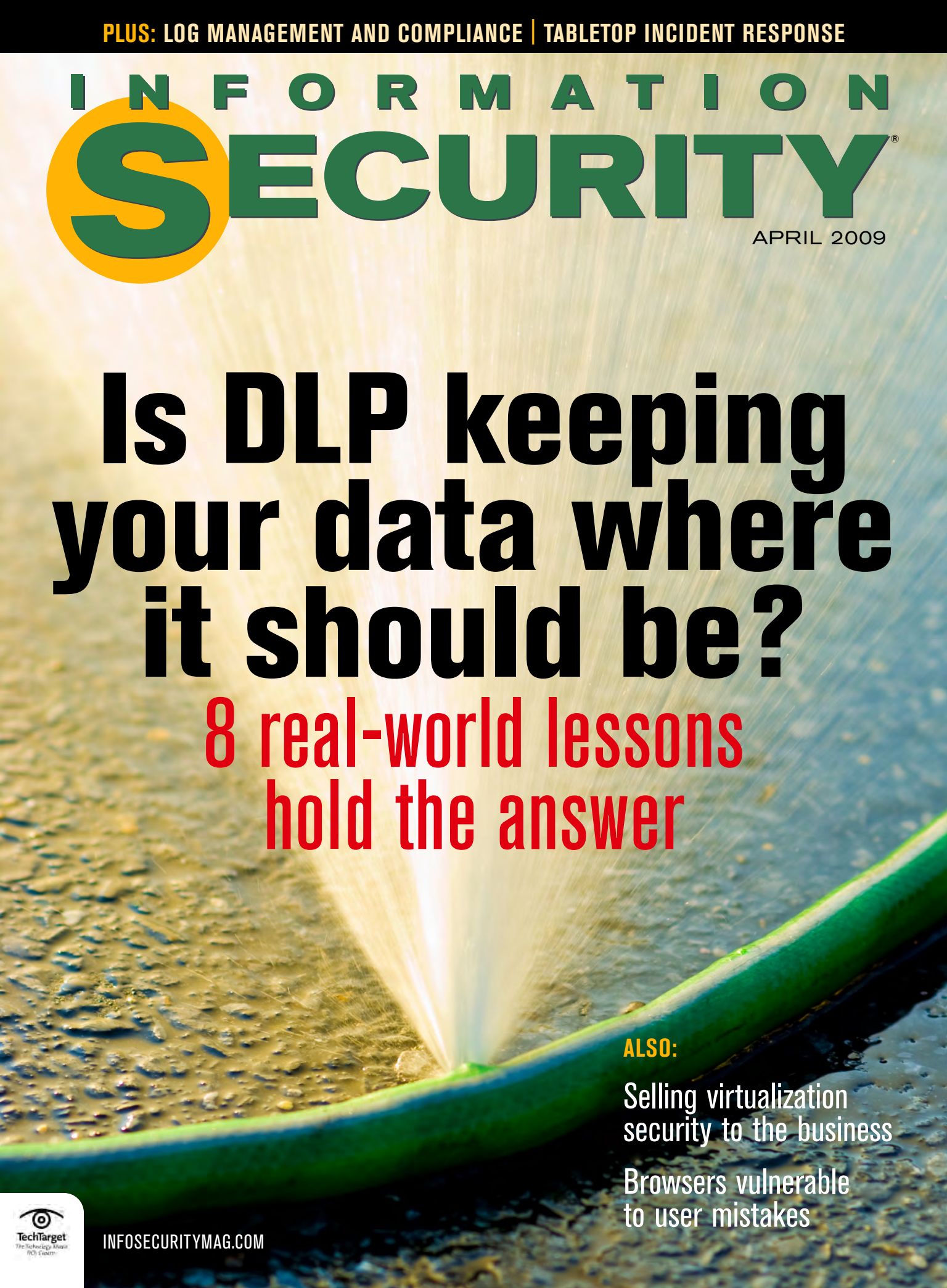
PLUS: LOG MANAGEMENT AND COMPLIANCE | TABLETOP INCIDENT RESPONSE

INFORMATION SECURITY®

APRIL 2009

Is DLP keeping your data where it should be?

8 real-world lessons hold the answer



ALSO:

Selling virtualization security to the business

Browsers vulnerable to user mistakes

TechTarget

INFOSECURITYMAG.COM

contents

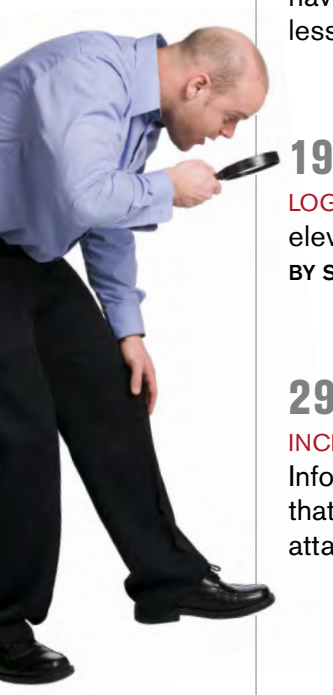
APRIL 2009

VOLUME 11 NUMBER 4

FEATURES

12 Get Real

DATA PROTECTION Data loss prevention implementations have viability in the enterprise; these eight real-world lessons help you use DLP to its fullest. BY RICH MOGULL



19 Whodunit?

LOG MANAGEMENT Tying log management to user identities elevates incident response and forensics to a higher level. BY STEPHEN NORTHCUTT

29 This Is Only a Drill

INCIDENT RESPONSE Delaware's Dept. of Technology and Information conducts annual incident response exercises that test the readiness of state agencies to respond to attacks. BY MICHAEL S. MIMOSO

6 PERSPECTIVES

No Free Lunch

Executive management sees virtualization as the cure-all, but CISOs need to ensure it is done securely.
BY JACK PHILLIPS

ALSO

3 EDITOR'S DESK

Embrace SaaS; You Have No Choice BY KELLEY DAMORE

8 SCAN

Beefed-up Browsers Cannot Contend with Human Element

BY ROBERT WESTERVELT

10 SNAPSHOT

Target: Apple

36 **Advertising Index**

Database security and compliance made simple.

More Global 1000 companies trust Guardium to secure their critical enterprise data than any other technology provider. We provide the simplest, most robust real-time database security, and activity monitoring solution for:

- Protecting Oracle EBS, PeopleSoft, SAP and other sensitive data.
- Preventing SQL Injection attacks.
- Enforcing change controls & vulnerability management.
- Blocking privileged users such as outsourced DBAs from accessing sensitive data.
- Automating compliance reporting & oversight.

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

Guardium®
SAFEGUARDING DATABASES™

Embrace SaaS; You Have No Choice

BY KELLEY DAMORE

Like it or not, software-as-a-service and cloud computing is the future.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

THE LURE OF SOFTWARE-AS-A-SERVICE IS SIMPLE: It comes down to cold hard cash.

So in this economic environment, it comes as no surprise that organizations, large and small, are looking to SaaS providers to offer them services where they pay for infrastructure or expertise on a monthly basis.

Salesforce.com is the poster child for the SaaS space offering hosted CRM. Other business applications using the SaaS model include HR, expense reporting and the like. We've seen SaaS models also pop up in the security space with Qualys, Webroot, Google, Veracode, Zscaler, Purewire , among others, offering security services ranging from messaging security to vulnerability assessment to application security testing. With huge data centers, Amazon and Google rent their capacity on a by-job basis.

It seems to me that in a relatively short amount of time this will be the way we use computing power and access applications. It will radically change the ways businesses operate—much like what Web browsers and email did in the 1990s.

And you've got to adapt. You'll have no choice. So the time is now to look at the security and regulatory implications of these types of services and get ahead of a wave that seems almost inevitable.

The reason SaaS works at the lower price points is because providers are able to host multiple customers on a shared infrastructure [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1313252,00.html]. And it's just this type of architecture could be very troubling for a security team. As a security manager, you have to insert yourself into the conversation and lay out a few necessary requirements [http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1337369,00.html].

The first must be clear separation of customer data. In addition, you need to determine whether you can get access to logging and audit trails for both compliance and security should an incident occur. Moreover, determine how secure are their Web applications? And what about insider threats at the provider's facility? What are your provider's access controls? How does your provider handle breaches or other insider threats?

Add in government and industry regulations and you've got a lot to muddle through.

But thankfully there is lots of time for discussion and fixes. The market is relatively new and many of these questions will need to be hashed out. It is your job as users of these services to force the SaaS providers to offer you the adequate answers you need.

It will take time but as other technologies before this, the industry, and security practitioners, will come up with a way to make it work.

Kelley Damore is Editorial Director of Information Security *and TechTarget's Security Media Group. Send your comments on this column to feedback@infosecuritymag.com.*

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

VIEWPOINT

Readers respond to our commentary and articles. We welcome your comments at feedback@infosecuritymag.com.

Seeing Green Over Digital Edition

I've canceled my subscriptions to a number of periodicals recently. I often find that in most cases the one or two articles of interest don't warrant the resources used to get that printed material to me. I am aware that digital-only editions may impact advertising rates, but I hope people continue to support publications that exist in digital format.

To see *Information Security* magazine in digital and PDF format really tickled me. I hope other people are happy with the PDF format and the periodical continues to get supported and disseminated.

Thank you for doing your part on reducing the waste of resources for printed materials. Cheers and kudos on taking the plunge. I will continue to read the PDFs, and am now back to cover-to-cover again.

–Name withheld on request

Thumbs Down

The concept of digital magazines is faulty from the get go; cheaper, but faulty. I scan/read paper magazines at home during TV commercials and slow shows, but I'm not going to do that with digital magazines because I'd have to keep the laptop fired up all the time.

As it is now, I spend way too much time during the week and on the weekend on a PC. I want to spend less, not more. And I refuse to read advertising on my work PC.

I tried the PDF but the quality, even magnified, is poor in comparison to print.

If you had a digital full index where I could jump to articles that interest me, I might print them and read them.

Otherwise, you are toast. sayonara!

–Craig Honour, CIO, Atlantic Marine

As a longtime reader, it's great to see *Information Security* magazine finally move to an electronic format. A big reason I appreciate this move is to cut down on paper use and, in turn, reduce my personal carbon footprint.

Now the next step is to modify the layout to take advantage of this format. I know: One step at a time.

–LeAllan Estrem, company withheld on request

And so another trade magazine disappears.

The Web pages can't be read while eating lunch, while traveling, and so on. Going to the trouble and expense of putting something on paper suggests to the reader that there's something of import. With just a website, I tend to think "Ho-hum, it's yet another of the bazillions of web pages out there."

–Bob Cromwell, Cromwell International

COMING IN MAY

Make the Call: IDS or IPS

You need to make a network security decision in your organization: Do you want an intrusion detection system? An intrusion prevention system? Or both? An IPS is not the same as an IDS. However, the technology that you use to detect security problems in an IDS is very similar to the technology that you use to prevent security problems in an IPS. Learn how to make this important call and distinguish between the similarities not only in product functionality, but in vendor messaging.

Automation Cures Compliance Blues

Virtually all regulations and contracts require documentation, audited requests and approvals, logging, and review of all the operational activities that companies engage in to protect information. Automation and better organization cure these process burdens. This article will discuss how companies can use technology to achieve compliance mandates common to many regulations.

IAM Evolving Before our Eyes

Move over traditional identity and access management technologies such as provisioning and Web access management. There's an evolution going on in IAM that introduces entitlement management, enterprise SSO, privileged account management, Active Directory bridge and virtual directory products. Read more about this evolving market and learn how to fully leverage your identity management investments.

MUST READ!

No Free Lunch

Executive management sees virtualization as the cure-all, but CISOs need to ensure it is done securely. BY JACK PHILLIPS

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

VIRTUALIZATION HAS TAKEN on a life of its own, sweeping across organizations of all sizes and shapes like a perfect antidote to all the inefficiencies in IT. Executive management has been rushing to inject this drug as quickly as possible, viewing all of the costs savings realized through virtualization as free. And in this economic environment, the pressure is particularly high to move quickly and ask questions about security later.

"Free" to a CFO or CEO means getting all the efficiencies without any commensurate risks. A few of the perceived freebies include faster time to market for new applications via "McServers," less physical space to house data centers and server farms, less power to cool and operate the data centers, faster and lower-cost disaster recovery.

But we in security know better. There are no free lunches in IT. Now that the antidote has taken effect in most organizations, some of the side effects are popping up. Things have moved so quickly that IT security has struggled to define its role in the new virtual world, to create the same relevance it has in the physical world.

"Free" to a CFO or CEO means getting all the efficiencies without any commensurate risks.

IANS, an information security focused research firm, surveyed about 200 security executives last year on virtualization. Seventy-five percent use some form of virtualization software in their production environments, either at the client or server level. However, among those organizations polled, only five to 10 percent of IT security teams were included in the decision to virtualize.

As virtualization deployments have grown in number, the implication of the survey results is clear: policies and architectures are not being updated to reflect the demands and constraints of a virtualized environment because IT security wasn't included in the upfront planning and implementation. It's time to strategically insert your voice into those conversations.

This year more than ever, IT security's livelihood lies squarely in how business owners perceive added security will grow revenue or lower operational costs—it's that simple. Of course, this has always been true, but 2009 will be the ultimate test. Prove relevance or perish—that's the new motto.

And so, creative CISOs are getting out of their offices and seizing every opportunity to position security as a business enhancer. Securing virtualized environments is one of those areas where security leaders are grabbing big wins in the perceived value of IT security to the organization's business. Here's the language

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

they're using with business owners:

- **Stealing the business is now easy.** Portability of virtual hard drives means the intelligence and processing of an entire business could be stolen, not just slowed down or hindered. This "lose-my-business" risk rather than the old "lose-my-bonus" risk should drive executives to allocate some operating budget for security.

- **Business applications are more vulnerable to security threats.** We don't understand the new class of vulnerabilities associated with this new thing called the hypervisor. The chance that critical applications running in a virtualized environment could be crippled by unknown vulnerabilities is now much higher. Low-cost architecture, zoning and security policy refreshment can go a long way to mitigating the unknown.

- **Invest with confidence.** If virtualization is here to stay, business owners are salivating at a faster path to introduce new technical functionality that can expand business capabilities. Virtualization can be a risky investment. Security's role is to validate when additional investment using virtualization is being made wisely and securely.

The security implications of this new world are becoming clear to security teams. In a year when IT security leaders have to prove relevance in the minds of both business executives and IT, securing the virtualized world should be a top priority.

Jack Phillips is co-founder and CEO at IANS, an independent research firm based in Boston. Send comments on this column to feedback@infosecuritymag.com.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
REAL-WORLD DLP IMPLEMENTATIONS
LOG AND IDENTITY MANAGEMENT
TABLETOP EXERCISE
SPONSOR RESOURCES

Analysis | BROWSER SECURITY

Beefed-up Browsers Cannot Contend with Human Element

Hackers continue to bore holes in Web browsers, exploiting users with social engineering tricks to gain unauthorized access to systems and data.

BY ROBERT WESTERVELT

MANY SECURITY VENDORS have sung the same tune over the last couple of years: the browser is not only vulnerable, it's the front line of most cyberattacks. That message couldn't have been any clearer at this year's CanSecWest conference.

Two researchers easily exploited zero-day flaws earning themselves thousands of dollars in prize money during a contest sponsored by TippingPoint's Zero-Day Initiative. It took the two young white-hat hackers only a few hours to uncover four critical vulnerabilities and break into systems running Apple Safari, Microsoft's newly released Internet Explorer 8 and Mozilla Firefox.

"It's a game of cat-and-mouse and it's going to continue to be a game of cat-and-mouse no matter how many security features are put in," says John Strand, a senior security researcher with Black Hills Information Security.

Just a day after one of the two hackers cracked IE8, Microsoft released the browser to the public http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1351376,00.html—flaw and all. But security experts praised the updated browser for its new cross-site scripting (XSS) filter that automatically disables XSS attacks when they're detected. An anti-clickjacking feature prevents users from clicking a hidden Web element. A SmartScreen filter was redesigned to make it more difficult for users to click through to a malicious Web page.

Security experts also lauded more technical security features. A data execution prevention feature in IE 7 is now enabled by default. Data-execution prevention makes it more difficult for attackers to run code in memory that is marked non-executable. It's partially what has made Windows Vista difficult for hackers to exploit.

But all the security features in the world won't block the social engineering methods used by attackers to exploit browser flaws and Web application errors. Tools are available for companies using Flash, AJAX and Java-based Web applications to test for coding errors that could lead to browser exploits. But the holes continue to exist, and the tools won't keep the user in check.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

"End users are going to continue to click on malicious links and browse to Web pages hosting malware," says Matt Watchinski, director of vulnerability research at Sourcefire. "You can't eliminate the human factor."

And the human factor applies to software developers, too.

Boaz Gelbord, executive director of information security at Wireless Generation heads a project for the Open Web Application Security Project (OWASP) http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1352074,00.html that is researching company spending on software development projects. A recent survey conducted by the project found that 61 percent of respondents had an independent third-party security review of software code to find flaws before Web applications are used live. Gelbord says the predominant thinking has been that companies are conducting code review in-house if they're even doing it at all.

"The approach that companies are taking is to have security developers with some security training looking out for major flaws," Gelbord says. "They're bringing in third parties who really have expertise to look for more difficult to find vulnerabilities."

> "End users are going to continue to click on malicious links and browse to Web pages hosting malware. You can't eliminate the human factor."
>
> –MATT WATCHINSKI, director of vulnerability research, Sourcefire

Even with experts crunching code for errors, issues will remain. The CanSecWest conference not only demonstrated that browsers are on the front line, it showed that hackers will find a way in not matter how many security controls are in place. With the release of IE 8, Microsoft demonstrated how a browser maker can mitigate the risk of an attack to a more manageable acceptance level. But the human factor will always remain.›

Robert Westervelt is news editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

Target: Apple

AN APPLE A DAY may keep the doctor away, but Apple sure isn't keeping hackers at bay. Researchers at the CanSecWest conference and SOURCE Boston demonstrated in short order last month how relatively simple it can be to crack the venerable Mac OS X.

—*Information Security* staff

12 BYTES OF ARBITRARY CODE

Researcher Dino Dai Zovi said a dozen bytes is all you need to defeat Mac OS X and gain access to root memory, establish a TCP connection and download malicious code. Dai Zovi demonstrated his hack at the SOURCE Boston conference.

10 SECONDS

Charlie Miller owns the Pwn2Own contest at CanSecWest. Miller won the hack-a-thon for the second consecutive year, exploiting a fully patched MacBook Air using a Safari code execution vulnerability. And he did so in 10 seconds.

3 BROWSERS, 1 HACKER

Going by the name of Nils, another hacker at CanSecWest took aim at the Web's three major browsers and battered them all. Most impressive was his takedown of Internet Explorer 8 running on Windows 7 using a zero-day bug—all this done a day before the browser's public release. Next to fall were Apple's Safari and Mozilla's Firefox; Google's Chrome was the only browser to emerge unscathed.

$5,000 PER BUG

Miller pocketed a cool $5,000 for his Pwn2Own win, along with a MacBook Air, while Nils carted off $15,000 for his trio of browser bugs. The details of each flaw were provided to contest sponsors TippingPoint, whose Zero Day Initiative rewards researchers who disclose bugs to the program.

OVER-HEARD

"Steve Jobs' fairy dust only protects against the most naive attackers. Writing exploits for [Microsoft] Vista is hard work. Writing exploits for Mac is a lot of fun."

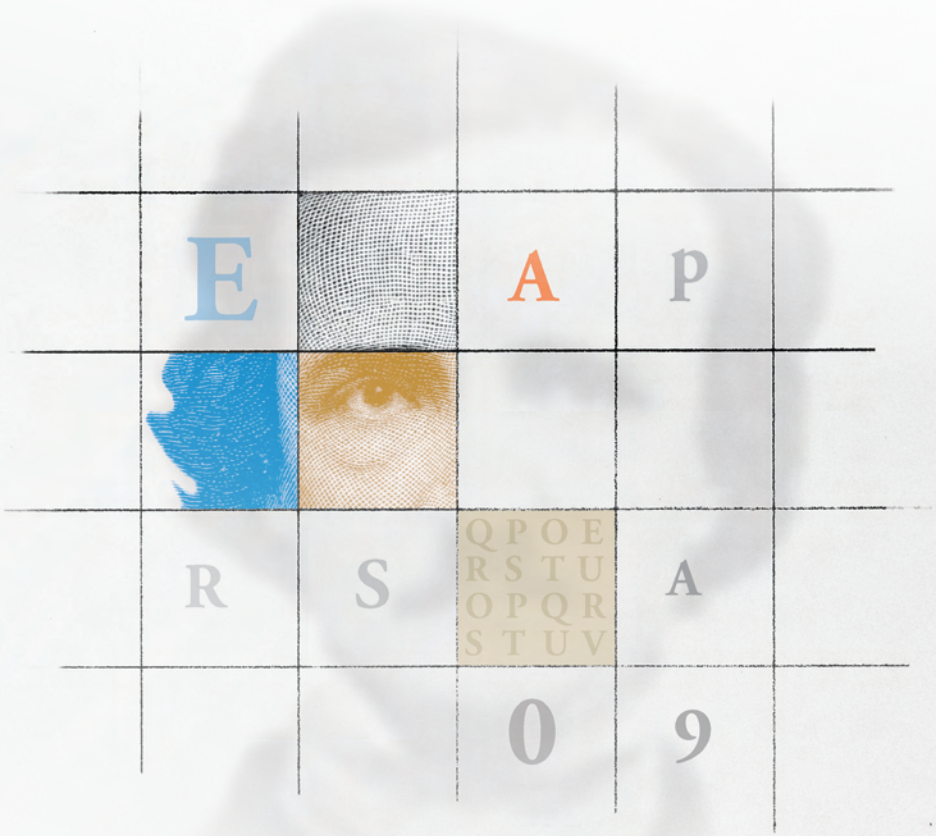
–DINO DAI ZOVI, security researcher

RSA® CONFERENCE

WHERE THE WORLD **TALKS SECURITY**

When the next security threat hits, be ready to hit back.

U.S. businesses lost an average of $289,000 in 2008 to security breaches.† No business or organization can afford exposure to that kind of risk. Educating yourself on the strategies and solutions you need to stop this exposure is your imperative. RSA® Conference is the one place where you can meet with experts, colleagues and vendors to find solutions that will positively impact your information security programs now and in the future. It's a security investment you can count on to deliver results — and it's all at RSA® Conference 2009.



REGISTER NOW

APRIL 20–24, 2009 | MOSCONE CENTER | SAN FRANCISCO

WWW.RSACONFERENCE.COM/2009/IS

ENTER PRIORITY CODE: IS049

†Computer Security International (CSI) Computer Crime and Security Survey, 2008.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

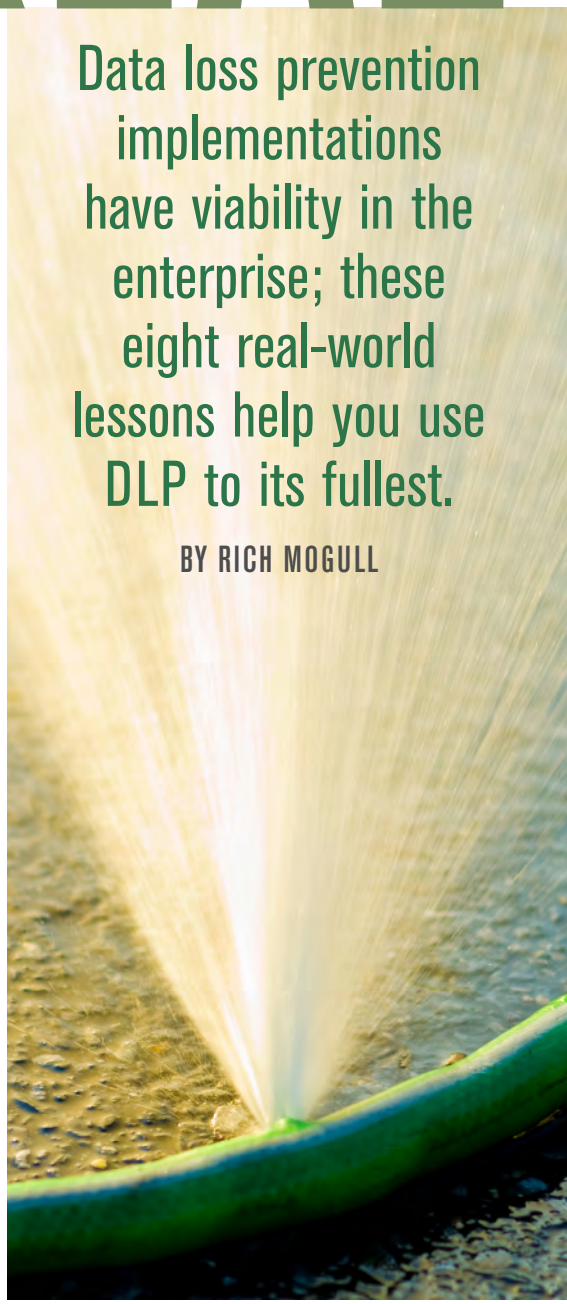
TABLETOP EXERCISE

SPONSOR RESOURCES

GET REAL

Data loss prevention implementations have viability in the enterprise; these eight real-world lessons help you use DLP to its fullest.

BY RICH MOGULL



THE REALITY OF any new technology, security or otherwise, rarely lives up to its promise. Once you move past the bright sheen of the product brochures and top-level user interfaces, only the practicalities of implementing the product in the real world remain. This is especially true of newer technologies we have little prior experience with, where our product expectations are defined by marketing, the press and the rare peer reference. It's only after these tools are tested in the real world, under full production conditions, that we really start learning how to either best implement them, or kick them back to the vendor for a little more polish (and a compelling business use).

Data loss prevention (DLP) is one of the most promising and least understood security technologies to emerge during the last few years. It dangles promises of ubiquitous content protection before our eyes, with shadows of complexity and costs looming over its shoulder. As with everything, the reality is somewhere in-between. We've interviewed dozens of DLP users (including our own contacts, random volunteers and vendor references) to find out how DLP works in the trenches of the real world. The result is a collection of lessons learned and use cases to help you avoid common pitfalls while deriving maximum value.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

LESSON 1: Users are confused by a confusing market

One of the more significant findings when researching this article was discovering extensive confusion as to just what comprised a DLP solution. In large part this is due to competing and contradictory messages from the vendor community. Data loss prevention is a generic term, and it's been used to brand everything from full DLP suites, to encryption, to USB port blocking. By our informal estimate, only 40 percent of the DLP users we talked to use a full DLP product. Of the rest, USB, file and drive encryption and email filtering were cited as the most common data protection techniques. Many of those users knew they weren't really doing data loss prevention, but they cited cost and complexity as their concerns with using a full DLP product (which protects information on the network, in stored data and on endpoints using deep content analysis). For more information on how we define DLP and its technology components, see an article from last February's *Information Security*: "Data Drain" http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1297405,00.html.

One large airline we spoke with is using a generic network sniffer/forensics tool with some basic keyword policies instead of a DLP solution. But this approach has severe flaws, with the security manager saying, "I'm not sure we can actually see everything going on." They are also looking to add USB port blocking, but more to protect against malicious software than to limit data loss. They do expect to look at DLP in 2010 or 2011.

Even though there are only around a dozen full-suite DLP solutions on the market, nearly every major (and many minor) security vendor claims some sort of DLP capability. We call those tools that offer some sort of content awareness—such as regular expressions—on a single channel such as email, "DLP as a feature." But many tools claiming DLP don't even offer that basic functionality. When standard encryption tools market themselves as DLP, it's no wonder customers are confused.

LESSON 2: Full DLP solutions take more effort to deploy, but are more effective and easier to manage

Although you can whack a nail with a big enough wrench, it won't ever work as well as a hammer, and can't touch the efficiency of a nail gun. DLP as a feature does have its place—particularly for clients on a budget, or with only basic data protection needs, but our interviews consistently showed higher satisfaction among those using dedicated DLP suites. Many of the clients using DLP features described it as a temporary measure until they were ready to consider full DLP. One user stated, "We are watching the marketplace closely, but don't want to be an early adopter."

The tradeoff is that dedicated DLP does take more effort to deploy than merely flipping on a feature switch in another product, but deployment requirements are fairly low. On average, a 5,000-person organization can deploy network monitoring with email filtering in a few hours or days, using one to three Full Time Equivalents. Additional network blocking (Web and FTP) usually requires integration with an existing Web gateway, and deployment complexity scales almost linearly based on the number of egress points. Content discovery (data-at-rest scanning) is more resource intensive since you need to manually add storage repositories to scan. Each repository may only take a few seconds to minutes to add, but you have to first identify them and obtain administrative credentials. Endpoint monitoring takes time to

test the software on your standard images, then deploys exactly like any other endpoint tool.

However, full DLP solutions include much more efficient workflow for managing policy violations, especially if compliance, human resources or legal will be involved. They also allow users to create a single data protection policy, and then apply it across multiple channels, rather than defining the information in multiple tools.

LESSON 3: **Set the right expectations and workflow early**

While deploying the technology is fairly straightforward, many organizations find they struggle more with setting the right expectations, defining workflow and building policies. We once had a client install one vendor's product and start monitoring using default policies without defining any incident management procedures or workflow. They stated: "We don't want to snoop on employees, so we don't worry about involving management or human resources," without realizing that most data leaks come from employees, with likely legal and HR implications.

A typical mistake is failing to define what types of data you want to protect, and how you want to protect it, before buying a tool (then being disappointed in the result). The other major pre-selection mistake is failing to engage business unit managers outside of security. One reference purchased an endpoint-only tool to prevent information leaks onto USB devices, only to find the tool shelved once sales management started receiving complaints.

When expectations are set properly, and the tool and policies deployed in a phased manner, DLP projects tend to go smoothly with minimal overhead.

When expectations are set properly, and the tool and policies deployed in a phased manner, DLP projects tend to go smoothly with minimal overhead. On average, a 10,000-employee organization with a handful of policies only requires 1-3 FTEs, usually split part-time under multiple employees, to manage policy violations. When basic policies are deployed, such as credit card protection, that same team may handle organizations up to 50,000 or more employees. On the other end, using poorly tuned or low threshold policies will require more incident managers, and one risk-averse organization purposely chose higher false positives for greater data visibility.

LESSON 4: **Poor identity management hinders good DLP**

One of the largest obstacles to a successful DLP deployment is poor identity management, especially in content discovery deployments. If you locate a file with sensitive data in an unapproved location, a poor directory infrastructure may make it nearly impossible to identify the file's owner. Without being able to identify the owner, protecting the file could break a legitimate business process. One health care organization reported that it might take it days to track down a single file's owner. Even though the DLP solution scans their infrastructure relatively quickly, the manual delays of tracking down users and managers (due to a haphazard Active Directory deployment) has dragged out their project by many months.

In another case, we received a report of an organization that almost fired the wrong employee when the IP address was tied back to the wrong user, due to a contractor improperly connecting their system.

LESSON 5: **False positives are a manageable concern**

The single most common worry over deploying DLP is the time required to manage false positives. The assumption is that policies based on keywords or generic 16-digit (credit card) numbers will constantly trigger false positives. But in real world deployments, users find false positives to be minimal as long as the right content analysis technique is used and policies are properly tuned.

For structured data, such as credit card and account numbers, most DLP tools have a range of advanced techniques to limit false positives. You can choose to only protect numbers from an internal database (instead of a generic expression), or set thresholds that alert only for multiple violations in a single document. For unstructured data, such as documents, DLP solutions use techniques such as partial document matching to alert only if a portion of a protected document (usually a few sentences) is found, as opposed to keywords.

One large financial institution reported much fewer false positives once they built DLP policies on their live databases. This same institution also highlighted the importance of real false positives vs. "false" false positives. "False" false positive happen when you alert on a real credit card number, but it isn't one you care about (such as an employee on Amazon). A mid-sized credit union reported that while they see some false positives, the vast majority are ones they want to see and evaluate.

LESSON 6: **Progressive deployments are most effective**

Nearly every organization we talked with reported deploying DLP in stages; starting with one component and policy, then slowly expanding. This allowed them to better understand the new technology, tune internal workflows and processes, and optimize policies.

Initial deployments tend to start as either network-centric or discovery-centric. With a network-centric deployment the organization starts with basic network monitoring, and then typically expands into email. Some organizations continue to expand into other network blocking, via gateway integration. In a discovery-centric deployment the organization starts with data-at-rest scanning, usually on servers and storage repositories, and then grows into endpoint scanning. This initial phase usually lasts one to two years (defined by budget cycles), then expands into the opposing channel or endpoint enforcement. We didn't find many DLP endpoint-centric initial deployments, perhaps because many organizations start with USB port blocking and encryption on the endpoint before moving into DLP.

Nearly every organization we talked with reported deploying DLP in stages; starting with one component and policy, then slowly expanding.

In all cases, organizations report finding it better to start with a narrow set of policies and then expanding once incident types and volumes are better understood. On average, DLP managers said it takes about three to six months to tune a new policy, depending on its complexity. Simple policies, such as protecting a single collection of documents, require very little tuning, but more complex policies take time to refine. The general rule is to deploy any policy in monitoring mode and tune it to meet business objectives before moving into active enforcement/blocking. User notification, education and disciplinary action during the monitoring phase materially lower violation counts and prepare the organization for potential business process impact.

LESSON 7: Endpoint DLP is still more limited than network or discovery

In network and discovery deployments, the DLP solution runs on high-powered, dedicated hardware. On the endpoint, the DLP agent must share resources with all the other cruft we load onto enterprise desktops and laptops. Thus, endpoint tools are more limited as to the type and number of policies they can run. Woe be on the DLP manager that attempts to load a policy containing the hashes for the entire customer database onto the sales team's laptop.

Not that endpoint DLP is unmanageable or too limited to be useful. Some tools communicate back to the central DLP server for content analysis when the system is on the same network. Since, in that situation, all email and network traffic are already monitored by the central server, only limited kinds of activities (like writes to USB drives) need to be offloaded. This also works well for endpoint discovery, where the local agent coordinates with the server for minimal impact. A few tools even support adaptive policies—where a smaller policy, such as a less-accurate regular expression, is only used when the endpoint can't see the DLP server. Yes, there will be more false positives, but remote activity can still be monitored and enforced.

Most DLP suite vendors started focusing more on the endpoint in 2008, but overall we see far less consistency across the different products than we do for network and discovery.

DLP ADVICE

Egress Filtering Made Easy

Data loss prevention technology is designed to mitigate the threat posed by data exfiltration on a network. Follow these four steps to lessen your risk:

ENSURE your DLP has access to any outbound connections that might originate from your transaction processing network, especially dedicated pipes that are not monitored by anything on the standard enterprise gateway

DON'T RESTRICT your DLP tool to only certain types of network traffic or only protocols running on standard ports. Attackers will use different combinations to move stolen data off your network.

COMBINE your DLP with a network proxy. This is crucial to properly manage egress filtering, enabling DLP to block as much as possible.

SET your DLP to alert when it detects encrypted files; this forces attackers to use non-standard encryption.›

–RICH MOGULL

Read the full text of this tip on SearchFinancialSecurity.com at http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1352298,00.html

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

LESSON 8: **Content discovery is hot**

A security manager for a group of casinos reported they decided to start with content discovery over network monitoring. "We want a full solution, but the largest benefit will be in discovery. We just want to know where everything is. It's breach avoidance."

When interviewing independent references, fully half of them stated they started with, or are considering, data at rest scanning before network monitoring. Of this group, reducing PCI compliance costs and risk is the single biggest driver. Using DLP content discovery, they can inventory their environment for sensitive data to protect, reduce audit costs, and cut down on unneeded data exposure. Reduced audit costs alone, over time, can sometimes offset the total cost of the DLP tool.

Across all of our interviews two key trends emerged. DLP is clearly a viable option for real-world data protection, and many see it forming the core of their data protection initiatives. It can identify where your data is located, where it's moving, and how it's being used. On the other hand, few organizations are deploying DLP to its full capabilities, and products aren't the magical panacea often presented in sales meetings.

Rich Mogull is founder of consultancy Securosis http://securosis.com/. 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

TABLE OF CONTENTS

EDITOR'S DESK

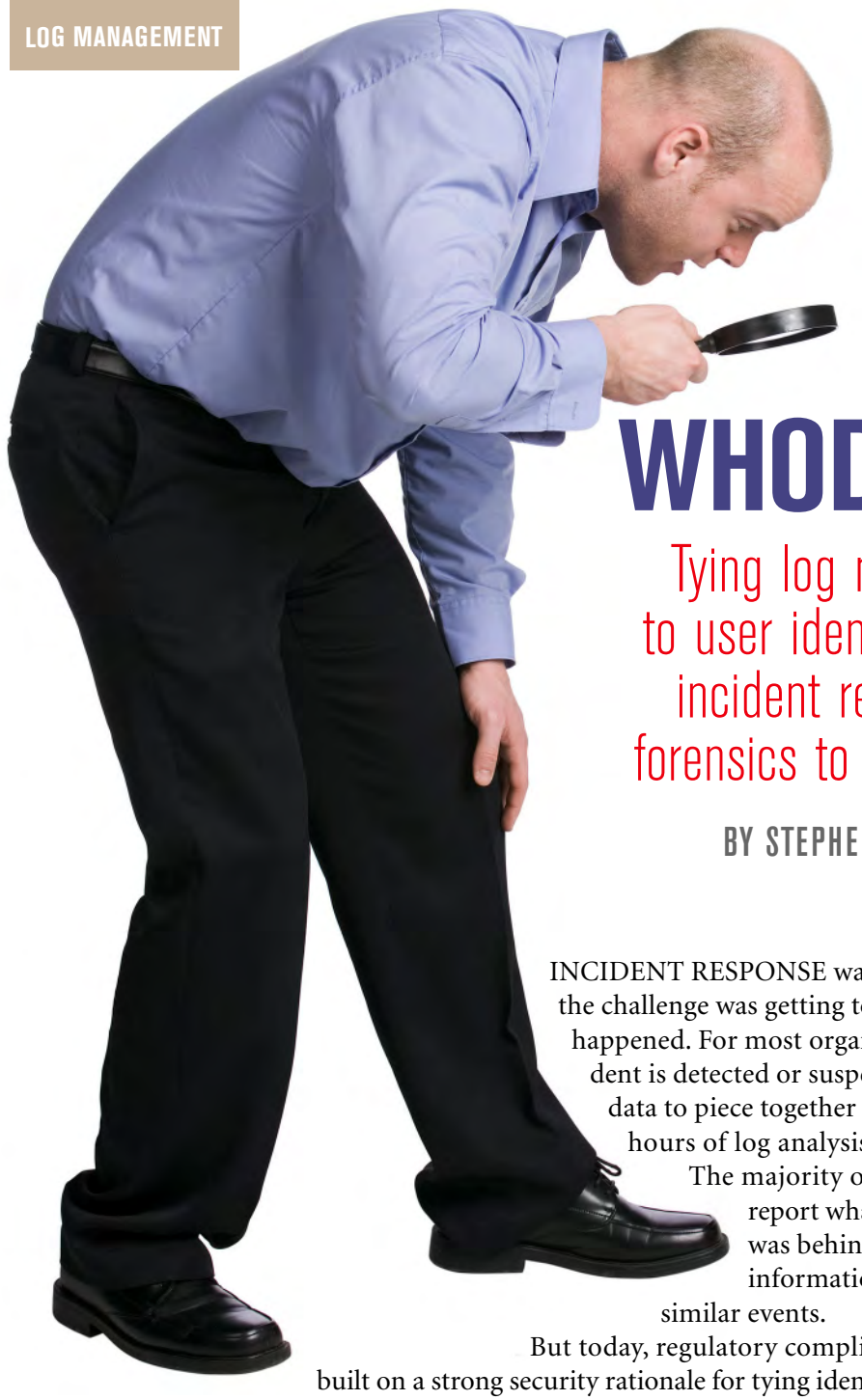
PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES



WHODUNIT?

Tying log management to user identities elevates incident response and forensics to a higher level.

BY STEPHEN NORTHCUTT

INCIDENT RESPONSE was tough enough when the challenge was getting to the bottom of *what* happened. For most organizations, when an incident is detected or suspected, gathering enough data to piece together what happened requires hours of log analysis. The reason is simple: The majority of security appliances report what happened, but not who was behind the activity, historical information about that system or similar events.

But today, regulatory compliance requirements are built on a strong security rationale for tying identity to activity. The reality is that compliance is driving organizations to do log management [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1274439,00.html], and tying identity to activity helps get budget. SOX, for example, calls for strict controls over access to financial records, and that means it's critical to spot unauthorized activity by human beings.

"Organizations that perform log analysis are constantly reacting to events on the network, while still trying to be proactive," says Ron Gula, CTO Tenable Security. "When logs are tied to user identities, if there is a critical event, the user (or likely user) of the event can be quickly identified." User identity is a critical piece of information that shortens the analysis decision cycle and helps eliminate unimportant issues or gives us a high confidence for the events we mark as actionable priorities. For example, he says, "you may have no idea how many login failures constitutes a probe, but if you were to graph all of the login failures by a user, you

may be able to spot patterns you didn't know you had to look for in the first place."

Knowing the "who" as well as the "what" is more than a benefit for investigators; it is absolutely essential to an organization's security and compliance programs. You need to know: Who gained unauthorized access to customer information databases? Who attempted to get root privileges on the domain server? Who cooked the financial records?

A classic compliance-related example of tying activity to identity comes from cases where the medical records of celebrities were improperly accessed. Some of these cases, such as Britney Spears' at UCLA Medical Center [13 employees improperly accessed her records in March 2008], get a lot of press . But professionals in the field report this is fairly common. The stolen information can be sold, not only to sensationalist tabloids as in the case of celebrities such as Spears, Maria Shriver and George Clooney, but also to insurance firms.

Needless to say, this has the potential to put medical institutions at risk of both lawsuits for breach of privacy or emotional distress, and HIPAA compliance violations. The Department of Health and Human Services has not done a good job of enforcing HIPAA compliance to date, but that's changing with the recent $2 million CVS fine [http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1330457,00.html] and the Obama Administration's emphasis on strong enforcement.

Tying user identity or activity is no easy task, but we're finally seeing the tools and developing the techniques that make tracking down the inadvertent or malicious offender.

Tracking Human Events

Why is tying identity to activity so difficult? At the heart of the problem is the "skinny" or "thin" event report (a term coined by Eric Fitzgerald of Microsoft). A computer, server or security appliance kicks out a report to syslog with the information it has at hand. It can't gather any other information about the event, state information, the person logged in and so forth. You're left with logs that typically report:

- Time and date of the event.
- IP Address or possibly hostname(s) involved.
- The program reporting the event.
- Severity. Common values are Fatal, Severe, Warning, Info, Debug, which are decided by the application and may or may not be accurate or useful.
- What happened from the reporting program's point of view.

Let's look at an example from Suhosin, a hardened version of the Hypertext Preprocessor (PHP) [http://www.hardened-php.net/suhosin/]:

Feb 24 09:56:43 [31321] ALERT - tried to register forbidden variable 'GLOBALS' through GET variables (attacker '41.204.211.204', file '/srv/www/live/sans/public_html/newsletters/risk/index.php')

Each of those fields is useful, necessary, but not sufficient. What is missing? To do a complete analysis, we generally need "fat" data—additional information that may not be available to the reporting program. Additional fields that are commonly

needed to create actionable information from event data include:

- When the event happened: Feb 24 09:56:43 Eastern time.
- Who initiated the activity: 41.204.211.204, according to nslookup, was assigned to webhost3.shadowrain.co.za at that time.
- Whether this is a stimulus or a response : It is a stimulus in this case, because webhost3 is initiating connections with www.sans.org.
- If the event we have collected is a response, have we identified the stimulus—or, in this case, since it was a stimulus, did we respond?
- What individuals and programs were involved? Ah there is the rub; we know the IP address, we know the machine name, but we have no idea *who* in South Africa is behind this activity.
- Did each event in the chain succeed or fail? This log entry is one of a series; webhost3 is probably running a scanner on www.sans.org. Hopefully, each of the probes fails.
- Has the event ended or is it ongoing? This probe has a start time and end time, so the event is over. We can only surmise that by looking at all the log entries from this IP address.

For years, putting the data together has been the responsibility of the security analyst. We flag an event in syslog because it has a key word we know indicates suspicious activity, such as "rejected," "dropped" or "denied." Then we take the information that we have from the syslog entry and begin to work backward and forward to find other related log events. Perhaps we have the IP address and need to consult the DHCP table to determine the host name and MAC address.

The high cost of manual correlation means many potential incidents are never investigated, and that means we fail to detect some events sometimes leading to devastating consequences.

Next, we might go to the system or domain controller event logs to determine who was logged on. Did they log on the first time they tried, or were there multiple attempts? Where did they log on from: Were they local, or was it a remote log on? This type of network forensics analysis is possible, but it takes a long time and a complete knowledge of where to get the information.

Each event may take between 30 minutes and several hours to run to ground, and the work is somewhat tedious, especially when we have to work with data on different time zones. The high cost of manual correlation means many potential incidents are never investigated, and that means we fail to detect some events sometimes leading to devastating consequences, Such as the spectacular Barings Bank and Societe General frauds *(see "Company Killers," p. 22)*.

On the other hand, if we can use software to collect this information and display it in a meaningful way, an analyst can make a pretty good decision as to the severity of a log event in a matter of seconds, and our ability to detect and respond to potentially harmful events improves dramatically.

The keys will lie in our analysts' ability to look for changes in user behavior or

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

attitude; report on segregation of duties, dual controls and access violations, and monitor activity and report on it. The good news is that we're getting the tools that are beginning to make this practical.

Tools Track Users

Since the stakes are so high and the need to tie identity to activity is so great, vendors are starting to deliver security solutions that can help. For instance, Sourcefire Real-time User Awareness (RUA) can be configured to send an alert any time a new user identity is detected, and this identity can be checked to see if it matches specific values.

Take the "Zippy" example. (This really happened. Though famous bank disasters are among the most serious account-related breaches, most security professionals with a couple of years of operational security experience have a security story involving a new, or modified account.) The company was a lab in which user

LESSONS LEARNED

Company Killers

Account abuse did banks in.

FAILURE TO DETECT and monitor new accounts or use of excessive privilege is a critical example of the need to tie activities to users and their roles. Consider these spectacular examples.

One such failure led to the 1995 demise of the venerable Barings Bank, the oldest merchant bank in the UK. Account 8888 had been set up to cover up a mistake made by another team member, which led to a loss of $20,000. That is bad, but it gets worse. Nick Leeson then used this account to cover his mounting losses as a day trader. When the smoke cleared, Leeson had lost $1.3 billion and ultimately destroyed the 233-year old bank. All of Leeson's supervisors resigned (under pressure) or were terminated.

Jerome Kerviel, a trader with the French Societe Generale bank, had access that allowed him to far exceed his authority in European stock index trades. He was able to make unauthorized transactions that led to a loss of somewhere in the neighborhood of 4.9 billion Euros (more than $7 billion US).

In 2006, Kerviel began a series of fake trades mixed with large real trades, some of which actually exceeded the bank's capitalization. Somehow, he avoided normal controls based on timing, and managed to keep winning, and losing, trades in balance to give the appearance of insignificant impact to the bottom line. A number of DLP-friendly tools as well as simple scripts can help us detect new accounts.›

–STEPHEN NORTHCUTT

Focused on finance?

Introducing SearchFinancialSecurity.com!

Now there's an online resource tailored specifically to the distinct challenges faced by security pros in the financial sector. *Information Security* magazine's sister site is the Web's most targeted information resource to feature FREE access to unbiased product reviews, webcasts, white papers, breaking industry news updated daily, targeted search engine powered by Google, and so much more.

Activate your FREE membership today and benefit from security-specific financial expertise focused on:

- Regulations and compliance
- Management strategies
- Business process security
- Security-financial technologies
- And more

www.SearchFinancialSecurity.com

SearchFinancialSecurity.com

The Web's best information resource for security pros in the financial sector.

names were created from the first letter of the first name and the first six letters of the last name. A new account log entry for "zippy" caught our attention immediately. Either we had an employee named Zeke Ippy or we had a problem.

If we had a list of all users, we could examine zippy to see if any user had a first name starting with "Z" and a last name with the string "Ippy." This can be done with a home-grown script using regular expressions, but over time, we're seeing vendors deliver more regular-expression capability so that tools can be configured to support business logic.

Security architects can now depend on one or more of logging and analysis industry tools that can deliver "fat" data that tie user ID and other related information to event logs. These tools include:

- Security information event managers (SIEMs).
- Log management devices, which are primarily collectors of log files.

DECISIONS

Caveat Analyst

Your conclusions are only as good as your data.

ANY DATA MODELING professional will quickly warn you that referential data is powerful and helpful to analyze and classify an event, but only if that information is correct and is correlated correctly. If you visualize yourself as the analyst making a decision on how to classify an event, then you can clearly see that if these types of fields are misleading or wrong, you could arrive at the wrong conclusion. As an example, if you were an analyst for a university investigating a log event:

Feb 25 02:55:19 [16934] ALERT - configured request variable name length limit exceeded - dropped variable '___df9d5760ba1af926bed589c89//modules/My_eGallery/index_php?basepath' (attacker '10.12.82.4', file '/srv/www/live/college/public_html/new/CS423/grades/display.php'

The login information for IP address '10.12.82.4' yielded a student name of John Brown, and the event history showed past warnings for hacking-type behavior. One might immediately leap to a conclusion that the event was hacking-related and John Brown was at it again. However, if any of that information was wrong, or correlated incorrectly, we might accuse John unfairly. What if John had plugged a wireless access point to the network connector in his dorm room and another student was using it while attempting to access the grades for his class? In fact, still another piece of referential data showed that John Brown was not even enrolled in CS 423. Why would you hack the grade server to change your grade for a class you aren't taking?

–STEPHEN NORTHCUTT

- Centralized consoles that offer a number of additional capabilities, not just logging and analysis. For example, Tenable and Sourcefire have several security products, which report in to central consoles and strive to deliver fat data.

These products receive the thin events and create fat data for analysis. As the vendors continue to add functionality, these product categories tend to overlap and are less defined than they were a couple of years ago. SIEMs, for example are now emphasizing their log management capabilities (or spinning off separate products) to capitalize on compliance-driven market demand. And some log management products are developing more SIEM-like capabilities.

The flow goes like this. An event occurs and a thin log file describing the event is created and sent to a collector. (A site may have one or more collectors.) The collector may store it as a raw, unaltered, pre-normalization event. The log event may also be stored with a matching cryptographic hash to prove it has not been tampered with.

The rules may be based on regular expression technology to parse raw events, but sophisticated products normalize the logs.

If the site wants to do more than simply store the log, a copy of the log event is sent to an analysis engine. The log event can be evaluated by rules that are designed to either confirm and record normal events, or designed to detect abnormal or bad events.

The rules may be based on regular expression technology to parse raw events, but sophisticated products normalize the logs. Normalizing breaks down raw data into component standardized fields that are stored in a database, so we may be able to correlate it with other information. Examples of the types of fields we might see in an event database include day of week, hour of day, ID, UTC time, local time, time zone, PID, OS name, OS version, application version, host name, host IP, host domain name, MAC address, application reason and severity type.

Once the data is normalized and in a database, our tools create a fat event by adding other referential data such as: the history of that IP address/MAC address/system name; related vulnerability scan information; history of similar event sand login, identity or access data. This level of information will help the analyst make an informed decision much faster. One warning note: Information isn't always what it seems, so don't leap to obvious conclusions about what the data appears to be telling you *(see "Caveat Analyst," p. 24)*.

Since referential data is important, organizations that take log analysis seriously want as much of it as they can get. One useful tool is the passive sniffer. These tools are typically placed near aggregation points such as the firewall and listen to and analyze the traffic passing by. They are able to determine what operating systems are associated with particular addresses. They also can determine the version of software that is running. This is a huge step up from the basic firewall log of port and IP address. In addition, they can pinpoint the existence of vulnerabilities. Because they are creating their referential state tables by listening to traffic, they are more current than static network inventory tables that are manually updated.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

There is an open-source example called P0f [http://lcamtuf.coredump.cx/p0f.shtml], and Sourcefire and Tenable Security have commercial products—Sourcefire Real-time Network Awareness (RNA) and Tenable Passive Vulnerability Scanner. Both companies offer a central console, sort of a mini-SIEM, to collect and manage the event data their various products create. Identifying the event in syslog and querying these vendor consoles is still a manual process, but it's a huge step up from everything being manual.

With sophisticated SIEMs, it is becoming increasingly possible to tie thin events to an identity in useful ways. It's been difficult to do previously because the average person has multiple accounts—email, Windows, VPN, intranet, app-specific IDs, IM, etc. While a SIEM can collect activity across these accounts, we must associate all of these accounts to a single person for the data to be actionable. Using ArcSight ESM, for example, an analyst selects one account ID as the user's unique ID. Then it is possible to map all the other accounts for that user to the unique ID. SIEMs such as ESM use several methods to connect log activity to identity, including agents and sending native operating system credentials.

One exciting capability of tying identity to activity is to use historical activity data into ArcSight's activity profiling technology to generate statistical patterns and create new rules.

The only way to detect changes in behavior with technical controls is to tie identity to activity over a long enough period of time to establish a baseline. What if the amount of Web connection time to social media such as Twitter and Facebook [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349703,00.html] suddenly increases? It might indicate that user is wasting time instead of working. Or, a major increase in time on LinkedIn might indicate establishing connections in advance of leaving the current organization. However, there is no way to detect an increase if we do not have a baseline.

You can expect a SIEM that supports identity to activity mapping to be able to integrate with Active Directory or Network Directory. This means in addition to the accounts, you also get group or role information. Even though organizations have been slow to implement network access control (NAC) [http://searchmidmarketsecurity.techtarget.com/tip/0,289483,sid198_gci1351628,00.html] at the enterprise level, the capability is built in to more and more software and appliances and it is starting to happen.

One exciting capability of tying identity to activity is to use historical activity data into ArcSight's activity profiling technology to generate statistical patterns and create new rules. For example, you might run the activity of the last 50 people who quit to compare and contrast their activities to those who haven't quit. When that activity is spotted again, you can auto-escalate a watchlist and make sure the person doesn't leave with data.

Or, in a down economy, if you have to announce that your organization can't

issue bonuses one year, you might profile the activity of users before the announcement compared to after the announcement. A recent study by The Ponemon Institute (sponsored by Symantec) interviewed 945 U.S. adults who had been laid-off, fired, or changed jobs within the last year and found that more than half took company information with them when they left [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1348948,00.html].

The rationale for taking the data included help getting another job, help starting their own business, or simple revenge. All of the participants in the survey had access to proprietary information, including customer data, employee information, financial reports, software tools and confidential business documents. The survey also found that just 15 percent of the companies examined the paper and/or electronic documents their former employees took with them when they left."

The Payoff

Every organization struggles with the amount of effort it takes to get real benefit from log file analysis. Obviously. one big win is compliance. Most regulatory bodies either require or strongly suggest log monitoring. The Consensus Audit Guidelines [www.sans.org/cag] specifically refers to the importance of tying identity to activity. Two examples are enforcing controls on dormant accounts and continuously evaluating need to know. In both cases, you have to know who the user is and what his role should be.

With log monitoring, nothing succeeds like success. Think of the value of an analyst who takes the time to run a suspicious event into the ground and finds something significant, such as an employee collecting a list of customer personally identifiable information and sending it to his Hotmail account. The damage can be minimized by rapid detection and response. Logging, which is usually considered dull and boring work, becomes exciting.

That is really one of the biggest benefits of tying identity to activity. Hits on the firewall, spam messages dropped, error conditions in a program, the amount of free disk space, are all important, of course. Humans, though, do the craziest things, and when you add the human part of the equation to log events, it is a whole new ball game. It wouldn't be surprising if the next few years yield a number of exciting security detection techniques as we correlate identity and get better at creating fat events for analysts to review.

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a post graduate level IT Security College. He is author/coauthor of Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security 2nd Edition, IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials *and* Network Intrusion Detection 3rd edition. *Send comments on this article to feedback@infosecuritymag.com.*

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

the academy

pro

www.theacademypro.com

home

www.theacademyhome.com

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

The Academy has gone one step further by creating The Academy Home to show the average home user how to protect themselves from threats on the Internet by providing videos on today's best end user security products.

Check out The Academy websites at www.theacademypro.com and www.theacademyhome.com today. You'll be glad you did.

Sponsored by

CORE IMPACT
GIGAMON
PANDA SECURITY
SOURCEfire
McAfee
SANS
exinda networks
Network Critical
cisco
SAINT
astaro
Check Point SOFTWARE TECHNOLOGIES LTD.
TENABLE Network Security
Nessus
GFI
peer1 Fully scalable hosting solutions
Shavlik Simply Secure.

TABLE OF CONTENTS

EDITOR'S DESK

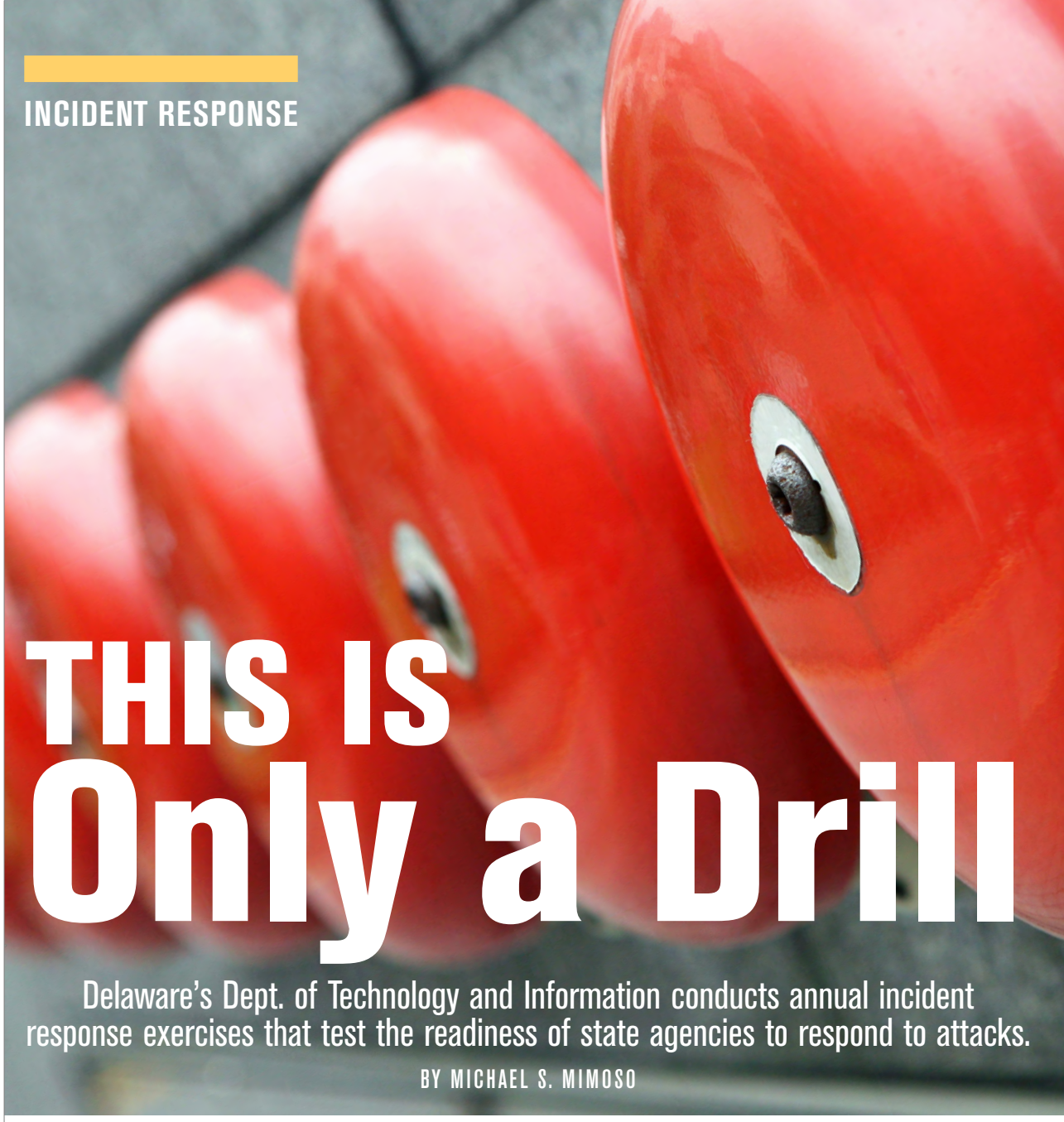
PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES



THIS IS Only a Drill

Delaware's Dept. of Technology and Information conducts annual incident response exercises that test the readiness of state agencies to respond to attacks.

BY MICHAEL S. MIMOSO

IF YOU'RE AN NFL FAN IN APRIL, you're well familiar with mock drafts. These pretend exercises portend to make a best guess at whom your favorite football franchise will select on Draft Day. Granted, while teams may be worth hundreds of millions of dollars, the NFL isn't playing the same high-stakes game as the federal and state governments.

So when a state such as Delaware calls all hands on deck for a mock exercise simulating a coordinated attack on information systems and communications, there's more at stake than who will be taking snaps for the next 10 seasons. Lives, critical infrastructure and national security are on the line.

Delaware's Dept. of Technology and Information (DTI) [http://dti.delaware.gov/] had conducted tabletop incident response exercises since 2005 to great results. Year after year, new insight was gained into technology and processes that weren't up to speed or needed a tweak. But the tabletop format was losing steam and organizers feared what had long been an effective evaluation tool would lose its value. IT people in particular aren't engaged for long without the ability to bang on a keyboard, write scripts and see measurable results. That was incentive enough for the state last year to add a hands-on aspect to the drill.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

"It's good to simulate attacks on the state's information resources so folks in various capacities of state government can play along and talk about response and what things we can put in place to perhaps prevent an attack from happening altogether," says the state's chief security officer Elayne Starkey. "It's good to practice—for the same reason you have fire drills."

PLANNING EVERY STEP OF THE WAY

Delaware's exercise is anything but fire drill. To the contrary, it takes six months to plan, and involves 125 people from federal and state agencies, including IT managers, law enforcement, the FBI and academics. Disaster recovery coordinator Lisa Wragg is the project manager who drafts the exercise's objectives, organizes a steering committee that reviews and approves those objectives, and then, using the Homeland Security Exercise and Evaluation Program (HSEEP) [https://hseep.dhs.gov/pages/1001_HSEEP7.aspx] as a model, plans out the sequence of events and milestones that must be met along the way.

Delaware's exercise is anything but fire drill. To the contrary, it takes six months to plan the exercise, which involves 125 people from federal and state agencies, including IT managers, law enforcement, the FBI and academics.

There are four preliminary meetings under the HSEEP model: a concepts and objectives meeting where the exercise objectives are mapped out and where the decision to include a functional, hands-on component was made; an initial planning conference where the concepts and objectives are finalized and approved, the venue is approved and participants selected; a midpoint planning conference where the sequence of events is established; and a final planning conference, where the review of the day's scenario and logistics is approved. The steering committee is a partner at each milestone, and that was made up of the state's high tech crimes unit, state police and the Delaware Emergency Management Agency.

"You have to create a scenario and put together an outline of the day's events. People need to have a reason why things are happening," Wragg says, adding that she used many of the lessons learned in DTI's three previous exercises to build this one.

"If you just throw people in a room and just start hacking them and not have a story to go by or understand why something is happening, it's kind of meaningless to them," Wragg says.

Last October's scenario had a timely script. Held a week before the presidential election, the plot involved a cyberattack by the fictional country of Dystopia on state agency websites, networks and states' voting infrastructure. The plot was hammered out months earlier, and reinforced last summer when attacks on the country of Georgia's state-run websites [http://itknowledgeexchange.techtarget.com/security-bytes/russian-cyberwar-yes-no-maybe-so/] were conducted prior to physical conflict during its war with Russia.

"That drove home the possibility of what could happen," Wragg says. "We needed to prepare for it. We needed the scenario to be a terror attack this time."

SIMULATED ATTACKS, REAL RESPONSES

Starkey says the attack scenarios are kept close to the vest with fewer than 10 people knowing what's about to take place. The added dimension of this exercise being a terrorist attack on the voting infrastructure required some careful treading. Starkey did not want to leave the impression on any of the participants—including the National Guard, Air Force, school districts, state police, FBI, Dept. of Transportation, Dept. of Labor, in addition to DTI—that the state's election system was vulnerable.

All of the players were present at the DTI emergency operations center on Oct. 29 for the exercise, and in her opening remarks, Starkey laid out the day's high-level goals: prevent cyberattacks, sharpen response procedures and recovery.

"One thing that was important to us, was that when we start the exercises, that we create an environment of trust, take away the threatening feeling in the room—dispel that right away," Starkey says. "In my opening comments, I stressed this was

STRATEGY

Three Keys To Success

UNDERSTAND THE THREAT LANDSCAPE AND PLAN YOUR TABLETOP EXERCISES ACCORDINGLY.

Motivated attackers are going to penetrate even the most ardent defenses. Companies that realize that this is the information security environment of 2009, are the ones realizing the need to run through functional and tabletop incident response exercises such as the one conducted by the Delaware DTI.

Lenny Zeltser, an incident handler with the SANS Internet Storm Center, says even enterprises with mature security practices find great value in these mock exercises. He defines three keys to success:

#1 **DEFINE YOUR SUCCESS CRITERIA.** "You need to define what it means to do well," Zeltser says. Have you responded to an incident within 30 minutes, and have a good sense for the scope of an attack either hours later? Or maybe you define success as learning within a pre-determined period of time what data was affected and whether the right people were notified and put in position to make decisions.

#2 **INVOLVE THE RIGHT PEOPLE.** "It's too easy to operate in a silo," Zeltser says. You might be one of 10 teams responding to an incident, and those nine other teams won't prioritize security the way you do. "That means you may have to have power or authority or good will to get them involved."

#3 **EVOLVE YOUR EXERCISE.** "Don't run through the same exercise every year," Zeltser says. Your incident response exercise should evolve just as your business changes, the economy grows or shrinks and security priorities change. ›

—MICHAEL S. MIMOSO

Security Topics Tailored to Your Needs

You rely on *Information Security* magazine every month for original, in-depth information and analysis on the security of your enterprise. But as you know, to secure your data and network you need to be well informed every day. Stop scouring the web; become a member of SearchSecurity.com and receive tailored messaging delivered right to your inbox with the latest news, current threats, expert advice, white papers, webcasts, and much more on the security topics that YOU select including:

Network Security
Intrusion Defense
Identity and Access Management
Email Security
Web Security
Current Threats
Application Security
Compliance
Security Management
Platform Security

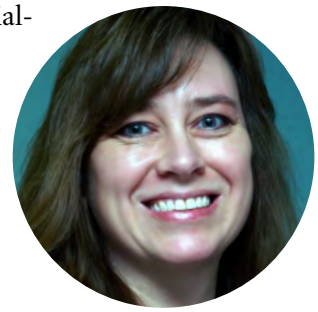
Stay informed 24/7. Activate your free SearchSecurity.com membership at www.SearchSecurity.com/join today.

SearchSecurity.com
The Web's best security-specific information resource for enterprise IT professionals

not real. I wanted them to feel like this is safe haven, and that we understood they were all at different points of readiness."

"Don't feel badly about not having a policy in place that you should, or a procedure not defined completely. This is the place to kick all that around," Starkey adds. "One of my key objectives is for them to leave that day with a little to-do list of things they want to take care of in the weeks after the exercise. We want them to each year to go away with ideas of things to do to strengthen their infrastructures, and to improve their ability to respond and recover from an attack like this."

At an appointed time, programmers and network security engineers began releasing attack scripts against websites that were built in a development environment and set up on a segmented network. Responders in the EOC would need to recognize problems with a site such as defacements or denial-of-service attacks and take appropriate countermeasures, which were evaluated.



"It was like a little NASA—rows and rows of computers, screens up on a big wall where the participants were sitting, and behind the glass was exercise control where the injects and scripts were released," Wragg says.

Website defacements were the first wave of attacks, launched against the home pages of various state agencies. As word spread of the attacks, other agencies began to take measures to harden their Web apps to avoid being taken down as well. Several, Starkey and Wragg said, beat attackers to the punch.

"It was like a little NASA—rows and rows of computers, screens up on a big wall where the participants were sitting, and behind the glass was exercise control where the injects and scripts were released."

–LISA WRAGG ,
Disaster recovery coordinator, state of Delaware

"That was incredibly motivating to the other agencies," Starkey says. "We highlighted it in one of the breaks and congratulated them on the good work they did."

In another room adjacent to the EOC, a tabletop-style scenario was set up where people of similar function would work together. The service desk was also there taking incoming calls for trouble tickets. As soon as the attacks happened, calls flooded the service desk. High Tech Crimes officials were at one station, and working with law enforcement, they quickly began tracing the source of the attacks. Meanwhile, the state's Joint Information Center (JIC), which included public information officers from different state agencies, were at another putting out coordinated media releases and crafting appropriate public responses, alerting citizens that they should take caution using agency websites.

"It was pretty cool and interactive," Wragg says.

Once that segment of the exercise was complete, the DTI held a quick briefing on the importance of preserving evidence. Admins are initially more concerned with the availability of systems and getting them back online, but in this instance, they had to

tread lightly to preserve the integrity of the scene and assist in tracking the source of the attacks. The participants were also evaluated on how well they used the state's incident command system, prescribed by the federal government. The framework is built for emergency management agencies and represents a set of standard response procedures.

The next wave of the attack involved more website attacks, this time the target was sensitive personal data. Simulated FBI warnings were sent out that terrorists had launched cyberattacks against critical infrastructure, and soon thereafter, calls began flooding the service desk with citizens reporting possible identity theft after accessing services on state agency websites. The response involved assessing the cause of the breaches and reviewing data protection procedures. JIC also worked up statements directing citizens how to protect themselves online, and if necessary, report incidents to police.

The final phase of the exercise combined another hack with a physical attack. Denial-of-service attacks were launched against agencies' sites and services, while simultaneously terrorists were disabling lines used by service providers statewide. The offshoot was that these attacks could possibly impair the state's ability to vote in the upcoming elections. Steps were taken to rapidly move critical infrastructure to redundant facilities and keep services available until the service providers to could complete repairs.

LESSONS

Things to Remember

LISA WRAGG, DISASTER RECOVERY COORDINATOR FOR THE DELAWARE DTI, WAS THE PROJECT MANAGER FOR LAST YEAR'S INCIDENT RESPONSE EXERCISE. SHE LAYS OUT SEVEN LESSONS LEARNED.

1. Assign a project planner.
2. Secure an executive sponsor; CSO Elayne Starkey was her sponsor.
3. Follow a master event list and build your scenario around that list.
4. Stick to your scenario; what look like minor changes could have a big impact down the line.
5. Outline the details of your scenario, including attack scripts.
6. Address current threats in your scenario.
7. Get an outside agency to assess how you do; SunGard's Incident Management Exercise Service did DTI's assessment.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

"The exercise creates a lot of interest in updating plans and going back and checking websites, making sure they're up to date and patched," Wragg says. "There is a lot of after-exercise activity. People want to do something."

MEASURABLE METRICS AND REVIEWS

Being the fourth such exercise, many of DTI's incident response processes are mature. Media and external communication are solid, Starkey and Wragg note, while adding that internal communication between agencies is an ongoing process.

"If we're looking for measurable stuff, some agencies quite frankly need help, and we're going to help them," Starkey says. "Quite frankly, I don't think we would have been able to identify who needed more help than others until we did the exercise."

Starkey says the agencies did well against the four stated objectives. All agencies identified vulnerabilities in their infrastructure leaving them susceptible to Web-based attacks. Each agency had a prescribed process for defending against attacks and rolled out those processes accordingly. Each addressed the preservation of evidence, with different levels of maturity in their respective processes. This was an area Starkey says ongoing education will be key going forward.

Business continuity [http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1330538,00.html] is also another area DTI will concentrate on going forward. The coordinated physical and cyberattack that played out in the final phase of the exercise stressed the importance of a continuity plan for critical services such as voting that must continue seamlessly should a key state network fail.

"Quite frankly, I don't think we would have been able to identify who needed more help than others until we did the exercise."

–ELAYNE STARKEY, CSO, state of Delaware

Breach notification was the final goal that each agency met with flying colors, much to Starkey's satisfaction since each agency information security officer was, in advance, given a procedure to follow on notification. Service desks were overwhelmed with calls; an indication the procedure was being followed.

In the end, Starkey says adding the functional component was definitely a game-winning touchdown, and that last year's participants would never go back to just a tabletop exercise.

"We have a catchphrase about this being a journey to compliance," Starkey says. "I recognize we're not there, we're not at 100 percent compliance across the board. We do see everyone moving different rates."

"If you look at the write-up after first year's exercise, the objectives were fundamental about increasing customers' awareness that cybersecurity was important. We've made incredible strides there to get them to pay attention, let alone comply with a 41-page security policy."

Michael S. Mimoso is Editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

REAL-WORLD DLP IMPLEMENTATIONS

LOG AND IDENTITY MANAGEMENT

TABLETOP EXERCISE

SPONSOR RESOURCES

ADVERTISING INDEX

the Academy 28
www.theacademy.ca
- Free infosec videos for security professionals from network admin to director of IT.
- Free information security videos for home users/end users.

Guardium 2
www.guardium.com
- Expert Podcast: Integrating DLP into the network infrastructure
- DLP: Enterprise Tools and Strategies

ISACA 4
www.isaca.org

RSA Conference 11
http://www.rsaconference.com

SearchFinancialSecurity.com 23
www.SearchFinancialSecurity.com

SearchSecurity.com 32
www.SearchSecurity.com/join

SystemExperts 18
www.systemexperts.com

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.