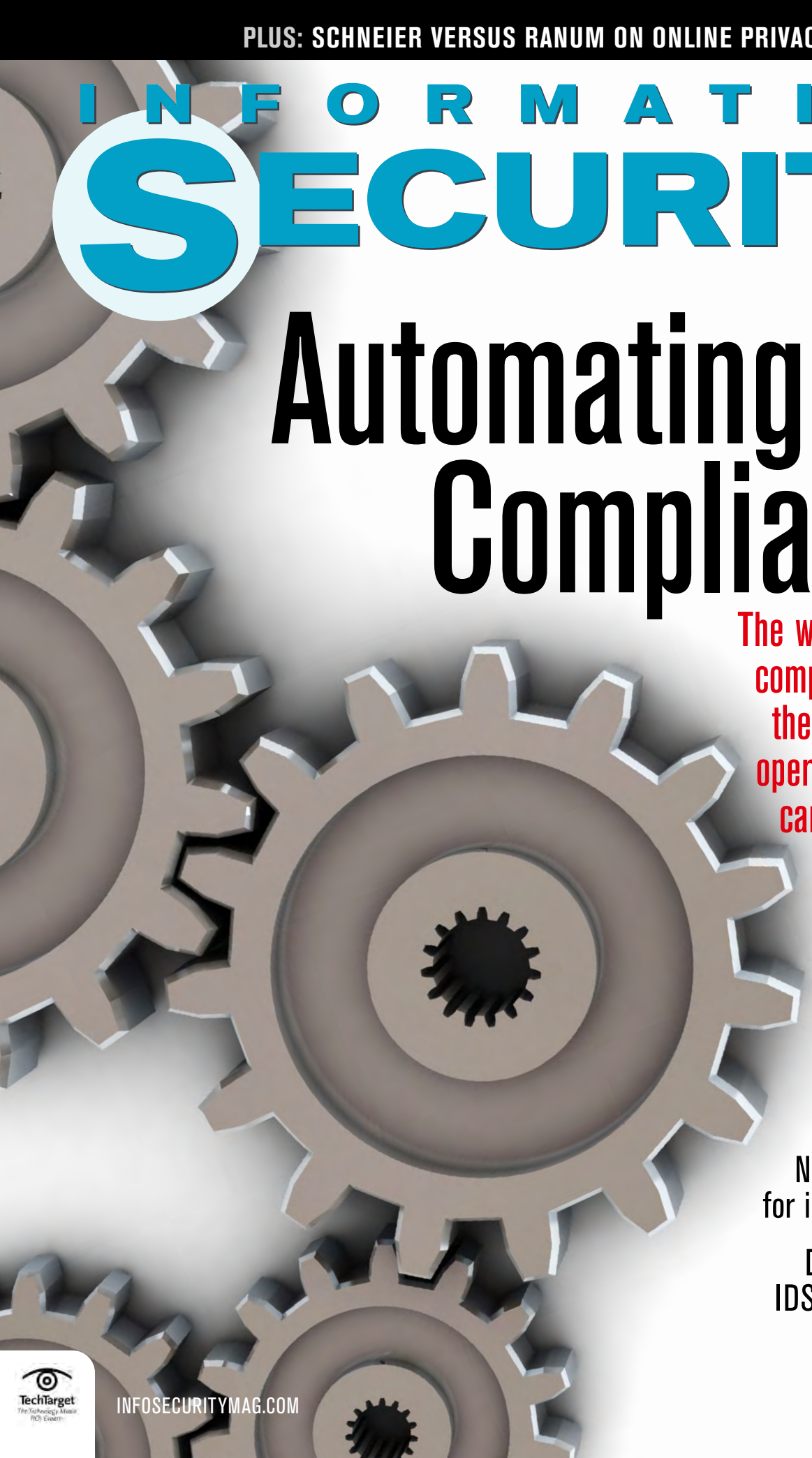
PLUS: SCHNEIER VERSUS RANUM ON ONLINE PRIVACY

INFORMATION SECURITY®

MAY 2009

Automating Compliance

The weight of regulatory compliance can break the back of your IT operation. Automation can help you gear up for your next audit.



ALSO:

New technologies for identity and access

Do you need an IDS, an IPS or both?

TechTarget

INFOSECURITYMAG.COM

contents

MAY 2009

VOLUME 11 NUMBER 5

FEATURES

ALSO

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

The Pipe Dream of No More Free Bugs

BY MICHAEL S. MIMOSO

Security researchers have declared they want vendors to compensate them for their independent search for vulnerabilities.

NO MORE FREE BUGS is the new security researcher credo. A few high-profile bug hunters have decided gratis is a goner and they're not giving away their work for nothin' no more. Vendors such as Apple, Oracle and Microsoft can find their own browser bugs and buffer overflows. These guys are taking their keyboards and fuzzers and are going home.

The reason for the change in attitude is apparently twofold: 1) Bugs are hard to find. What used to take a couple of hours of spare time to find now takes a weekend—or a week, or a month; and 2) yesterday's young bug-finder is today's adult complete with spouses, kids, mortgages and bills to pay. They're not going to be satisfied with a tip-of-the-cap mention in the Patch Tuesday bulletin any more.

Gratis is a goner.

The revolution began at the CanSecWest conference in March in Vancouver where Charlie Miller won the Pwn2Own contest for the second consecutive year, and was paid $5K for the bugs he used to crack a fully patched MacBook. Shortly thereafter, Miller, Dino Dai Zovi, another Apple bug-hunter, and Alex Sotirov, a prolific Windows breaker, held up a modest cardboard sign bearing Miller's declaration of No More Free Bugs. And it was on.

> "How important is it to them that their products and users be secure? If they think it's important, then they should consider giving me compensation."
>
> –CHARLIE MILLER, security researcher

They told attendees they want to get paid for work they're doing. Big software vendors such as the above-mentioned Apple, Oracle and Microsoft, who happen to employ very expensive security researchers of their own to ferret out bad code and patch problems before they reach the customer, are benefitting from free QA testing from these guys. Those days are over, they say.

Well, fine. But here's a question or two: Who is asking you guys to mess around with Windows, Mac OS X or Oracle DB? And while we're at it, why should the vendors pay you for work they did not contract you to do?

I talked to Charlie Miller and asked him that very question. I also asked him about critics who equate No More Free Bugs and demands for payment to extortion (I believe extortion is a ridiculous extreme in this case, considering the individuals involved and their motivations).

Miller concedes the point that bug finders aren't hired guns and emphasized he'd never blackmail a vendor with a bug he'd found.

"Regardless, I have piece of information that makes their product and their users more secure," Miller says. "How important is it to them that their products and users be secure? If they think it's important, then they should consider giving me compensation. They're more than free to have their security guys look for the same bug, so be it. They're under

no obligation compensate, and we are under no obligation to give them the bug."

"What we really want is there to be some way researchers are compensated for important security vulnerabilities—something that affects millions of users," Miller says.

Miller outlines a scenario he'd like to see where CERT or some other organization, supported by government and/or vendors, pay researchers. "Microsoft is paying an obscene amount of money ($250,000) for information about the author of Conficker. I think they can pay a million dollars toward a fund for researchers. Likewise for Apple, Oracle and others."

There's also talk of starting up a website where researchers would be able to report bugs that have been reported to vendors. Miller says the bugs would be verified and then posted to a feed that would illuminate the lag between disclosure and a fix.

Miller insists this isn't about disclosure, and shoos away the argument that sitting on a bug does more harm than good, countering with the thought that if there were compensation at the end of the bug-finding rainbow, he'd be more motivated to look for them.

TippingPoint's Zero-Day Initiative (ZDI) and VeriSign's iDefense Vulnerability Contribution Program (VCP) already offer payment for vulnerabilities. Bugs reported to these programs are disclosed to the affected vendors and details are shared with customers. Payment amounts are not disclosed because contributors are asked to sign non-disclosure agreements promising not to reveal the rewards. Ironically, ZDI sponsors Pwn2Own and has handed Miller a pair of cash awards for his efforts, despite Miller's general disagreement with ZDI.

> "I'd be completely shocked if it ever happens. Vendors are happy with the status quo; everyone is happy except us."
>
> –CHARLIE MILLER, security researcher

"Their motivation in buying vulnerabilities is making their research of vulnerabilities easier so they can write more signatures for the IDS they sell," Miller says. "It doesn't matter to them how critical a bug is, they still have to make a signature for it. If you're Microsoft or Cisco, and I have a vulnerability that would let me write the next Conficker, (ZDI) wouldn't have the same interest the vendors would have, which would be to keep their customers safe. I love that they pay researchers, but it's probably not the best solution."

At the end of the day, Miller, Dai Zovi, Sotirov and anyone else standing behind the cardboard placard of No More Free Bugs aren't likely to start getting paid now, since they've never been before. And Miller understands this genie isn't going back into the bottle.

"I don't blame companies for not paying us. If I were getting free food from somewhere, I would never buy food again. It's the same with researchers and free bugs," Miller says. "We need to stop giving them information for free."

"I'd be completely shocked if it ever happens. Vendors are happy with the status quo; everyone is happy except us," Miller says. "No one is motivated to change except for us. The only thing we can do is hold back. Are we going to change things? We're going to do what we can do."

Michael S. Mimoso is Editor of Information Security. *Send comments on this column 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.

VIEWPOINT

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

The Merits of SAS 70

David Mortman's "Bad Things Come in Threes" (Perspectives, March 2009) makes a lot of good points on how to understand security controls at service providers, and to be careful on what they give you as proof that they have good security. There are several tools, seals, and reports that service providers use to market themselves as having good security controls.

David seemed to pick on the SAS 70, and I disagree with his statements. He mentions a SAS 70 is a financial controls audit, and you should be interested in them only if you are concerned with a vendor's financial controls. When SAS No. 70 was released by the AICPA in the early '90s, it was designed to be a tool for financial statement auditors needing assurance on a service organization's system of internal control to meet SAS 55 requirements.

Over the past decade, uses of the SAS 70 report have changed and SAS 70s have migrated to be used in non-traditional ways. David gave us one example, compliance with Gramm-Leach-Bliley Act (GLBA). There are many other examples.

For years, companies have been obtaining SAS 70s for uses outside of the financial controls area. For example, a SAS 70 is commonly requested when a service organization is processing highly sensitive transactions on behalf of its clients and need to provide assurance on the confidentiality and integrity of its customers' data. Application service providers (ASPs) are also providing assurance via SAS 70 report, not only on the functionality of their application but the security over it as well. Today, most SAS 70s are more focused on information systems and commonly include control objectives for information security. In 2001, SAS 94 was released that amended SAS 55, requiring auditors obtain knowledge of a company's system of internal control related to information systems. This amendment further boosted the need for SAS 70s to include IT.

He is right that a SAS 70 review is not a security audit. It was never designed to be a security audit, rather a tool to provide assurance on internal control systems including but not limited to financial controls. Nevertheless, you cannot discount the value provided by SAS 70s. You can pick up any SAS 70 report issued today and the majority of the report will describe the controls and tests of controls related to information systems areas, including information security.

David is right, the SAS 70 should not be the only source of security assurance, but it can be very valuable if your service organization (vendor) designs their report to include descriptions and tests of security controls that you rely upon. It is true that SAS 70s may not

CONTINUED ON NEXT PAGE

COMING IN JUNE

Risk Methodology

Too many organizations are comfortable allowing vendor marketing and compliance demands guide the direction of their security programs. In turn, little regard is given to analyzing risk specific to a business and then designing systems and writing policies accordingly. This feature looks at a homegrown risk assessment methodology currently in use at the University of Washington and walks you through the steps in detail necessary to identify, evaluate and mitigate risk.

Physical-Logical Convergence

Many companies are realizing their physical and IT security teams can no longer work in silos. Charged with the similar task of protecting access to assets, companies are finding ways to merge operations around access to physical and digital assets. It's not an easy journey, as you'll learn in this feature. Experts and security professionals will provide details on the benefits and challenges of this growing trend.

What's Next for SIMs

In this feature, we'll talk to users on the front lines about their current SIM implementations and take a look into what the future holds for the next-generation SIM products. How are companies leveraging SIMs to increase efficiency and cost savings in their security programs? How will future versions of SIM help companies make the most of these tools?

CONTINUED FROM PREVIOUS PAGE

give a complete picture of information security controls and other "proof of security" may be needed to meet your requirements. You actually have to read the SAS 70 report to determine which control objectives and tests of controls were included in the review. You might be surprised.

–Clint Jennings, CPA, CISA, CISSP, CGEIT,
Assistant Vice President – Internal Audit,
HCA - Hospital Corporation of America

Final Words on Digital INFORMATION SECURITY

I was saddened to see *Information Security* will no longer send printed copies to its subscribers. What saddens me most is that I will not longer have an opportunity to read your magazine unless I print it out. Much of my day is spent in front of a computer or working with them. The last thing I want to do when I go home is spend more time at a computer. Magazines and journals are saved for when I have the opportunity to read them.

Printing your magazine defeats the purpose you are trying to accomplish, saving our environment.

–Steven Yarmush, Operations/technology manager,
Berks Community Federal Credit Union

How sad it is to see a great magazine go away. I do not consider something online as being a magazine. To do away with the print version is to do away with the magazine altogether.

The online version is not easy to use, hard to impossible to download due to its size, and just not convenient. I so enjoyed the magazine, and now it's gone as far as I am concerned.

I read magazines in my off time, during lunch or travel, in the evenings, etc.—when a computer is not around. Without a printed version, I doubt I will ever see this magazine again. So sad—it was one of the best information security magazines around.

–Robert (Bob) Childs, VP/Information security officer, First Community Bank

At Your Service

A service-oriented approach is the best way to demonstrate security's value and win support for security initiatives.

BY LEONARD C. WIENS

THE TACTICS AND PERSONALITIES assumed by security teams have bred some rather novel approaches for implementing and promoting security practices within organizations. We've likely all seen the iron-fisted security group, which prefers the stick over the carrot, and tries to garner support and compliance through the spread of fear and uncertainty. Having seen an information security manager brute force C-level executive passwords and post them for all to see, I long ago concluded this approach doesn't work. Too often, security professionals damage relationships with key stakeholders through such aggressive tactics.

Other security teams attempt to raise awareness for their practice through the more benevolent approach of security metrics. But implementing metrics that demonstrate the monetary value of a security practice to the C-suite is a conundrum. Realistic security metrics related to monetary value simply don't exist and never will except in a very few unique, isolated scenarios.

While their approaches are radically different, the iron-fisted and the metrics-minded security professionals are trying to accomplish the same goal: garner support for their initiatives. A better alternative is to use a service model.

In order to survive and demonstrate true enterprise value, security teams must re-commit to a service-oriented approach.

In order to survive and demonstrate true enterprise value, security teams must re-commit to a service-oriented approach. Even if a security organization already enjoys support within the C-suite, positive working relationships generated by a service philosophy will always result in stronger, more robust security practices. A service-focused approach must accomplish five things:

1. **Align with business needs:** This is obvious, but oftentimes business groups have pent-up demand for security services that aren't being fulfilled, such as employee forensic investigations or employee/contractor security training. Frequently, such demand doesn't require a whole lot of digging to uncover. A service mindset always looks for easily aligned services that can help establish the information security brand and focus within an organization.

2. **Be timely and responsive:** As with any service, timeliness and responsiveness is integral to a security service's success. Especially within IT, when particular security services (such as an information security project risk assessment) are likely to be

viewed initially with skepticism, a security team must not be seen to stand in the way of a project's timelines. This also means getting involved early in projects so that any security holes can be remedied as part of standard project activities.

3. Provide quality: What good is a service if it doesn't fit business requirements? If security recommendations are over the top or not properly thought out in relation to operational business constraints, they will be dismissed, and rightfully so. As a result, the business may not be quick to re-engage security on future projects. Quality security offerings must demonstrate a sound awareness of both security principles and business operations.

4. Use salesmanship: A service-oriented security team doesn't necessarily mean performing new and exciting security activities that have never been tried before. What most likely changes is the approach to the activities performed. How does one sell the concept that a security assessment is really a needed service? With earnest, well presented salesmanship. Frankly, not all security professionals are up for this challenge.

5. Be pragmatic: Let's be honest with ourselves: Information security is not the most important aspect of any organization, private or public. It's an organizational enabler in the best of times, a risk-mitigation practice in the worst of times, and security professionals need to accept this. Too many planned security initiatives or goals are so burdensome to an organization that they do not make sense to pursue. Too many security professionals unreasonably hinder a sound business project because of security concerns.

Pragmatism, however, shouldn't be confused with cow-towing or compromising on issues we know are important. But supporting and enabling business goals and being seen as a valued contributor to the enterprise is part of a service-oriented mind-set. Pragmatism is good for everyone, including your security initiatives and goals.

Leonard C. Wiens, CISSP, CISA, is manager of information security services at Husky Energy in Calgary. Send comments on this column to feedback@infosecuritymag.com.

Analysis | SENATE BILL 773

Power Grab or Necessary Step?

The Cybersecurity Act of 2009, also known as S.773, would give the president unprecedented authority over federal and private networks. Experts debate whether it's a power grab, or a signal of the seriousness of threats to critical infrastructure. BY MICHAEL S. MIMOSO

CRITICAL INFRASTRUCTURE SECURITY has been dinged from every direction lately: attacks on the power grid; plans for the Joint Strike fighter jet stolen; hospitals hit by Conficker; testimony before Congress on the shoddy state of affairs and the need for attention and oversight.

Yet the one that has civil libertarians and folks on both sides of the aisle concerned the most is the Cybersecurity Act of 2009, a bill proposed by West Virginia Democrat Jay Rockefeller and Maine Republican Olympia Snowe. On its surface, the bill isn't a radical departure from what experts have been asking for all along. The senators want to establish a cybersecurity advisory panel that includes public and private industry representatives, create a national cybersecurity strategy, develop security standards for software used in federal systems, appropriate money for research and development and sponsor educational initiatives around cybersecurity.

All well and good until you get to sections 14 and 18 of Senate Bill 773.

Provisions in section 18 would give the president the authority to shut down a critical infrastructure network during a cybersecurity emergency that threatens national security. The bill does not define a critical infrastructure network nor does it limit the president's power to federal networks. Section 14, meanwhile, would establish the Dept. of Commerce as a clearinghouse of threat and vulnerability information for federally and privately-owned critical infrastructure systems and networks. This section says the Secretary of Commerce would "have access to all relevant data concerning such networks without regard to any provision of law, regulation, rule, or policy restricting such access." The secretary would also manage how information is shared between the government and public and private infrastructure operators.

While some might interpret this as a power grab on the part of the government, others are saying the bill isn't likely to fly as is and that it's merely a discussion starter.

"The main intent, I think, is to send a signal to the White House that Congress is serious about [cybersecurity]," says Jim Lewis, director and senior fellow of the Technology and Public Policy Program at the Center for Strategic and International Studies

(CSIS). Lewis points out that the Defense Information Systems Agency (DISA) has similar authority to unplug Dept. of Defense networks. Lewis adds that even if ultimately the president doesn't get the authority to unplug privately-owned networks, he should have it for .gov domains.

Others, however want to know why such a dramatic tack is being taken by Congress. The bill, as written, would essentially federalize cybersecurity and drag power away from private owners of utility and communications systems who may not be so anxious to let the government make the call about disconnecting them from the public grid.

"I think that anyone familiar with the bill automatically has serious problems with it," says Jennifer Granick, civil liberties director at the Electronic Frontier Foundation (EFF). "We are paying attention to it, and ISPs, critical infrastructure operators and civil libertarians are paying attention. Few things are that remarkable, but that's the way things work in Washington. This will likely be toned down or dropped. This has to be radically amended before it's widely adopted."

"We need to protect against average threats, rather than legislating for the extraordinary."

–JENNIFER GRANICK,
civil liberties director, Electronic Frontier Foundation

Granick says government could take less grandiose measures to address network and critical infrastructure security, such as using its considerable market power to push for more secure software out of the box, and promote security basics such as encryption and patching of systems.

"If the real purpose of this bill is to protect critical systems, then we want to legislate for common events," Granick says. "We need to protect against average threats, rather than legislating for the extraordinary."

Another provision in the bill calls for an identity management and authentication program for government and critical infrastructure information systems and networks. Is this a precursor to a national ID program, or a jab at online privacy?

"There's reason to fear that this type of study is just a precursor to proposals to limit online anonymity. But anonymity isn't inherently a security problem. What's "secure" depends on the goals of the system. Do you need authentication, accountability, confidentiality, data integrity?" Granick wrote in an EFF blog. "Each goal suggests a different security architecture, some totally compatible with anonymity, privacy and civil liberties. In other words, no one "identity management and authentication program" is appropriate for all Internet uses."

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

Crisis Averted?

WHILE CONFICKER did not wreak havoc on April 1, researchers say the danger has not passed and the botnet could find a way to download powerful attack code. In fact, eight days later a new Conficker/Downadup variant was on the loose, with connections to the Storm botnet. —*Information Security* staff

285 million

Number of records compromised in 2009 from 90 confirmed breaches*

43

The number of fixes Oracle released as part of its quarterly Critical Patch Update, repairing flaws in its database management system, application server and application product lines

08/01/09

The day the enforcement of the Red Flags Rule by government and industry regulators is set to begin

*Source: 2009 Verizon Business Data Breach Investigations Report

OVER-HEARD

"This is the American way of life that is being threatened. We need continuous automated monitoring and real oversight of these critical systems and it needs to be a top priority."

–ALAN PALLER, director of research at the SANS Institute

In response to *The Wall Street Journal* story that said malware was discovered on electrical grid computer systems suggesting that someone abroad could damage the system in a time of war or during a national security crisis.

Should we have an expectation of online privacy?

POINT *by* MARCUS RANUM

IN A RECENT COURT DECISION, a Canadian judge ruled that Internet users have no reasonable expectation of privacy with regard to warrantless collection of subscriber/IP address information from a suspected child pornographer's ISP. Couple that with the Bush administration's cheerful bypassing of warrants for wiretaps against U.S. citizens, and those are just two of the more public instances we've heard of where privacy has been trampled. (There's no need to mention the many governments that don't hesitate for a second to collect whatever information they can regarding their citizens' activities.)

Does this mean that the notion of online privacy is in jeopardy?

From the beginning, online privacy was probably more of a goal than a reality—a goal that was near and dear to a few technologically sophisticated users: the Cypherpunks [http://www.activism.net/cypherpunk/manifesto.html], and the Electronic Frontier Foundation. Everyone else either assumed their actions were private, or didn't really care. Indeed, most people's lives really aren't worth looking at, unless you're somehow involved with them personally, so "so what?" is probably a pretty decent strategy for most people.

> "If you're even moderately technologically sophisticated, you can achieve a fair amount of online privacy with very simple techniques."
> —MARCUS RANUM

What we've seen is that governments are consistently willing to ignore their own wiretapping rules—so much so, in fact, that a cynic might say that the rules exist only to encourage a false sense of confidence in the targets. It makes you wonder, doesn't it?

The big surprise, to me, is that anyone falls for it.

If you're even moderately technologically sophisticated, you can achieve a fair amount of online privacy with very simple techniques. You don't have to sit back and wish that government and business would suddenly decide to always play nice and respect your agenda. If you're a member of the tinfoil hat brigade [http://people.csail.mit.edu/rahimi/helmet/], you can achieve an amazing amount of online privacy, with some difficulty. There are plenty of open source and freeware tools for hard drive encryption, tunneling data within data, steganography, and—of course—more operating systems than you can be bothered to keep track of. I'm pretty sure that, if I joined the tinfoil hat brigade, I'd be able to quickly assemble a communications system that was so secure it'd be practically unusable.

Here's a guy for whom online privacy is an issue: I was hanging out at a photographer's studio and he arranged a small illicit purchase using text messaging on his cell phone. When I found this out, I was speechless—I'd never seen anything so dumb in years. But

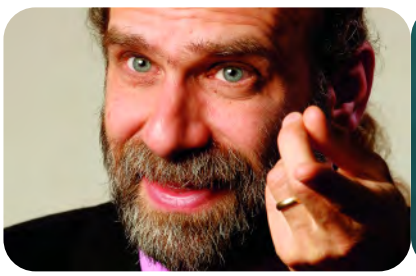
he laughed at my paranoia and said "Of course I didn't refer to it by name! I just asked my friend for a 'package.'" I pointed out that if his friend was ever busted, the police only had to pull the friend's phone call records, and suddenly he wasn't laughing. At a certain point, you've got to just shake your head and chalk it up to evolution in action. People who are using public data networks to do naughty, terroristic, or counter-revolutionary things have simply got to protect themselves. To a government or business, privacy looks indistinguishable from sedition or crime.

Privacy has always been something special, enjoyed by those who are wealthy and powerful enough to afford guards, walls and lawmakers. It speaks well of techno-geek society that we tried—and tried hard—to democratize the data networks and protect their users, but the end-game was inevitable. From one side, you're either a member of the tinfoil hat brigade or an activist Cypherpunk. Seen from the other side, you're a pre-selected terrorism suspect or a blob of marketing data waiting to be analyzed and sold.

Which are you?

Marcus Ranum is the CSO of Tenable Network Security and is a well-known security technology innovator, teacher and speaker. For more information, visit his website at www.ranum.com.

COUNTERPOINT *by* BRUCE SCHNEIER



IF YOUR DATA IS ONLINE, it is not private. Oh, maybe it seems private. Certainly, only you have access to your e-mail. Well, you and your ISP. And the sender's ISP. And any backbone provider who happens to route that mail from the sender to you. And, if you read your personal mail from work, your company. And, if they have taps at the correct points, the NSA and any other sufficiently well-funded government intelligence organization—domestic and international.

You could encrypt your mail, of course, but few of us do that. Most of us now use webmail. The general problem is that, for the most part, your online data is not under your control. Cloud computing and software as a service exacerbate this problem even more. Your webmail is less under your control than it would be if you downloaded your mail to your computer. If you use Salesforce.com, you're relying on that company to keep your data private. If you use Google Docs, you're relying on Google. This is why the Electronic Privacy Information Center recently filed a complaint with the Federal Trade Commission: many of us are relying on Google's security, but we don't know what it is.

This is new. Twenty years ago, if someone wanted to look through your correspondence, he had to break into your house. Now, he can just break into your ISP. Ten years ago, your voicemail was on an answering machine in your office; now it's on a computer owned by a telephone company. Your financial accounts are on remote websites protected only by passwords; your credit history is collected, stored, and sold by companies you don't even know exist.

And more data is being generated. Lists of books you buy, as well as the books you look at, are stored in the computers of online booksellers. Your affinity card tells your supermarket what foods you like. What were cash transactions are now credit card transactions. What used to be an anony-

mous coin tossed into a toll booth is now an EZ Pass record of which highway you were on, and when. What used to be a face-to-face chat is now an e-mail, IM, or SMS conversation—or maybe a conversation inside Facebook.

Remember when Facebook recently changed its terms of service to take further control over your data? They can do that whenever they want, you know.

> "The courts need to recognize that in the information age, virtual privacy and physical privacy don't have the same boundaries."
> –BRUCE SCHNEIER

We have no choice but to trust these companies with our security and privacy, even though they have little incentive to protect them. Neither ChoicePoint, Lexis Nexis, Bank of America, nor T-Mobile bears the costs of privacy violations or any resultant identity theft.

This loss of control over our data has other effects, too. Our protections against police abuse have been severely watered down. The courts have ruled that the police can search your data without a warrant, as long as others hold that data. If the police want to read the e-mail on your computer, they need a warrant; but they don't need one to read it from the backup tapes at your ISP.

This isn't a technological problem; it's a legal problem. The courts need to recognize that in the information age, virtual privacy and physical privacy don't have the same boundaries. We should be able to control our own data, regardless of where it is stored. We should be able to make decisions about the security and privacy of that data, and have legal recourse should companies fail to honor those decisions. And just as the Supreme Court eventually ruled that tapping a telephone was a Fourth Amendment search, requiring a warrant—even though it occurred at the phone company switching office and not in the target's home or office—the Supreme Court must recognize that reading personal e-mail at an ISP is no different.

Bruce Schneier is chief security technology officer of BT Global Services and the author of Schneier on Security. *For more information, visit his website at www.schneier.com.*

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.

Automating Compliance

The weight of regulatory compliance can break the back of your IT operation. Automation can help you gear up for the next audit.

BY RICHARD E. MACKEY

JUST AS A CHECK-BOX approach to compliance doesn't guarantee security, good security practices aren't necessarily enough to meet regulatory compliance requirements.

The point is, you may actually achieve a substantial degree of data security if you see securing access to sensitive information as an exercise in operational security. But, that alone won't pass muster when the auditors come in.

Virtually all regulations and contracts, from HIPAA to FFIEC guidelines to the PCI DSS, require documentation, audited requests and approvals, logging, and review of all the operational activities that companies engage in to protect the particular regulated information. Many organizations find this additional dimension troublesome and underestimate the added organizational and process burden that comes with it.

Most regulations and regulatory guidance are carefully written to avoid suggesting particular technologies, and none provides any requirement for automation of your compliance activities. However, for all but the smallest organizations, the "paperwork" associated with compliance can become unmanageable without some technological help.

In fact, technology can improve an organized approach to workflow, documentation and verification to meet compliance requirements common to many regulations.

Common Regulatory Requirements

Regulatory compliance requires organizations be able to prove they have controls in place. The mandates:

- Effectively protect the regulated information or operations
- Are enforced consistently
- Are inspected for correctness and integrity regularly
- Provide the necessary transparency to prohibit circumvention

These requirements put pressure on organizations to manage identity and access control effectively; monitor the state of systems to ensure that vulnerabilities or configuration changes do not degrade their trustworthiness, and ensure that some disinterested party is charged with watching all the use and administration of the systems.

Fortunately, regulations have many similarities in the kinds of controls they require. While they may call these requirements by different names, the regulations are trying to achieve the same basic goal: protect the confidentiality, integrity, and/or availability of a particular class of information. For HIPAA, it is health information. For PCI, it is payment card information. Regardless of the specifics, it pays to have a set of rules that allows all your compliance activities benefit from the commonality.

Following these rules is the foundation for meeting regulatory requirements:

Identify regulated information. HIPAA requires that organizations identify all systems where electronic protected information exists and ensure that all required controls are in place on the those systems. Similarly, PCI requires that companies clearly define their cardholder data environment and base all control requirements on how that area is cordoned from the rest of the company.

In any event, organizations need to erect barriers to segregate regulated information from the rest of the environment. Technologies such as firewalls, intrusion detection and intrusion prevention are the main tools used to establish and enforce the separation between environments. Of course, once these mechanisms are in place, they need to be monitored.

Determine who has authorization to access the regulated information. All regulations require organizations to maintain tight controls over the people who are allowed access to protected information.

This means more than access control. It means ensuring that supervisors and information owners are involved in the approval access and that they only provide access to appropriate individuals. It also means that there must be records of the entire approval process and account creation.

While this process and the records associated with it can be captured manually, even smaller

companies find it difficult to install the discipline required to do it well. This aspect of regulatory compliance is one of the main reasons why so many companies are turning to identity and access management (IAM) products to gather approvals, notify interested parties, capture audit logs, and even automate account creation and disablement.

Make sure that only appropriate people have access to the regulated information. Once accounts are created, they need to be recertified periodically by the same people who approved the creation of the account. Even when organizations are good about requiring and capturing account creation, many do not do a good job of carrying out the periodic checks.

This is another area where IAM systems are valuable. They can help you automate the process recertification, reminding supervisors and information owners periodically that checks and approvals are necessary, and capturing the approval process.

Monitor who has accessed the regulated information. Even if we know who *can* access the information, the question is "who *has* accessed the information?" Regulations call for capturing and monitoring access to protected data.

Monitoring does not mean saving the activity to log, only to be unearthed in the event of a suspected incident. It means sorting through the information captured and looking at the access that authorized (or unauthorized) individuals and applications have had to the information. This task is almost impossible without the help of technology to both gather and reduce the logs to a consumable format and size.

Vulnerability management and configuration management systems are the most popular security tools designed to help organizations meet compliance requirements.

Know and monitor the state of the systems and the network in which they exist. This "rule" is relatively vague, but understanding state is a broad area that needs to be adapted to the particular regulation. The idea here is that you need to know the current state of the operating systems, applications, networks, and any associated vulnerabilities these components may have. Examples of state are network configurations, operating system versions and configurations, and device firmware versions.

Keeping these points in mind when designing your compliance program can help you stay ahead of regulatory and contractual requirements. This is because regulations differ to a significant degree on the specificity of technical controls. PCI, on one hand, is relatively prescriptive in that it discusses protocols, vulnerability management practices, password standards, and the requirement for dedication of a single system to a single function. On the other hand, HIPAA, GLBA, and others refer only to best practices in most of these areas. By staying on top of the configurations and state of all your systems and networks, you will be able to adapt to requirements as they become more explicit. For example, if you track the versions and vulnerabilities of software you have deployed, you can more easily adjust your patch frequency to match the requirements of prescriptive standards like PCI.

There are a variety of technologies to help track and control the state of your systems. Vulnerability management and configuration management systems are the most popular security tools designed to help organizations meet compliance requirements.

Automating Identity Management

One critical element of compliance is controlling access to regulated information. However, before you start choosing technology to manage access, it pays to step back from the technical aspect of access control and think about it conceptually.

Almost every regulation makes the point that only people with a business requirement for access should be given access. Determining who should have access is the job of information owners, supervisors, and information custodians.

So, by stepping back, we see that the first consideration in assigning and controlling access is establishing who is responsible for making those decisions. These responsible parties establish the rules for guiding the assignment of organizational roles and ultimately all access controls.

These rules form the basis of your access control policy and are a critical part of compliance. The organizational structure, combined with the access control policy, is what is referred to as governance. Unfortunately, there is no technical mechanism that can sort out who should have access; it is a process driven by people.

Even when you have the high-level rules and structure defined, there is more work to do: You need to apply the policy to your entire organization. Basically, this means identifying which people take on roles of supervisors who approve access, the administrators who are responsible for custodianship of the systems housing the protected information, and what approvals are necessary to allow particular types of access.

Even when you have the high-level rules and structure defined, there is more work to do: You need to apply the policy to your entire organization.

Identity Management the Hard Way

Once you go through this process, you are at a point to decide what mechanisms you will use to manage it. You can certainly capture the approval workflow in a spreadsheet or database and track all the activity manually, but that's both inefficient and prone to error.

Another common—but unacceptable—practice is to advise the various parties of their responsibilities and let them manage the approval process on their own. In this model, the logging for the requests, approvals, and provisioning is typically left to the email system, and it is unlikely that anyone can oversee the process.

Auditors will find multiple compliance problems with this approach: There is no systematic enforcement of the process and no guaranteed record of the requests and approvals. Finally, even when all the requests and approvals are captured, the email system may not be controlled to the extent that it would allow an auditor to reliably follow the events that led to approval.

A third way to attack the problem is to leverage a trouble ticketing system. This can be an effective way of requesting, approving, and tracking requests for access and—if configured appropriately—provide some level of reporting. This approach is often a good, and relatively inexpensive, first step in automating the required request and approval workflow. However, ticketing systems are not purpose-built for tracking identity management operations, so they may not have a number of features that systems design for the task would.

Making Identity Management Work

Many organizations come to the conclusion that the complexity of the task and the requirement for a verifiable audit path justifies the purchase and deployment of an identity and access control system. These systems are not simple to deploy, and they are not cheap, but they can help meet several requirements from many regulations. They can also help organizations improve their security in the process.

Identity and access management systems are really two systems that are typically packaged together. The first is identity management, the process of creating accounts for people (and other entities, such as services). IAM systems also handle access control which takes the identities and assigns privileges or authorization to access resources. Access management incorporates both users (or principals) and resources.

One of the reasons these systems have become so popular is that they support the administration of identity and access across different identity stores, applications and, in many cases, multiple identities for the same people across different systems. In other words, the promise of these systems is that they will eventually allow organizations to have a single centralized service to manage "all" accounts.

All of the leading identity and access management systems support integration with Windows, UNIX systems, Active Directory, LDAP, and much more.

While identity management and access control are different jobs, they share many common elements. Both require:

- An auditable approval workflow, reporting of state (accounts and access)
- Notification of changes
- Integration with underlying technologies, such as operating systems, authorization systems, directories and devices

All of the leading identity and access management systems support integration with Windows, UNIX systems, Active Directory, LDAP, and much more. This integration allows these systems to support automatic creation and deletion of accounts and automatic changes to authorization. The leading products are also extensible, so you can integrate your own applications and systems into the mix.

While this automation capability is very useful, the two most important IAM features for compliance are the abilities to specify a strict approval workflow and audit those approvals. This allows you to demonstrate to an auditor that you have a formal identity management and access control policy and a mechanism to enforce it.

The systems orchestrate the entire process from notification through the capturing of all approvals (or rejections). They can even remind you periodically that account and access recertification is necessary and capture the activity in logs for auditors.

As an added bonus, these systems can automatically recognize and prohibit role conflicts. For example, it is important for many organizations to ensure that certain types of transactions be requested and approved by different people to provide transparency and avoid fraud. While defining these roles and conflicts is a manual process, identity management administrators can define the relationship between the roles, so conflicts can be automatically detected and prevented.

Automating State Management

State management is a broad area that includes system and network configuration management, vulnerability management, and monitoring. Every regulation requires you to track and control the state of all systems, networks, and devices in the target environment.

Effective state management can be accomplished with a variety of manual processes. Organizations often maintain detailed specifications of configurations of all systems and devices in documents and spreadsheets, and conduct periodic manual audits.

The larger and more complex your environment, the more cumbersome this manual process can be and the more automation can help. Many products that can be purchased separately or as parts of an integrated suite provide automated management of state. They tend to be organized around two functions: configuration management and vulnerability management:

Configuration management and monitoring. Configuration management systems allow you to specify and monitor configurations of services, ports and protocols. Some products require agents to be deployed on the monitored systems, some monitor remotely, and some determine configuration by passively monitoring network traffic.

Configuration monitoring tools can be programmed to look for behavior that violates compliance requirements. For example, with PCI DSS compliance, they can look for insecure protocols such rsh and Telnet, or the presence of open ports in the cardholder data environment. Vendors continue to develop regulation-specific templates to scan for violations.

Vulnerability management systems determine the versions of operating systems, services and applications and match them against published vulnerability announcements.

Vulnerability tracking and patch deployment. Vulnerability management systems determine the versions of operating systems, services and applications and match them against published vulnerability announcements. They require a subscription to a vulnerability tracking service and can substantially reduce the amount of work you will need to devote to scouring vulnerability announcements and comparing versions and vulnerabilities.

These products also provide dashboard displays of systems, versions, vulnerabilities, and the severity of vulnerabilities on your systems. Your network zones will appear as an array of green, yellow and red boxes depicting the severity of vulnerabilities on each system. Some of these products also calculate risk based on asset value. For example, a system running a vulnerable Web server that is exposed to the Internet poses a higher risk of compromise than one only exposed to your corporate network.

Vulnerability management systems can be integrated with patch deployment tools to automate the distribution and application of patches that address vulnerabilities. While this type of automation can be a time saver, it doesn't cover one of the most critical manual steps in state management: change control.

Recognizing state problems is the first step in good management. Bringing the systems into technical compliance is a process that requires discipline, thought and a clear audit trail. Vulnerability management tools can help, but the entire process can never be completely automated.

Once a vulnerability is identified, good practice and most regulations require that you

conduct a risk assessment to determine whether there is more risk in allowing the vulnerability to exist or patching the vulnerability immediately without adequate testing. Business and technical representatives must weigh factors such as planned downtime, potential outages and software incompatibility against the likelihood that the vulnerability will be exploited. The business may be willing to accept the risk of compromise for some period, may require additional compensating controls such more monitoring, or may even accept the risk of downtime if the risk of an exploit is too great.

This kind of risk-based approach can be problematic if you are subject to PCI, which requires that systems be patched within a specified time period. However, you may be able to convince the assessor that your acceptance of risk is appropriate if you can provide evidence of the risk assessment, the reasoning behind your decision, and compensating controls that achieve an equivalent level of risk mitigation. The combination of a clear understanding of your state with good risk management and configuration control will go a long way with any auditor.

If you are structuring your security practices to comply with HIPAA, identity theft laws, PCI or other regulations, it pays to focus on the fundamentals like identity and access management and state management. Both these activities require well-defined processes and organizational discipline, but they can also benefit from appropriately applied technology.

If you create the right organization and policy and apply systems like identity management and vulnerability management technologies prudently, you can not only ease your day-to-day operations, but significantly reduce the risk of failing an audit and reduce the effort needed to pass.

Richard E. Mackey, vice president of SystemExperts. Send comments on this article to feedback@infosecuritymag.com.

Do you need an IDS or IPS... or both?

BY JOEL SNYDER

We'll cut through the hype and explain the benefit of both technologies.

While threat management continues to be a top priority, it is more important than ever for cash-strapped security professionals to fully understand the functionality of intrusion defense tools in order to make good purchasing decisions.

Intrusion defense systems (IDS) and intrusion prevention systems (IPS) are a particularly confusing area because the products are so similar, the vendors are all the same, and even the acronyms are hard to tell apart. We'll explain the capabilities of each and how to decide whether you need one or both technologies.

Differentiating IDS and IPS

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.

It's important to start out with the understanding that IDS and IPS are very, very different tools. Even though they have a common base, they fit into the network in different places, have different functions, and solve different problems.

An IPS is best compared to a firewall. In a typical enterprise firewall, you'll have some number of rules: maybe a hundred, maybe a thousand. Most of those rules are "pass" rules: "allow the traffic through." Thus, the firewall gets a packet off the wire and starts through its rules, looking for a rule that says "allow this packet through." If it gets to the end of the list and there's no rule saying "allow this packet through," then there's a final "deny" rule: "drop everything else." Thus, in the absence of a reason to pass the traffic, the firewall drops it.

It's important to start out with the understanding that IDS and IPS are very, very different tools.

An IPS is like that, but inside out: it has rules, maybe hundreds, maybe thousands. Most of those rules are "deny" rules: "block this known security problem." When a packet shows up at the IPS, the IPS looks through its rule list from top to bottom, looking for some reason to drop the packet. At the end of the list, though, is an implicit "pass" rule: "allow this packet through." Thus, in the absence of a reason to drop the traffic, the IPS passes it through.

Firewalls and IPSes are control devices. They sit inline between two networks and control the traffic going through them. This means that the IPS is in the policy side of your security house. It's going to implement or enforce a particular policy on what traffic is not allowed through.

The obvious affinity of firewalls and IPSes from a topological point of view has led us to the world of UTM, where an IPS is incorporated into the firewall. UTMs let you have both security services (blocking security threats, allowing known good traffic) into a single device. We'll talk about the ultimate in compression of IPS and firewall, the UTM (Unified Threat Management) firewall later.

The main reason to have an IPS is to block known attacks across a network. When there is a time window between when an exploit is announced and you have the time or opportunity to patch your systems, an IPS is an excellent way to quickly block known attacks, especially those using a common or well-known exploit tool.

Of course, IPSes can provide other services. As product vendors search to differentiate themselves, IPSes have become rate limiting tools (which is also helpful in Denial of Service mitigation), policy enforcement tools, data leak protection tools, and behavior anomaly detection tools. In every case, though, the key function of the IPS is a control function.

What can IDSes do?

If an IPS is a control tool, then an IDS is a visibility tool. Intrusion Detection Systems sit off to the side of the network, monitoring traffic at many different points, and

provide visibility into the security posture of the network. A good analogy is to compare an IDS with a protocol analyzer. A protocol analyzer is a tool that a network engineer uses to look deep into the network and see what is happening, in sometimes excruciating detail. An IDS is a "protocol analyzer" for the security engineer. The IDS looks deep into the network and sees what is happening from the security point of view.

In the hands of a security analyst, the IDS becomes a window into the network. The information provided by the IDS will help the security and network management teams uncover, as a start:

- Security policy violations, such as systems or users who are running applications against policy
- Infections, such as viruses or Trojan horses that have partial or full control of internal systems, using them to spread infection and attack other systems
- Information leakage, such as running spyware and key loggers, as well as accidental information leakage by valid users
- Configuration errors, such as applications or systems with incorrect security settings or performance-killing network misconfiguration, as well as misconfigured firewalls where the rule set does not match policy
- Unauthorized clients and servers including network-threatening server applications such as DHCP or DNS service, along with unauthorized applications such as network scanning tools or unsecured remote desktop.

This increased visibility into the security posture of the network is what characterizes an IDS, and which differentiates the visibility function of an IDS from the control function of an IPS.

Of course, since both IDS and IPS have the word "intrusion" as the beginning of their acronym, you may be wondering why I haven't mentioned "intrusion" as part of the function of either IDS or IPS. Partly that's because the word "intrusion" is so vague that it's difficult to know what an intrusion is. Certainly, someone actively trying to break into a network is an intruder. But is a virus-infected PC an "intrusion?" Is someone performing network reconnaissance an intruder…or merely someone doing research? And if a malicious actor is in the network legitimately—for example, a rogue employee—are their legitimate and illegitimate actions intrusions or something else?

The more important reason for leaving "intrusion" out of the description for both IDS and IPS is that they aren't very good at catching true intruders. An IPS will block known attacks very well, but most of those attacks are either network reconnaissance or automated scans, looking or other systems to infect—hardly "intrusions" in the classic sense of the word. The best Intrusion Prevention System in this case is the firewall, which doesn't let inappropriate traffic into the network in the first place.

It's the misuse of the word "intrusion" in referring to these visibility and control technologies which has caused such confusion and misguided expectations in staff at enterprises that have deployed either IDS or IPS.

Yes, an IDS will detect true intrusions. Yes, an IPS will block true intrusions. But these products do much more than that—they provide greater control and greater visibility, which is where their real value is.

So which do I buy?

If all products were either an IDS or an IPS, then the answer to the question of "which should I buy" would be easy: buy an IDS if you want visibility, and buy an IPS if you want control. But IPS and IDS vendors don't make it easy for us, because they have developed and released hybrid products which combine IDS visibility on top of IPS control.

For most enterprises, especially ones who don't have an IPS or an IDS already, the right answer is "buy an IPS." A visibility tool only brings you value if you have time to look at what it's telling you. With tight budgets and overstressed staff, the kind of senior security engineer it takes to really get value out of an IDS is in short supply. Buying a product that no one is going to look at isn't going to do you much good. Without regular and disciplined use of the visibility aspects of an IDS, the only real effect you'll see is in increased power bills.

This doesn't mean that an IPS is a "set it and forget it" kind of device. To get value out of an IPS, you must tune it to match your own network and application and system mix. If you don't, you'll either have a high rate of false positives, which can interrupt legitimate traffic, or you'll miss a lot of attacks, in which case the IPS is not bringing you very much value. An IPS that never has a false positive is probably

ALL-IN-ONE

What About UTM IPSes?

THE COMBINATION OF an IPS and a firewall into a single system, with a single management system, is attractive. Unfortunately, most unified threat management systems (UTMs) are designed for SMB deployment, an environment where the simplicity of the management system is one of the most critical design requirements. Combining IPS management with firewall management is a very difficult task. In fact, no product vendor has successfully managed to merge their web-based firewall management system with a good IPS management tool.

You shouldn't assume that an IPS incorporated into a UTM firewall will offer the same types of controls and protections as a standalone IPS.

This does not mean that there aren't great UTM firewalls with embedded IPSes; it just means that the management systems for the IPS part of these products are quite different (and often separate) from the firewall parts.

If your prospective UTM firewall vendor has bundled the IPS and firewall functionality all into a homogeneous single web interface, you're looking at a product where the IPS is getting second rate management tools. This may be fine in environments where you're only interested in control, such as at branch offices or where only a small set of systems are being protected.

To find an enterprise-class IPS combined with a UTM firewall, look for products which are, paradoxically, *less* integrated: a standalone IPS and standalone firewall combined in the same chassis, for example.

–JOEL SNYDER

not doing a good job at protecting your network.

However, you will get value out of an IPS without a large time investment in managing and tuning it, and analyzing what it's telling you about your network. That's because the IPS will be there, providing additional defenses, and helping to protect you against common errors. Since most security problems are the result of human error rather than targeted attacks, the IPS is an outstanding way to bring a defense-in-depth strategy to network security.

Most IPS vendors, because of their IDS heritage, sell products which actually combine both IPS and IDS functions. They have the powerful malware and attack recognition engine needed to identify and block attacks, but they also have additional rules and tools designed to enhance network visibility.

As you're considering IPS, IDS, or combination products, remember to focus on your primary requirement. If you are looking for additional control, the most important part of the picture is the IPS detection engine. IPSes need the ability to quickly detect and block attacks, at very high speeds and without degrading network performance, throughput, or latency.

If you're looking for visibility, network forensics, and analysis capabilities, the most important part of the picture is the IDS management console. You have to be able to navigate through the information provided by the IDS in a quick and natural way to gain network and security visibility. While the detection engine is important, it's not nearly as important as the management system. Without an effective way of extracting information from the IDS—and this is as much your training as it is the management console you install—you won't see much value from an IDS.

Joel Snyder is Senior Partner for Opus One. Snyder has built and secured some of the largest and highest profile networks in the world for major ISPs, government agencies and Global 2000 companies for the past 27 years. In addition to many consulting projects, Joel has authored several books and hundreds of technical articles; designed compilers, data management applications, conferencing systems, security systems, and anti-spam tools. Snyder is also a technical editor for Information Security *and has written numerous feature articles and technical reviews on subjects including e-mail security, spam controls and security management systems. Send comments on this article to feedback@infosecuritymag.com.*

Identity management for changing times

Identity management technology is adapting to meet enterprise needs. Learn what products can improve security and ease compliance.

BY MARK DIODATI

DOES IT FEEL LIKE THE WORLD of identity management is calcified with the same old products and a glacial pace of innovation? Strong authentication, directory services, provisioning, Web access management, and federation have been around for years but what's new?

In fact, there are a lot of developments in the identity management space and newer technologies such as privileged account management, Active Directory (AD) bridge, and entitlement management are taking off as companies look to ensure security and meet compliance demands.

While large enterprises have deployed a mix of identity management products, few have enjoyed the synergies that these products bring when they are integrated. Let's look at some of the benefits the new technologies provide and strategies that can help an enterprise fully leverage its identity management investments.

Old School Identity Management

Traditional identity management products have become an intrinsic part of the IT infrastructure and continue to be deployed today. They include:

- **Directory services** and authentication products are the oldest examples of identity management products. Directory servers use the Lightweight Directory Access Protocol (LDAP) to present data. While relatively difficult for developers to work with, LDAP has emerged as the standard repository for user and policy information.

- **Provisioning** systems add, delete, and modify user accounts across heterogeneous platforms. These systems typically include workflow (to enable the approval of changes to user accounts) and role management capabilities, which can provide security and compliance benefits.

- **Web access management (WAM)** systems provide single sign-on (SSO) and authorization services for heterogeneous Web applications. WAM systems work solely with Web applications and do not require client software besides a Web browser.

- **Strong authentication** systems leverage at least two factors to provide higher identity assurance. The most commonly deployed strong authentication system in the enterprise is the one-time password device (OTP). The device displays a unique code, which is combined with a personal identification number (PIN) to provide two-factor authentication. Other strong authentication mechanisms include smart cards (which also leverage a portable hardware device and a PIN) and biometrics.

- **Federation** technology was a response to the challenge of providing single sign-on services to users at separate organizations. Unfortunately WAM systems weren't up to the challenge as they leveraged the HTTP cookie for session management, which did not work across corporate boundaries. The default standard in federation is Security Assertion Markup Language (SAML).

New School Identity Management

Newer types of identity management technologies such as privileged account management, Active Directory (AD) bridge, security information management (SIM), entitlement management, virtual directory, and enterprise SSO products are seeing broad adoption. In most cases, these markets are growing at a greater rate as compared to traditional identity management products. They include:

- **Privileged account management** is a market segment growing fast, with most large, regulated enterprises either having already deployed or planning to deploy the technology. While provisioning systems are very good at managing user accounts belonging to real users, they are terrible at managing generic privileged accounts like the UNIX root account. These accounts are required by the target platform (try deleting the root account from a UNIX system and see what happens), so access to them needs to be controlled. The accounts are also shared by many administrators; the result is a lack of accountability.

In the hands of evil-doers, these generic privileged accounts can inflict real damage, because they can bypass security controls, destroy or breach confidential data, and cover tracks by deleting audit data. Privileged account management products

provide greater accountability because the account must be checked out by the administrator and the password associated with the account is changed frequently.

• **AD bridge** is another segment that is seeing explosive growth. These products extend authentication, authorization, and identity management from Microsoft Active Directory to non-Windows platforms like UNIX, Linux, and Mac OS. Using Active Directory, enterprises can manage identities and provide centralized authorization to these platforms. Additionally, these products enable the authentication of non-Windows users against Active Directory, and provide single sign-on between Windows, UNIX, Linux, and Mac OS platforms. AD bridge products are very popular because they enable enterprises to leverage their significant investment in Active Directory to provide security services for other platforms and close out audit findings in the process. AD bridge products can also smooth over the integration of the increased number Mac OS systems in the enterprise.

• **Security information management (SIM)** is not usually considered an identity management technology. Recently, however, enterprises have been using SIM products in ways that complement their identity management initiatives. In addition to incident management, enterprises are now leveraging SIM products to assist with authorization. With the SIM product, application owners can evaluate user access over a specified time at the beginning of an application security review. Getting authorization right means getting security right, with the added benefits of closing compliance gaps and audit findings.

• **Entitlement management** products provide a much deeper level of authoriza-

PURCHASING

Full Evaluation Required

ORGANIZATIONS CAN RUN INTO PROBLEMS IF THEY DON'T CHECK OUT ALL THE PIECES OF AN IDENTITY MANAGEMENT SUITE.

WHEN CONSIDERING AN identity management suite, don't make the same mistake that many of your colleagues have made by failing to thoroughly evaluate all identity management products under consideration before a purchase.

Most organizations begin their evaluations by looking for a single product to meet a pressing need. At purchase time, the vendor then offers the customer a steep discount to compel the purchase of multiple identity management products. The deployment of the primary product goes well, but then the organization finds out that the other purchased products don't meet its needs, or require significant customization to work.

Multiple products from the same vendor can be a good fit, but organizations need to vet all of the products before writing the check. The additional evaluation work takes time, but it's worth the effort. Install the identity management products in your development environment, and test them against your existing applications, particularly your enterprise resource planning (ERP) applications and Active Directory infrastructure. Finally, don't hesitate to get a pilot user group to test the products. ›

–MARK DIODATI

tion capabilities than WAM systems with the added benefit of eXtensible Access Control Markup Language (XACML) interoperability. This interoperability provides investment protection by enabling enterprises to build components which should work with multiple entitlement management products. When the products were first introduced several years ago, enterprises had to develop their own custom components. The vendors are now providing plug-ins for application servers like IBM WebSphere and Microsoft Windows platforms (including SharePoint). Entitlement management products are hardly mainstream, but many large financial institutions with challenging compliance mandates have deployed them.

• **Virtual directories** products provide a valuable service. They enable maximal consumption of user and policy information by the security applications that need this information. Virtual directories can present this information via LDAP. Behind the scenes, virtual directories map the information from a variety of repositories, including relational databases, LDAP directory servers, Active Directory, and even the mainframe without implementing an expensive and time-consuming meta-directory. In the past, the default consumer of information from virtual directories has been WAM systems. Recently, enterprises are deploying virtual directories for other identity applications including entitlement management, federation, and enterprise single sign-on (SSO).

• **Enterprise SSO** products try to solve the "last mile" problem by reducing the number of sign-ons to client/server and mainframe applications. Enterprise SSO products have been available for well over a decade, but their deployment has recently picked up, especially in the healthcare and financial service markets. Enterprise SSO products have become easier to deploy because they require less customization than in the past. A new trend is transaction-level integration between enterprise SSO systems and the target application. One example of transaction-level integration is a healthcare application that prompts the enterprise SSO application to re-authenticate the doctor before allowing the writing of a prescription.

Integration

In many cases, identity management products can be blended to reap additional benefits.

For example, organizations are integrating enterprise SSO with provisioning and strong authentication products to improve application security. Provisioning products provide better security because they can change passwords more frequently in both the target application and the user's enterprise SSO wallet. Strong authentication systems (like OTPs) solve the "keys to the kingdom" problem— eliminating weak password-based authentication, which enables access to many applications.

Meanwhile, WAM and federation products are "best friends forever" because neither product provides the complete security package for Web applications, but when combined, work synergistically. WAM provides the authorization and session management, while federation provides the enterprise-to-enterprise (E2E) SSO functionality.

Another trend in the enterprise is the coupling of provisioning and strong authentication systems (e.g., OTP or smart card). When integrated, the provisioning system

can manage most aspects of the authentication device. Two benefits are the elimination of near-duplicative identity management processes and timelier identity lifecycle management, which becomes especially important when employees are terminated.

Another integration example is the use of Active Directory in conjunction with an AD bridge product to provide central authentication and authorization services for non-Windows platforms. One vendor, Likewise, provides a free, open source AD bridge product that can unite Active Directory to non-Windows platforms.

Suites Not Necessarily the Answer

Instead of going to the trouble of integrating identity management products, why not just buy a suite from a single vendor? The ostensible benefits of purchasing a

PRODUCTS

ID Management Vendors

HERE IS A PRODUCT SAMPLING OF IDENTITY AND ACCESS MANAGEMENT SOLUTIONS. BY MARK DIODATI

Privileged account management

Cloakware, www.cloakware.com
Cyber-Ark Software, www.cyber-ark.com
eDMZ Security, www.e-dmzsecurity.com
Lieberman Software, www.liebsoft.com
Passlogix, www.passlogix.com
Quest Software, www.quest.com
Symark, www.symark.com

Active Directory bridge

Centrify, www.centrify.com
Likewise Software, www.likewise.com
Quest Software, www.quest.com
Symark, www.symark.com

Security Information Management

ArcSight, www.arcsight.com
CA, www.ca.com
EMC/RSA, www.emc.com
IBM, www.ibm.com
Intellitactics, www.intellitactics.com
NetIQ, www.netiq.com
Novell, www.novell.com
SenSage, www.sensage.com

Entitlement management

Bayshore Networks, www.bayshorenetworks.com
CA, www.ca.com
Cisco Systems, www.cisco.com
IBM, www.ibm.com
Jericho Systems, www.jerichosystems.com
Oracle, www.oracle.com
Sun Microsystems, www.sun.com

Enterprise SSO

ActivIdentity, www.actividentity.com
CA, www.ca.com
Novell, www.novell.com
Passlogix, www.passlogix.com
Sentillion, www.sentillion.com

Virtual directories

Optimal IdM, www.optimalidm.com
Oracle, www.oracle.com
Radiant Logic, www.radiantlogic.com/main
SAP, www.sap.com
Symlabs, www.symlabs.com

suite include a lower average price per product, and vendor-specific synergies between the products.

While it is probable that the average software cost per product will be lower, experience has shown that most organizations end up paying more due to substitute software products or customization services. *[See sidebar, p. 31]*

As for vendor-specific synergies between products, very few exist. These synergies are generally divided into two areas: a common administration console, and enhanced interoperability between products. A common administration console across the vendor's identity management products provides value if the same IT people are managing multiple identity management products. Identity management products from the same vendor provide very few interoperability features over the interoperability that exists across identity management products from different vendors. Some examples of cross-vendor interoperability include: federation products which support cookie types for different WAM systems; WAM products which work with virtually any directory server; and provisioning systems that target platforms from different vendors.

IAM in a Tough Economy

While there are numerous benefits to IAM technologies, the current fiscal environment means that identity management projects are facing increased scrutiny. Organizations must be especially careful about identity management product selection, derive more value from their existing products, look for hard cost savings, and consider building identity management functionality in-house.

While there are numerous benefits to IAM technologies, the current fiscal environment means that identity management projects are facing increased scrutiny.

First, organizations should look for buried treasure within their identity management product licenses to determine if they can get more value from their existing solutions. For example, many early WAM deployments started and ended with Web servers because the WAM technology did not provide authorization to other platforms such as application servers and ERP applications. Times have changed, and today the WAM system may be able to provide security for these platforms without additional license purchases.

Another cost-saving strategy, is the use of Active Directory in conjunction with an AD bridge product to provide central authentication and authorization services for non-Windows platforms.

As IT budget gets cut in difficult economic times, the buy versus build equation changes. In many cases, organizations can tactically solve some problems by developing small identity applications. Examples include self-service portals, provisioning connectors for internally developed applications using Service Provisioning Markup Language (SPML), and developing SIM applications using tools like Splunk.

As the economy improves, organizations will swing back to a buy mentality and identity management products will continue to evolve to meet organizational needs. Privileged account management, AD bridge, and virtual directory products will close

compliance gaps and reduce costs.

Advancements will indeed take hold where identity management technology evolves to provide identity services. What's more, the service-based approach will enable the products to interoperate more deeply via standards-based protocols offering more integration than ever before.

Mark Diodati, CPA, CISA, CISM, has more than 19 years of experience in the development and deployment of information security technologies. He is senior analyst for identity management and information security at Burton Group. Send comments on this article to feedback@infosecuritymag.com.

ADVERTISING INDEX

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

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

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

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

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

SR. VICE PRESIDENT AND GROUP PUBLISHER
Andrew Briney

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Neil Dhanowa ndhanowa@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Meghan Kampa mkampa@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

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

LIST RENTAL SERVICES
Kelly Weinhold
Phone 781-657-1691 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

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.