INFORMATION SECURITY®
MARCH 2010

Linking 'Who' and 'What'

Integrating identity management and SIMs ties policy violations to user activity

TechTarget
The Technology Media ROI Experts
INFOSECURITYMAG.COM

contents

MARCH 2010

VOLUME 12 NUMBER 2

FEATURES

ALSO

Game Changer?

BY MARCIA SAVAGE

The HITECH Act ups the ante for HIPAA enforcement, but will it really lead to security improvements in the health care industry?

HEALTH CARE ORGANIZATIONS have had to comply with HIPAA's security and privacy requirements for several years now, but compliance depended on who you talked to. Some companies took the regulation very seriously and worked hard to secure protected health information (PHI). For others, security was far down on the list of priorities, if on the list at all. But how could you blame them? The requirements aren't specific and there was little enforcement to speak of.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act, aims to change that that with its increased penalties for HIPAA non-compliance and broader enforcement. But will it really be a game changer and increase information security in the health care industry?

It's critical that more health care organizations make an effort to protect sensitive health information. A breach that exposes a patient's confidential data could have serious and lasting consequences. As Khalid Kark, vice president and principal analyst at Forrester Research points out, health care records aren't like credit cards, which can be cancelled and changed if they are exposed in a breach. "Once health care information is gone, it's gone," he says. And according to data from security-services firm SecureWorks, criminals are increasingly targeting health care organizations *(see "HIPAA Gets Some Teeth," p. 35)*.

For security teams in health care organizations, HITECH's increased penalties could help win funding for projects that have languished due to the lack of HIPAA enforcement.

For security teams in health care organizations, HITECH's increased penalties could help win funding for projects that have languished due to the lack of HIPAA enforcement. Kark says health care organizations have lagged in security spending compared to other industries. The new legislation isn't exactly clear on how the federal government will audit compliance with HIPAA's security requirements, but it widens the number of enforcers by giving state attorney generals the ability to file a federal civil action for harmful disclosures of protected health information.

Already, security managers in health care have a case to cite to their bosses: Connecticut Attorney General Richard Blumenthal wasted no time in executing his new authority, suing Health Net of Connecticut for alleged HIPAA violations due to a lost portable disk drive. It's not hard to imagine more lawsuits by attorney generals—including those wanting to curry public favor for political purposes.

And while HIPAA only offered high-level security guidance, HITECH is specific, at least in some areas. It doesn't require encryption, but it's very clear about what type of data encryption processes are required to make PHI useless and unreadable to unauthorized people in order to avoid notification requirements in the event of a breach. HITECH also requires business associates

that handle protected health care information to comply with HIPAA, which could help close up holes in patient record privacy and puts pressure on health care providers to verify third-party security. In addition, the legislation imposes new disclosure rules for PHI.

But how realistic are all these provisions, especially for small health care providers that may not have the security resources? Encryption is difficult for any enterprise, let alone a small organization without the money, security skills or staffing to deploy and manage it. Plus, the legislation doesn't do much to clarify HIPAA's security provisions, still leaving much room for interpretation. Let's hope HITECH doesn't simply lead to a plethora of security breach notifications that the public eventually becomes numb to.

At its heart, HITECH aims to encourage adoption of electronic health record technology with lucrative incentives. Kark says HITECH makes it clear that if an organization expects to receive incentives, its EHR implementations must be secure. However, for small organizations the incentives may not be enough to make the switch, he says: "The cost may be too prohibitive for them." Just trying to understand the voluminous federal requirements for "meaningful use" of EHRs could be too daunting for some.

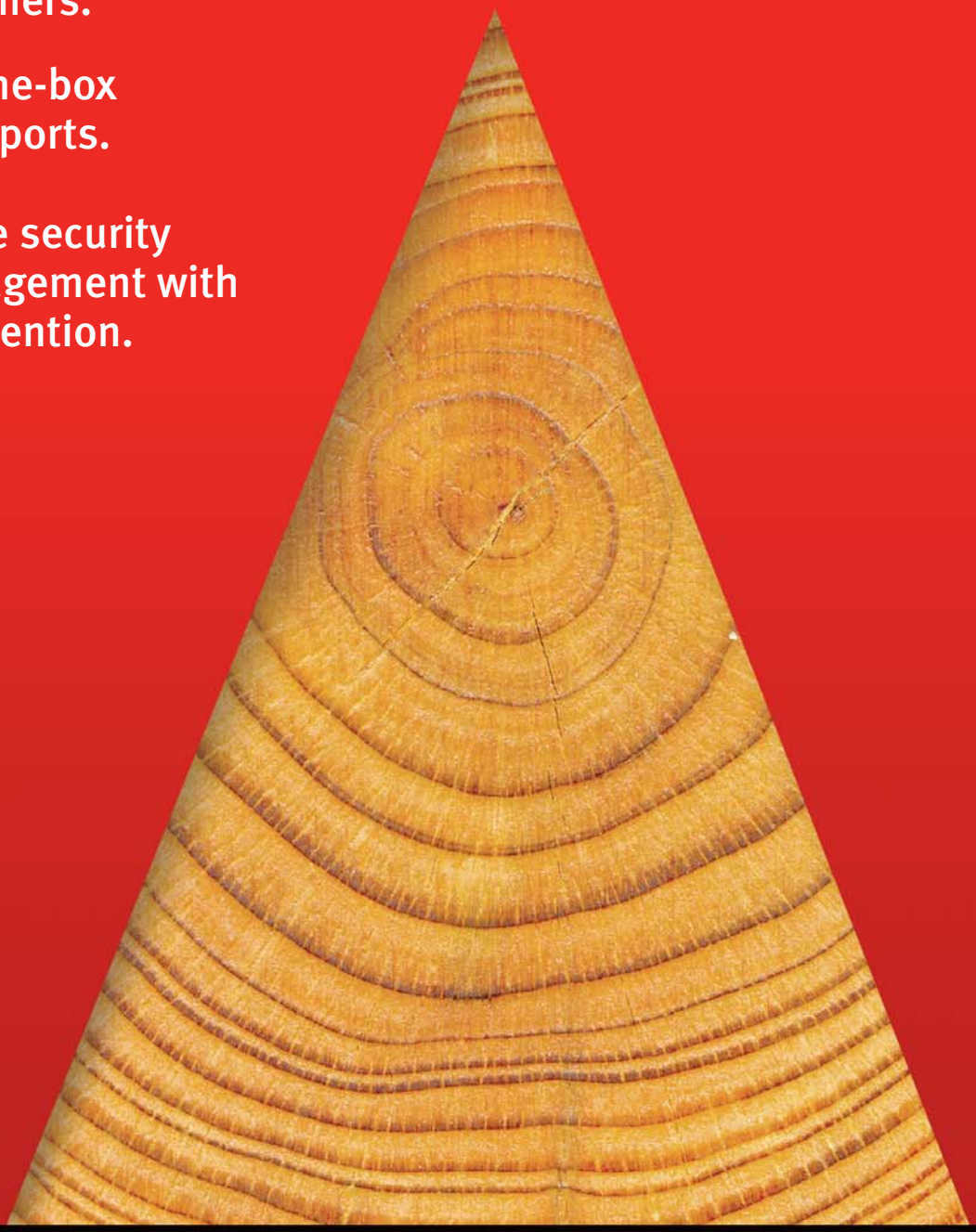
HITECH needs to force some real changes in the health care industry and not be more well-intentioned but ultimately ineffective legislation.

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

2,000+ customers.

1400 out-of-the-box compliance reports.

Content-aware security incident management with data loss prevention.



For an enduring solution to your enterprise security information event and log management needs:

Find security in the RSA enVision® platform.

RSA®

The Security Division of EMC

www.rsa.com

Security Information and Event Management | Data Loss Prevention | Identity & Access Management

COMING IN APRIL

Endpoint Protection

Just because you have desktop antivirus and firewall doesn't mean you have comprehensive endpoint protection. This feature will explain how to ensure you are protecting all your endpoints: desktops, mobile devices and even USB drives. In particular we'll focus on the pain created by smaller but powerful endpoints that may not even be sanctioned within an organization and how to deal with them.

Fraud Prevention

Online banking fraud continues to escalate, forcing financial institutions to continually improve their fraud detection and prevention systems. This feature will provide an overview of the technology available, look at the pros and cons of the technology, and help enterprise security managers to evaluate fraud prevention solutions. We'll also examine other types of technology such as security information management systems that can help detect fraud.

Recovery Strategies

Last year was tough for almost all security departments as businesses cut costs to weather the recession. But with some signs of an economic recovery, what should security teams be doing? This feature will look at how security departments handled the recession and what they should be focusing on to position themselves for an economic recovery.

In every issue:

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

MUST READ!

Let them

roam

lose laptops

surf

audit

cut budgets

who cares

You do! Liberating your people and freeing up time and resources makes productive sense. Sophos security and data protection solutions deliver: Install, set and forget. Easy on your time, easy on your system and easy on your business, everything from Endpoint to Compliance, Email, Web and Encryption is covered and all accessed and controlled with refreshing simplicity.

Now, with security taken care of, you've got the rest of the day to do all the other things that can't wait.

See for yourself – learn more about Sophos today.

SOPHOS

simply secure

Ignorance is Bliss

Many organizations fail to build a comprehensive intrusion detection architecture that uncovers genuine threats. BY PAUL ROHMEYER

HOW WOULD YOU know if your organization has been breached? It's actually a simple question and the answer is often an assertion of some degree of incident detection capability. However, as one CIO wryly told me during a network assessment, if he chose to spend time and money building a detection architecture that actually worked, it might somehow prove he has security problems. Unfortunately, I don't think he was entirely kidding.

Despite significant advances in detection technologies [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1354842_mem1,00.html], many organizations are woefully behind the times with respect to building robust capabilities to successfully identify genuine incidents. Detection is not simply a technical toolset but a complex capability, one that ideally includes well-defined technical and process domains, managed by competent staff. Weakness in any one domain severely diminishes detection effectiveness.

Despite significant advances in detection technologies, many organizations are woefully behind the times with respect to building robust capabilities to successfully identify genuine incidents.

Unfortunately, in many organizations, detection is simply not viewed as a strategic security capability. The result is that activities are limited to deployment of signature-based network intrusion detection system (IDS) sensors that track rather obvious simplistic and typically non-threatening actions, such as port scans. It may be necessary to track port scans to see who may be interested in mapping your asset landscape, but these simple out-of-the-box IDS techniques are not examples of significant detective capabilities for current threats. Moreover, many companies do not have sufficient analytical capabilities to correlate data from multiple gathering points to detect broad attack patterns or complex attacks, despite the wide availability of technologies aimed at solving this very problem.

Some choose to outsource the management of technical detection devices. However, many who do virtually ignore the data provided back to them by their service provider, all the while proudly displaying their managed services contracts to regulators and auditors, as supposed evidence of organizational detection capability. While such

contracts seem to have satisfied many regulators and auditors, a proclamation of compliance by an auditor should not be taken by the organization as evidence of a functional capability.

Weak detection capability presents multiple problems. Obviously, such limitations could result in organizations being victimized by network intruders for extended periods, resulting in significant losses of information and perhaps impacting computing resource availability. Another problem is the inability to conduct an adequate forensic investigation after a breach is discovered. Sophisticated detection technologies typically provide some mechanisms useful for capturing historical data that could be beneficial in post-incident analysis; analysis results also may be combined in the form of metrics to support the improvement of controls. Sparse event data about incidents could also weaken civil and criminal cases the organization may wish to pursue. Similarly, failure to develop a strong detective capacity could potentially indicate management's negligence in technology management and therefore a failure to exercise appropriate "due care."

The creation of effective detection capabilities requires development of a comprehensive architecture, including both technical and process components that work to detect activities that may actually threaten organizational assets. This includes not only technical architecture such as intrusion detection/prevention and security information and event management systems [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1357841_mem1,00.html] but supporting oversight activities as well. A technical toolset to detect threats to assets, if allowed to be the sole emphasis of detection design efforts, is entirely irrelevant in the absence of sufficient operational monitoring and response processes.

Periodic network penetration testing is sometimes misinterpreted as a valid test of detection capabilities. Technical techniques for testing the effectiveness of a detection architecture such as pen testing are only effective in conjunction with close correlation of response actions, which evaluates both success in technical detection (does the IDS identify the test attack?) and appropriate defenses (did the owner of the IDS notice the automated alert and, subsequently, did they react appropriately?). One approach I have employed during security assessments is the use of test techniques of successively increasing severity. In other words, we knock on a door with increased strength and watch for (a) the moment when the knocking is noticed and (b) the appropriateness of the response actions relative to the attack type. This sort of testing supports evaluation of overall detection effectiveness.

Organizations face a clear choice in many realms of security that can be reduced to one very basic concept: Is the goal of the effort to satisfy auditors or is it to actually identify threats in progress in order to better protect information? Those that take minimalist approaches, such as subscribing to low-quality managed detection services without designing appropriate internal processes to act on the data are either kidding themselves, their regulators, or both.

Paul Rohmeyer is a faculty member in the graduate school at Stevens Institute of Technology. He provides technology risk management guidance to firms in the financial services industry, and previously held management positions in the financial services, telecommunications and pharmaceutical industries. Send comments on this column to feedback@infosecuritymag.com.

The one security blanket you won't be embarrassed to take to work.

ISACA® Certifications

ISACA certifications increase your value to employers and clients.

Being a CISA®, CISM® and/or CGEIT®:

- Counts in the hiring process.
- Enhances your credibility and recognition.
- Boosts your earning potential.

Secure Your Career: Get Certified.

Visit *www.isaca.org/infosecmag.*

Register for the 12 June 2010 exam

Final registration deadline—7 April 2010

ISACA®

Trust in, and value from, information systems

Analysis | AUTHENTICATION

Balancing Tougher Authentication with Customer Privacy

Knowledge-based authentication helps catch fraudsters, but could raise privacy concerns.

BY ROBERT WESTERVELT

LONG, FRIGID WINTERS and tough regulations forbidding utility companies from shutting off customers during the cold winter months drove a Midwestern oil company to use knowledge- based authentication (KBA) to root out fraudsters.

The company, which didn't want to reveal its identity, experienced a sudden influx of new customers just before the winter. Once it got a KBA system up and running, call center operators posed a series of multiple choice questions to people seeking new accounts. Those who could answer the questions verifying their identities were set up with service while fraudsters trying to activate delinquent accounts under fake names were quickly rooted out.

"People with large unpaid bills were trying to get their service turned back on for the winter," says Joram Borenstein, senior product marketing manager in RSA's identity and access assurance group; RSA, the security division of EMC, provides the authentication service. "While it's tough to deny heat to someone, you can't stay in business if people are trying to defraud the system."

Those who could answer the questions verifying their identities were set up with service while fraudsters trying to activate delinquent accounts under fake names were quickly rooted out.

Dynamic knowledge-based authentication, the technology that has given many financial firms a way to verify customers before approving high-risk transactions, is now being used by a broader number of firms from e-commerce websites to hospitals and telecommunications companies.

As the technology hits primetime, it's being used to verify more people and firms using it for the first time quickly learn that some of the questions being returned by KBA systems can be too probing. To eliminate false positives, those behind the software algorithms used to create verification questions are trying to

keep it sharp, tapping into an ever expanding number of data sources from credit bureau information to house sale data. Ezzie Schaff thinks social networks are next and that could rouse privacy advocates.

Schaff, vice president of risk management at online jeweler Ice.com, says he's been very cautious that his company's 16 call center operators don't turn away customers by asking prying questions. Schaff says he's conducted background checks before hiring the operators, who use KBA when handling credit applications. Extensive training is also held to ensure operators know when to ask a question and when a question digs too deep into a customer's privacy.

"With the advent of proxy servers and proxy IPs, it is getting easier and easier for people to mask their ID and their location, so we have verify they are who they say they are," Schaff says. "At the same time, we don't want to have upset customers. It's a fine balancing act."

RSA acquired Verid in 2007, a technology that mines databases and uses a proprietary algorithm to come up with verification questions. RSA's Borenstein says the company is expanding its data sources; it recently added data from boat and airplane sales and leasing databases. But he stopped short of saying data from social networks would be mined next.

Social networks themselves don't keep extensive records on account holders, but Twitter, Facebook and LinkedIn work with third-party analytics vendors, such as Omniture, (now part of Adobe Systems) DoubleClick., and Google Analytics—firms that use browser cookies, which could be used to build a unique profile on a person.

A study released last summer by researchers at Worcester Polytechnic Institute (WPI) and AT&T Labs found social networks inadvertently leaking user identities. The research worries privacy advocates who say the account numbers could be coupled with browsing data and retained in databases. Peter Eckersley, a staff technologist at the Electronic Frontier Foundation, says the study is an example of the erosion of privacy and that most people don't even know the extent to which their Internet activity is being tracked.

Whether KBA technologies begin to filter in a person's Internet activity by tapping into the data held by third-party analytics firms, or somehow mining an individual's Internet presence on Twitter, Facebook and other websites, is yet to be seen. But RSA competitor TriCipher also sees the future of authentication getting more personal. Vatsal Sonecha, TriCipher vice president of business development and product management, says library or video rental records could offer valuable data to help verify an individual's identity. However, Sonecha says he has not seen "large-scale implementations go down that path."

As knowledge-based questions get more personal, Mark Diodati, a senior analyst at Burton Group, says merchants and other users of the technology must use private data responsibly or risk facing a loss of trust with their customers. Diodati says call center operators don't have to use probing questions that may be too sensitive to the customer; they can tap the KBA system for less sensitive questions.

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

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

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

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

Check out The Academy Pro at
www.theacademypro.com

the academy pro

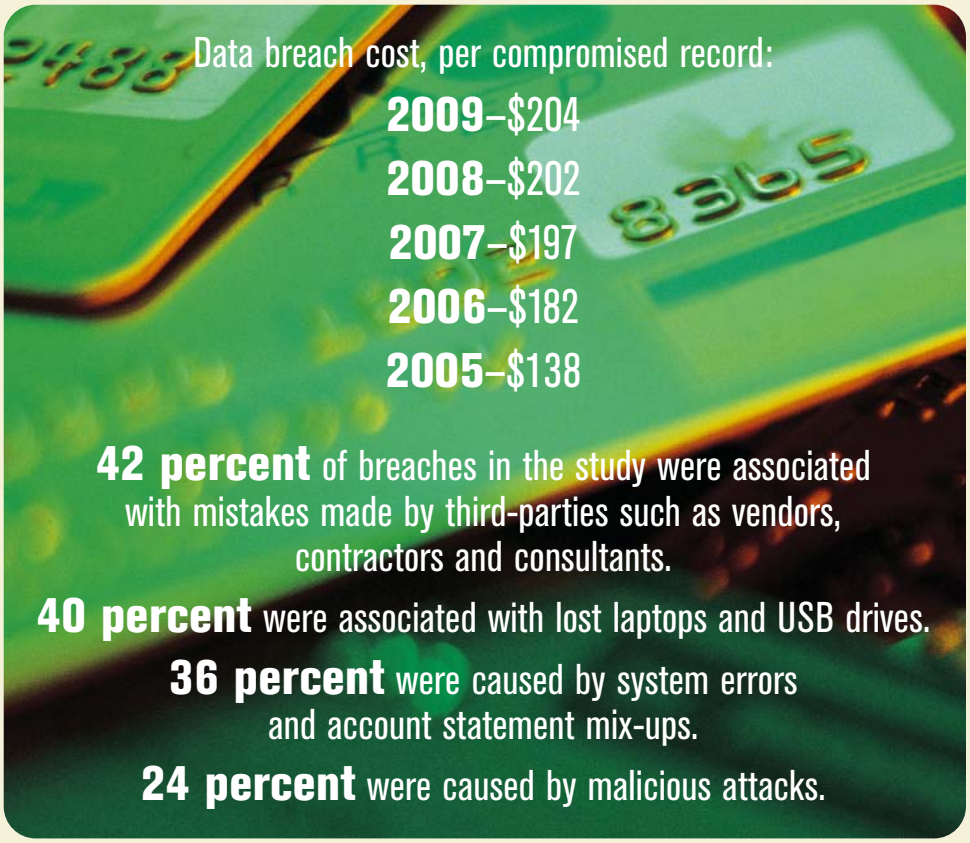
Sponsored by:

www.theacademypro.com

Continual Climb

THE COST OF a data breach increased for the fifth straight year, reaching $204 per compromised record in 2009, according to a recent study by the Ponemon Institute. The research firm interviewed 45 companies, many which had suffered multiple breaches, to compile its report. The cost includes lost business due to an incident, breach notification expenses, legal costs, new technology investments and employee education.

—*Information Security* staff



OVER-HEARD

"If handled properly, companies will survive a breach [but] there's no excuse for not taking a defense-in-depth approach toward security and maintaining a secure environment. Just because you will survive doesn't mean you'll want to go through the pain or put your customers through the aggravation of having a breach."

–LARRY PONEMON, chairman and founder, Ponemon Institute

34,000+ customers.

200 million online identities protected.

40 million authenticators deployed.

For an authentication solution that is truly strong,

Find security in RSA.

RSA®

The Security Division of EMC

www.rsa.com

Security Information and Event Management | Data Loss Prevention | Identity & Access Management

Develop an Effective Information Security Career Plan

BY LEE KUSHNER AND MIKE MURRAY

Distinct work environments and skill requirements make information security a complex career choice. A well thought-out career plan helps you achieve your goal.

WE SPEND A great portion of our lives dedicating ourselves to our information security careers. Few can argue that as a group, information security professionals are knowledgeable, passionate and dedicated to our profession. Yet for the amount of time we spend working "in" our careers, we spend proportionately less time working "on" our careers. As a result, we ignore the bigger picture: planning our careers.

The importance of career planning encompasses many of life's key components including intellectual stimulation, personal satisfaction and financial reward. Spending time developing a written career plan can provide you with an effective reference tool in your journey toward career satisfaction and professional goal attainment.

A written career plan is your personal road map designed to assist you in getting from your current information security position to your career destination. In its basic form it should consist of a baseline (your current skills and experience), a long-term career goal, and an understanding of the skill development and career experiences necessary to receive consideration for attaining your goal. The complexity of the information security profession is the primary reason that a career plan is necessary. The information security profession offers distinct work environments and skill specialties that provide information security professionals with many career choices.

The development of our profession can be summarized into four distinct employment segments:

- those providing information security directly to corporations;
- those providing information security to the government;
- those providing information security consulting services;
- those who work for information security product companies.

Since each of these specific entities have different missions, skills do not transfer that easily. There are many skill criteria that would enable someone to succeed in one of these sectors, but could work

Information Security magazine's mission is to provide security professionals with the strategic and technical vision around products and industry trends to help you do your job better. Starting this month, we're also going to help you nurture your career development. We've asked experts **Lee Kushner** and **Mike Murray**, co-founders of InfoSecLeaders.com, to contribute a bi-monthly column focused on helping you shape your skills to meet your career objectives, all within context of what's happening within the security industry. Their column starts this month with a detailed look at the importance of developing a formal career plan, to serve as your personal road map to follow as you strive to achieve your long-term career objectives and professional goals. We're anxious for your feedback, please send any comments to feedback@infosecuritymag.com.

against them in another. By taking time to plan your information security career, you can determine the work environments that align best with your career goals, personal characteristics, and provide yourself with the most flexibility for personal career choices.

In addition to the diverse work environments, the information security profession is the intersection of people, process, technology, and business. Any of these items would be difficult to master, however information security professionals are expected to be competent in all of them. Factor in differing industry regulations, evolving technologies, diverse personalities, and distinct businesses and an information security professional is left with many choices on where to focus their time and energy.

In addition to the diverse work environments, the information security profession is the intersection of people, process, technology, and business.

The development of a written career plan should help an individual identify areas of personal interest and correlate these interests with career choices that provide them with the best chance of achieving their long term career goals.

A career plan can also provide you with some guidelines for making career decisions and assessing specific career opportunities. As your information security career progresses, you will be presented with a variety of different opportunities to either utilize your current skill or develop new ones. Some of these positions can help accelerate your career progression while others may cause you to detour. In many cases, the excitement caused by the introduction of a new challenge or a new environment can cloud your judgment. When these opportunities arise, you will have the ability to consult your career plan to determine how the framework of the particular opportunity will help you address your "career gaps." Filling a career gap by developing those technical, management, leadership or general business skills you need to learn to accomplish a long-term goal will enhance your chances of reaching it.

Your career plan will enable you to think more clearly about the opportunity and its benefits, and hopefully enable you to make a better informed decision about your future and position choice.

A career plan will enable you to figure out which specific information security skill you need to develop and what experience you need to acquire. It is often easy to say "I want to become a chief information security officer," but it is another thing to fully understand the skills and experience necessary to be considered for such a position.

When you develop your career plan and identify your goal, you will need to go through a "career gap assessment." A career gap assessment will begin with an honest assessment of your current skills and experiences. This honest assessment should help you determine your personal strengths and weaknesses.

After this personal assessment is complete, you should research which skills, education, and experience would be required to achieve the position that you desire. Upon completion, you should be left with an understanding of where you are currently and what kind of commitment, sacrifice, and personal investment you would need to make in order to achieve your long-term career goal.

At the end of this exercise, you will be able to determine your personal willingness to attempt to achieve this goal. If you determine that you are unwilling to put in the necessary work and professional development to achieve this goal, you should select another goal that is better aligned with your personal level of commitment. Keep in mind that developing career goals is easy, achieving them requires a great deal of hard work.

Taking the necessary time to plan your information security career can have a dramatic impact on your professional happiness. Your career plan will serve as your personal "road map"

to follow and should enable you to make rational career decisions that will accelerate your journey towards accomplishing your long -term information security career goals.

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

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

RSA® CONFERENCE | Where The World Talks Security

SECURITY DECODED

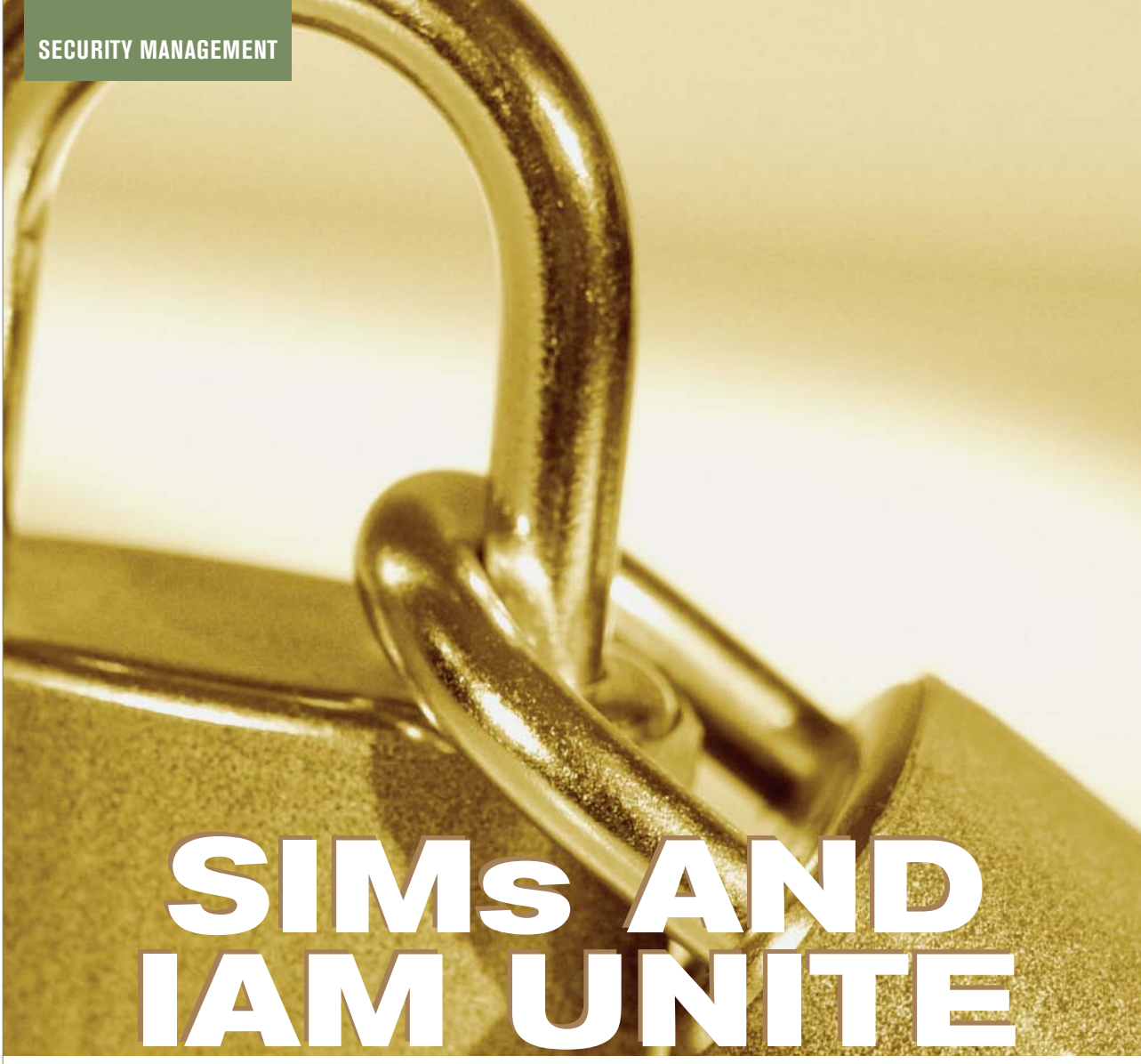
Continue the conversation.

Join us in Japan and Europe.

RSA® Conference
Japan
September 9-10, 2010
Tokyo, Japan

RSA® Conference
Europe
October 12-14, 2010
London, U.K.

www.rsaconference.com



SIMs AND IAM UNITE

Joining security information management with identity management ties policy violations and vulnerabilities to user activity.

BY RANDALL GAMBY

TRADITIONALLY WITHIN COMPANIES, the IT security organization has mitigated risk through its set of policies, procedures and technologies, while user access and authorization has been controlled through the use of identity management processes and technologies managed by the IT organization. By bringing these two functions together, organizations increase their effectiveness to a level that is greater than the sum of the parts.

IT security departments have begun deploying security information management systems (SIMs) within their organizations to monitor and report on information asset vulnerabilities. SIMs focus on remediating risk through scanners placed throughout the organization to gather data on information policy violations and then reporting on overall vulnerability to defined risks using management scorecards. While becoming more and more effective, these technologies act only as an early-warning radar system by recognizing when a large policy violation activity has occurred—which is then followed by a triage process to verify and remediate the problem.

Also today most SIMs have been configured only to concentrate on identifying incidences where sensitive information is attempting to leave the company's domain from authorized channels. While this reporting is important in any organization, ultimately managers are looking to SIMs to provide more proactive management of asset vulnerabilities and controls, rather than just reporting on incidents, to reduce fraudulent activities. But this functionality will go unrealized until the human component of security can be combined with the information views offered by today's SIM tools.

As security managers look inside their organizations to find where useful user authorization and role information can be found to be married with their SIMs' data, they're finding that the most complete information doesn't come from the traditional human resources (HR) systems, whose data is more functional in nature, but from IT's identity and access management (IAM) systems. These systems, unlike the HR tools, are geared toward identifying the role or responsibility a person plays within the organization in order to grant them proper access to the systems and information they need in order to perform their duties.

In the past this access was granted through managing a series of entitlements, coarse-grained access rights. But the current trend is to consolidate multiple entitlements under a single role-based access and control (RBAC) definition for consistency and manageability. For example, if all Web-development engineers need the same 20 entitlements to the same 10 systems to do their job, it is easier to consolidate all these entitlements under a single RBAC object, such as "Web engineer" and assign or remove their accounts using this single value in the account request used by their provisioning process than managing 200 entitlements (20 entitlements x 10 systems). By basing user identity and access on an RBAC model, IT processes for on-boarding, changes and off-boarding user accounts become more timely, greatly simplified, and made more effective.

LINKING SIM AND IAM REDUCES RISK

So how can these two disparate technologies work together to reduce risk to the organization? SIM technologies are the central tool used by security managers to

PROCESS

Triage

IT security generally verifies and remediates a policy violation discovered by a security information and event management system in the following manner:

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

recognize when a policy violation activity has occurred. However, in order to fix an identified vulnerability, a triage process must be followed to verify and remediate the problem. This typically requires an IT security person to delve deeper into the information provided and determine the downstream effects of the activity *(see "Triage," p. 21)*.

While this is process is usually effective, SIM tools deal with information and systems, not people. Many times, the IT security person assigned the remediation activity doesn't have access to the knowledge of whether a person was involved, when they were involved, and which person initiated or caused the violation to occur. If a person is involved then they have to ask a series of questions. Was it a fraudulent activity perpetrated by a disgruntled insider? Did an unauthorized person from outside the company gain access to an internal system? Was this a case of an authorized person doing an activity that the general user population isn't authorized to do, for example an HR person sending tax identification numbers to an outside benefits partner? Did a developer have an error in his programming that caused sensitive information to be sent to another application as part of the data feed from one system to the next? Because this information isn't in the native SIM solution, the IT security person must take the time to track down this information causing undue delays in determining if this incident does indeed pose a serious risk to the organization.

By having access to the organization's IAM information, the SIM system has access to not only which user maps to the IP address/ username in the incident report, but it can also determine from their role(s) whether this was an authorized activity or not.

Take, for example, when a data loss prevention (DLP) tool identifies to the SIM system that credit card information was found in an information packet destined for a system that is outside the domain of the organization and was blocked. While the SIM system will identify the date, time, type of violation, destination IP address, source IP address, username and severity of violation, it doesn't tell who the person was that initiated the transaction or whether the person was authorized to send out this type of information. By having access to the organization's IAM information, the SIM system has access to not only which user maps to the IP address/ username in the incident report, but it can also determine from their role(s) whether this was an authorized activity or not.

This means that IAM technologies take on a role as a feed to the SIM system. They enhance and provide the information needed for the SIM system to provide more complete information so incidents can be remediated quicker with higher confidence factors. SIM technologies can also benefit IAM technologies by identifying issues which may not be inherently obvious such as separation of duties (SoD) violations—for example users who have access to information which they also

administer—or flagging activities of a system administrator who manually bypasses authorization controls on the system they manage.

What's more, through their information channel monitoring capabilities, SIM technologies can help organizations monitor what employees are doing, even when applications move into the cloud. They can also give special attention to information and activities being conducted by certain outsiders within the boundary of the organization through these persons' roles established by the IAM systems.

RECONFIGURE IAM TO WORK WITH SIMs

But in order to achieve the benefits explained above, a certain minimum level of functionality must be deployed. As IT security personnel look at using RBAC and IAM technologies to help in providing better controls over user compliance for authorized access to information, they're finding their current IAM deployments aren't configured properly to help address the threats and unauthorized exposure of information that the SIM technologies are looking for. This means there are some basic limiting factors that must be addressed before any work can be done in integrating these two technologies to meet their needs.

- **UNIQUENESS:** One problem is the fact that no two companies are the same. That means defining a set of user activities to watch, or information assets that must be protected, monitored, reported on and controlled, will vary greatly, even within like industries. Details around the size of the organization, the corporate culture and management style, physical location of facilities, number/type of applications and services, types of clients and customers, regulatory compliance and reporting requirements, third-party partnerships, etc. can greatly influence how IT security personnel manage asset vulnerability reporting.

While IAMs prevent unauthorized users from accessing unauthorized systems, they generally have difficulties managing authorized users using data in an unauthorized way.

- **AUTHORIZED ACCESS:** While IAMs prevent unauthorized users from accessing unauthorized systems, they generally have difficulties managing authorized users using data in an unauthorized way. For instance, an account executive needs full access to a company's customer relationship management (CRM) application to perform their duties. But detecting that this person has decided to leave the company and is copying their client list to an outside source so they can take the list with them when they leave is almost impossible to detect within the IAM tools.
- **RBAC IS AN ART:** RBAC projects are significant activities and companies are still learning how to classify user responsibilities and roles. In many cases, RBAC projects are working to extend this control mechanism across the enterprise. This means there may still be large populations of users within an organization that are not being managed by roles. In addition, knowledge workers, program managers and executives are especially difficult to pigeonhole due to their ever-changing job responsibilities. If a

SIM tool wishes to use RBAC objects in understanding user functions and responsibilities, the variability of a person's role must be understood to prevent false positives.

• **REDUCED FUNCTIONALITY WHILE INTEGRATING:** It has taken years to deploy, configure and tune IAM and SIM tools to perform the complex functions they do today. This means that in order to integrate these two technologies, great care must be taken to ensure that any activity to integrate these two technologies doesn't cause them to lose some of their current capabilities while trying to enhance the security of the organization.

• **SCOPE OF COVERAGE:** While IAM and SIM technologies are becoming an integral

1 Bank, 3 SIMs, 100,000 Nodes, 40 Million Events

Scale is a more pressing need than new functionality for one financial services firm.

YOU'D BE HARD PRESSED to find a better proving ground for new functionality in a security information and event management system such as identity management than the Bank of New York Mellon.

The global financial services company's uses three SIM products, including one from ArcSight that monitors more than 100,000 nodes, including endpoints, server infrastructure, NAC, DLP, antimalware and more. VP of global security architecture Daniel Conroy says integration with IAM and other technologies such as fraud monitoring are the way SIMs have to go. But those technologies, identity management in particular, have to get their act together before it can happen.

IAM's challenges aren't limited to integration and implementation issues because of the diversity of roles in any large organization, and the fluid nature of user permissions and access control.

"Merging with identity management is the way it has to go down."
–DANIEL CONROY

"Merging with identity management is the way it has to go down," Conroy says. "I'd like to see SIMs ultimately be more interactive with these [other] tools, be more self-aware and for example, go to asset management systems and pull data from there versus manually doing it. More plug and play out of the box."

BONY Mellon is certainly a SIMs power user given its massive global infrastructure. Conroy says his company's SIM handles upwards of 40 million daily events, a number he expects to triple soon as they begin monitoring outbound connections as well.For now, Conroy wants to see his SIM chug along; scale and quality correlation, analysis and reporting taking precedence over new capabilities.

"You need it to scale to a certain number of events per second. With some products if it comes above a certain number of events per second, it can crush the box and become a problem," Conroy says. "Events per second is what SIM comes down to. If you have analysts looking at data from 16 different products in one console, there's your ROI right there." ›

–MICHAEL S. MIMOSO

part of any organization's security and IT infrastructures, in most organizations they are not deployed across the entire enterprise. Certain lines of business, geographic locations, agencies, third-party partners and others may not have one, or both, of these technologies deployed, or they may be deployed unequally, limiting their use for these domains.

• **ROLE VS. ACTIVITY:** Just because the SIM technology detects an activity and uses a RBAC role to determine if the user involved in this incident is authorized to perform the activity detected, in the case of an unauthorized activity, the SIM system will not know how broad the user's access is in determining the degree of the vulnerability and the exposure of risk to the organization. This causes IT personnel doing remediation tasks to ask: Does the remediation need to include impeding the user from performing additional activities that caused the incident by shutting off their access? Or was this activity a single occurrence caused by not educating the user on proper usage procedures?

While the list above outlines some of the main limiting factors in integrating SIM and IAM technologies, the reality is as security and IT personnel meet to discuss the merger of their respective domains, many other organization-specific issues are sure to surface. Having good communications between these two groups is essential in order to move forward in integrating these two technologies. Understanding and fully documenting these limiting factors is also crucial as organizations move forward integrating their SIM and IAM technologies.

ESTABLISH CONTROLS, FRAMEWORKS FOR SIM-IAM COMBO

Combining SIM and IAM provides the link needed to tie user access to data use and exposure. While understanding any limiting factors is critical to the success of any deployment, it's not just a case of doing an integration project between the two but understanding the role each plays in securing the organization and which functions each provides as they begin to work together. This process starts by understanding the level of risk IT security management is willing to take and understanding any potential asset vulnerabilities. No technology can fully eliminate vulnerabilities and attacks. This means management (commonly referred to as Policy Management Authorities - PMAs) must establish the controls and frameworks around how the technology tools will be used. The two most common standards that are followed are COSO (Committee of Sponsoring Organizations) and COBIT (Control Objectives for Information and Related Technologies) standards for controls and frameworks. It's imperative these controls be defined before any additional work is done.

Combining SIM and IAM provides the link needed to tie user access to data use and exposure.

Once the controls are in place, IT security management and personnel must establish areas of control around any identified risks or asset vulnerabilities (also

known as Policy Decision Points - PDPs). This activity directs any tools to be used to the areas of the organization that are most vulnerable, or which must be monitored due to regulatory and other business requirements. As an organization's monitoring capabilities mature, the scope of monitoring can then be systematically expanded to include other areas of the organization including subsidiaries, partners, suppliers and software as a service (SaaS) cloud environments.

With the definition of the control mechanisms completed, an organization can now execute its enforcement through policies and tools (also known as Policy Enforcement Points - PEPs). SIM and IAM technologies fall within this realm. By providing an integrated enforcement front, the organization can now monitor, detect, and remediate incidents efficiently and have a more complete view of vulnerabilities and attacks. In addition to integrating IAM information into the SIM systems to combine human interactions with the information being monitored, scorecards and dashboards can be established to identify incidents as they occur as well as let IT security management know how well the organization is protecting its most guarded information. In addition, by bringing these two technologies together, security managers can now take on a proactive stance to IT security by identifying that not only is information safely flowing through the right communications channels, but also that users are being properly authorized to access only the information they're entitled to see.

By providing an integrated enforcement front, the organization can now monitor, detect, and remediate incidents efficiently and have a more complete view of vulnerabilities and attacks.

While SIM and IAM integration can provide an organization with a more complete view into their IT security effectiveness, there are many other security mechanisms that will help complete the picture. A few of these include: good policies and procedures, physical security services, HR employee background checks, application rights management, and of course the diligence of the IT security personnel. But just as the U.S. government is striving to bring together the information collected from its various intelligence organizations to identify risks to the United States, integrating an organization's various control technologies, such as SIM and IAM, will increase the security effectiveness of the organization against inside/outside attacks and shore up previously unknown vulnerabilities.

Randall Gamby is an enterprise security architect for a Fortune 500 insurance and finance company who has worked in the security industry for more than 20 years. He specializes in security/identity management strategies, methodologies and architectures. Send comments on this article to feedback@infosecuritymag.com.

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

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

FOR MORE INFORMATION CONTACT: SECURITY@GLASSHOUSE.COM

WWW.GLASSHOUSE.COM

GLASSHOUSE

Proving Your Worth

Follow these steps to create a successful security metrics program.

BY ANDREW JAQUITH, FORRESTER RESEARCH, INC.

SECURITY BUDGETS have proven to be more resistant to the recession than many areas of IT, but they haven't been completely recession-proof. Security spending, which rose like a rocket ship with double-digit increases from 2002 through 2007, started to sputter about two years ago. Organizations report that discretionary security projects have been delayed or "sent back to the lab" for further evaluation. For 2010, Forrester Research expects that overall security budgets will rise less than 5 percent over 2009—higher than in the previous year, but not by much.

The reluctance to increase security budgets places increased pressure on security managers to justify their projects. Security, sadly, is one of those professions where victories are taken for granted and go unnoticed, but failures are embarrassingly public. To the untrained eye, security

staff, technologies and processes cost a lot of money but produce little tangible output on a day-to-day basis, other than a vaguely satisfied feeling that "nothing bad happened" today. As a result, smart security managers, sensing sudden vulnerability in their budgets, seek better ways to measure and prove the value of what they do every day.

But before plunging into a security metrics program, there are a number of issues to keep in mind. We'll look at some of the missteps that can lead to frustration and failure and the ingredients for an effective program.

METRICS MISTAKES

Some enterprises, daunted by the challenge of "measuring nothing," simply haven't made metrics a priority yet. Other organizations start ambitious security metrics programs but are tripped up by three major pitfalls, especially in the early stages of program development:

- **Try to boil the ocean.** Faced with the pressure of not wanting to miss something important, enterprises try to measure "everything" they can think of: every threat and vulnerability class, dozens of operational metrics ranging from patching to spam to identity management, and multiple takes on how to quantify application risks and defects.
- **Pick convenient metrics, rather than meaningful ones.** Nearly every security product enterprises own has some sort of reporting feature that generates numbers the vendor deems important. It's easy to use these as a starting point, and in some cases they make good metrics. But most are just statistics that you can file in the "fun facts of the day" folder. Your boss does not care how many spam e-mails your gateway blocked or the number of "policy violations" your desktops have—whatever those are.
- **Miss the forest for the trees.** Good security metrics should have five qualities. Most organizations know how to pick metrics that satisfy the first four qualities: namely, that they are expressed as numbers, have one or more units of measure, are measured in a consistent and objective way, and can be gathered cheaply. But only a few pick metrics that satisfy the most important criterion: contextual relevance. That is, the metrics must help someone—usually the boss—make a decision about an important security or business issue. Too many organizations use metrics to erect Byzantine temples to "security-ness" that measure the minutiae of what they understand rather than what the boss needs to know. Failure to pass the "so-what" test makes a metric potentially interesting but not insightful.

LESSONS LEARNED

The truth of the matter is that setting up a security metrics program is not easy. But it need not be stressful either. Putting together a metrics program means having the right perspective. Here are four lessons drawn from the experiences of enterprise security leaders:

- **Clarity and context eases acceptance.** The meanings of some security metrics are very clear. It's easy to understand what the metric "average time to patch a workstation" means and how it might be derived; the units of measure are clearly expressed. The meanings of the word "patch" and "workstation" need no explanation. But what about an "application risk score" of 93? How much better is it compared to a score of, say 80? In these cases, experienced program managers make a point of explaining how the scores are derived. Their exhibits and dashboards clearly and succinctly explain what went into

their less-obvious formulas, and how readers should interpret the results.

- **Insights flow from comparisons.** Yale Professor Edward Tufte wrote in his superb book *Envisioning Information*, "If the numbers are boring, then you've got the wrong numbers." One of the best ways to gain real insights about the health of the security program is to stop treating the organization as a monolith. When you slice security metrics by business unit, division, manager or geography, revealing patterns always pop out. Which of your divisions are stars, and which are "cowboys" or renegades? By comparing different groups against each other, metrics that you are measuring become a lot more interesting, and insights readily apparent.
- **Less is more.** In the computing and consumer electronics world, fans of Apple's products appreciate their minimalist, clean designs and streamlined user interfaces. What makes Apple's products special is not what the company puts in, but what it leaves out. Similarly, New England Patriots coach Bill Belichick's weekly game plans ask team members to excel at just a few things. "If you do these three or four things, you will win," he tells his players. Successful security measurement programs work the same way. Many, many factors go into making security organizations work well. But effective measurement programs focus teams by restraining the number of measures they have to worry about.
- **Balanced Scorecards keep everything in perspective.** Nearly 20 years ago, Robert Kaplan and David Norton of Harvard University developed a concept called the "Balanced Scorecard." Invented as a better way to measure company performance, the Balanced Scorecard sets up four complementary perspectives that are critical to predicting long-term success: Financial, Customer, Internal Processes, and Learning and Growth. Adapted to security, the Balanced Scorecard helps bridge the gap between information security and management. Response to the Balanced Security Scoreboard concept in Forrester workshops has been electric.

CREATING A BALANCED SECURITY SCORECARD

What goes into a security scorecard—"balanced" or otherwise? Because every organization is different, the composition and number of metrics depend very much on the business context and priorities of each company. That said, successful scorecards are concise, clear and comprehensive. They don't bore readers with their length or baffle them with mystery terms. And they include enough key performance indicators so that the totality of the security program's activities is covered. When starting a security measurement program, an organization should:

- **Take cues from management.** The security organization, and the senior management team it reports to, has a set of principles that shapes what the security program does and the impulses it responds to. These principles might be concerned with protecting information: "Be a good custodian of our patient's medical records" or "Protect our innovations no matter what." It might be concerned with reputation ("just keep our company out of the papers"), service excellence or cost control. These principles influence which metrics to select for the Financial and Customer perspectives in particular. Anticipating what hot-button issues the management team responds is key.
- **Pick a small number of metrics for each perspective.** The four perspectives of the Balanced Scorecard enforce an ordering principle on the composition of the metrics you

DASHBOARD

The Balanced Security Scorecard

Sample metrics for each perspective

Financial perspective
- Cost to secure workstations, per host
- Security assessment costs
- Costs to secure revenue-generating systems
- Cost of compliance activities

Internal Process perspective
- Average time to patch workstations
- Percentage of endpoints without any severe vulnerabilities
- Cycle times to deprovision users
- Average time to fix critical vulnerabilities, by system type
- Cost of critical data leak incidents, per incident

Customer perspective
- Number of reportable privacy breaches
- Audit items that are customer or partner related
- Regulatory audits completed per period

Learning and Growth perspective
- Number of security architecture consultations by business units
- Percentage of users with weak passwords
- Average time elapsed since last security class, by user or group

select for your dashboard. You can't be "over-weighted" in the Internal Process perspective because it means you skimp on Learning and Growth. But at the same time, too many metrics overall make the scorecard too difficult to comprehend. What works best is to have three or four metrics for each of the four perspectives. Figure 1 shows a sample of the kinds of metrics a security manager might want to use.

- **Mix perennials and seasonal metrics.** Building a metrics program is like tending a garden: To keep it fresh and interesting, seed it with a base of metrics that you can always rely on (the perennials), but sprinkle in additional metrics for short periods of time. "Perennial" metrics should reflect the long-term managerial priorities for the security organization, such as keeping tabs on staffing levels, tracking compliance with benchmarks, and monitoring risk assessment scores. "Seasonal" metrics should be added to shine a spotlight on operational areas that need near-term improvement, such as data leakage, application security or abuse of social media.
- **Use sunshine to create peer pressure.** As mentioned earlier, slicing and dicing metrics by business units or geographies is a terrific way to make the data more interesting. But it has another side effect: When you share data on a cross-section basis, you create a subtle form of peer pressure that motivates the laggards to perform more like the leaders. Nobody wants to be in last place. One company several years ago made a game of it: Each manager received a T-shirt with his or her application vulnerability score printed on it. You can imagine the fun at the meeting as managers introduced themselves by their numbers instead of their names ("Hi, I am '53'. What's your score?") to break the ice. Then they swapped lessons learned about why they had scored comparatively well or

poorly. Now in truth, a T-shirted "sunshine policy" may not be appropriate for every organization. The key, though, is to share cross-sectional performance information in a judicious and non-judgmental way.

GET GOING

If you don't have a metrics program already, setting one up from scratch might seem hard to imagine, and even harder to implement. But measurement is a lot like physical fitness. While visible progress won't be instant, there is no excuse preventing you from starting today. Start by figuring out what data sources you have, what your team (and bosses) value, and what the scorecard ought to look like when you are done. Use the Balanced Scorecard as an organizing principle. There is no time like the present and the payoff will be invaluable.›

Andrew Jaquith is a senior analyst at Forrester Research covering client and data security. He is the author of Security Metrics: Replacing Fear, Uncertainty and Doubt. *Send comments on this article to feedback@infosecuritymag.com.*

Secure your business in

15 MINUTES.

Get around-the-clock protection.

Managing a mid-size business and keeping it secure can seem like two full-time jobs. Give McAfee just 15 minutes a day and get around-the-clock protection. With daily security practices, you can protect your networks, systems, data, email, and web... then get back to business.

Learn more: www.mcafee.com/mid/secure15

McAfee Secure in 15 toolkit:

Learn about the Secure in 15 methodology, get a daily practice calendar, a helpful practitioner's guide specifically developed for EMEA organizations, and much more. Start proactive security management today.

Visit www.mcafee.com/mid/secure15

McAfee®

HIPAA GETS SOME TEETH

The HITECH Act expands on HIPAA's security requirements and increases penalties for non-compliance.

BY MARCIA SAVAGE

THE HEALTH CARE INDUSTRY was buzzing with the news: For the first time, a hospital was being audited for compliance with HIPAA security requirements. The audit of Piedmont Hospital [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1268985,00.html] in Atlanta by the U.S. Department of Health and Human Services' inspector general in 2007 was surprising for hospitals, health insurers and others in an industry accustomed to a lack of enforcement of federal privacy and security requirements.

A year later, HHS took another unusual step, meting out a $100,000 fine to Seattle-based Providence Health & Services [http://itknowledgeexchange.techtarget.com/security-bytes/hipaa-violations-cost-seattle-health-care-provider/] for HIPAA security and privacy violations. The organization had lost backup tapes, optical disks and laptops containing unencrypted protected health information on more than 360,000 patients.

But those enforcement actions could be small potatoes compared to what's ahead. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act signed into law last year, earmarks about $19 billion in incentives to encourage adoption of electronic health record technology but also expands on HIPAA's security and privacy requirements. In addition to instituting new breach notification rules and extending the rules to health care business associates, HITECH implements a new tiered system that increases civil monetary penalties for noncompliance and also allows state attorney generals to file civil actions for HIPAA violations.

"HITECH is perceived as the enforcement arm of HIPAA," says Barry Runyon, research vice president covering health care IT at Gartner. "The stakes are higher and more people can enforce it.

"What it's done has kind of jump-started HIPAA. Health care delivery organizations' programs languished for a while," he adds. "When there's no enforcement, people tend to get complacent. HITECH is making them revisit their security plans and look at their controls—essentially what they should have been doing."

Let's take a look at the ramifications of the HITECH Act on security and privacy in the health care industry and its impact so far.

HIPAA: UNEVEN COMPLIANCE

For years, organizations that had to comply with HIPAA were frustrated not only by the lack of enforcement but the lack of specifics in the federal law's requirements for protecting electronic personally identifiable health information. The Health Insurance Portability and Accountability Act [http://www.hhs.gov/ocr/privacy/] was enacted in 1996; health care providers, health plans, clearinghouses and other covered entities were required to comply with the law's privacy rule in 2003 and with the HIPAA security rule in 2005.

"HIPAA security [compliance] is all over the map. The security rule is just too open to interpretation."

–BRYAN CLINE, director of information security, Catholic Health East

"HIPAA security [compliance] is all over the map. The security rule is just too open to interpretation," says Bryan Cline, director of information security at Newtown Square, Pa.-based Catholic Health East.

Some organizations do the bare minimum to comply while some take a mature, risk-based approach to information security and devote enough resources and training to have a strong program, he says.

Historically, the health care industry hasn't spent as much as other industries on security, says Khalid Kark, vice president and principal analyst at Forrester Research. "There's always this tension: Do you want to improve service and how you treat people, or would you rather spend that money on security?"

A survey of 196 health care IT and security professionals [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1373822,00.html] by the Chicago-based nonprofit Healthcare Information and Management Systems Society (HIMSS)

released last fall showed that security accounts for three percent or less of overall IT spending in a majority of health care organizations.

Even if HIPAA wasn't ambiguous, it had "no teeth or enforcement," says David Finn, health IT officer at Symantec and former CIO at Texas Children's Hospital. "The fines weren't significant enough to raise the risk management flag for a lot of institutions." HITECH removes a lot of ambiguity with its breach notification rules and increased penalties, he says.

Even if HIPAA wasn't ambiguous, it had "no teeth or enforcement."

–DAVID FINN, health IT officer, Symantec, and former CIO, Texas Children's Hospital

BREACH NOTIFICATION

Under rules released last August by HHS [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html], an organization with a breach involving unsecured protected health information (PHI) must notify the affected individuals. The notifications must be provided no later than 60 days following the discovery of a breach and must include a description of the breach and what the organization is doing to investigate it, among other details. If more than 500 individuals are affected, then the organization must notify major media outlets in affected states and HHS; HHS will list the breaches and the entities involved on its website.

"That's not something any hospital wants to do," Finn says of the media notification.

Organizations need to have a process to assess whether there's been a security breach that requires notification, says Kathryn Coburn, founder of Pacific Palisades, Calif.-based Coburn IT Law, which focuses on health care IT. The security or privacy of protected health information is deemed to be compromised only if the disclosure poses a significant risk of harm to the individual, she says.

The process requires a risk assessment that considers the amount of data lost and potential exposure of that data to determine whether notification is required, says Joseph Granneman, CTO/CSO of Rockford Health System in Rockford, Ill.

"If a folder of information is left at a restaurant and someone returns it to you, there may not be much risk for that patient information. Whether you consider this a breach or not will be based on what the information was," he says. "If it was just a listing of names without other financial/medical identification, it may not be considered a breach because there is little risk to the patient."

Notification isn't required if the PHI is unreadable or indecipherable through encryption according to National Institute of Standards and Technology (NIST) standards [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html]. Paper records must be shredded so the PHI can't be reconstructed, and electronic media purged or destroyed per NIST guidelines.

Many health care organizations are looking closely at encryption and need to assess the appropriate levels of encryption for their systems, says Beau Woods, solutions architect for SecureWorks, an Atlanta-based security-services firm. "Some of the older software doesn't allow you to encrypt to a standard that is compliant with HITECH," he notes.

HIGHER PENALTIES

HITECH ups the ante on enforcement and penalties for HIPAA violations in several ways. The new law provides a tiered system of civil monetary penalties based on the level of knowledge of the non-compliant organization (from knowing to willful neglect), and corrective actions taken, says Lisa Gallagher, senior director of privacy and security at HIMSS.

For example, if a violation was due to reasonable cause and not willful neglect, the penalty is $1,000 for each violation. But if the violation was due to willful neglect and not corrected, the penalty is $50,000 per violation with a maximum fine of $1.5

TOOLS

HITRUST Framework aims to bridge the compliance gap

Tool updated to reflect new HITECH requirements.

HEALTH CARE ORGANIZATIONS looking for some help in meeting HIPAA and HITECH security requirements might want to check out the Health Information Trust Alliance (HITRUST) Common Security Framework.

Frisco, Texas-based HITRUST, in collaboration with health care, IT and professional services executives, introduced the CSF last year. The CSF, designed to be used by any organization that stores or exchanges personal health or financial information, incorporates security requirements from HIPAA and HITECH as well as other standards and frameworks, including the Payment Card Industry Data Security Standard, NIST and COBIT.

HITRUST released the 2010 version of the CSF last month with updated references to HITECH and improvements based on industry feedback. The CSF is available free of charge at HITRUST Central [https://www.hitrustcentral.net/].

Daniel Nutkis, HITRUST CEO, says HITRUST has worked to reach out and educate organizations on risk management and how the CSF can help. Tracking the level of adoption is difficult, but HITRUST is working with about 30 states on their use of the CSF, he says. Under HITECH, states' health information exchanges and the organizations that connect to them must be secure.

Khalid Kark, vice president and principal analyst at Forrester Research, says the CSF fills a void in the health care industry and that adoption of it by states could have a huge impact on its acceptance.

HITRUST also offers the CSF Assurance program, which the company says can help streamline the process of security assessments for health care organizations and their business associates. The program, which has authorized CSF assessors, aims to provide a consistent approach to assessing and reporting compliance to multiple parties.

The HITRUST CSF "indicates there's a focus on security in our industry that didn't exist in the past," says David Finn, health IT officer at Symantec and former CIO at Texas Children's Hospital.

–MARCIA SAVAGE

million for all such violations in a calendar year. Previously, the civil penalties for HIPAA security and privacy violations set a maximum civil fine of $100 per violation and up to $25,000 for all violations of an identical requirement during a calendar year, according to Gallagher.

HIPAA also provided for criminal penalties of fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intention of selling it for commercial or personal gain, or for malicious purposes. Previously, the U.S. Justice Department ruled that a covered entity could be criminally liable for HIPAA violations, not individuals, but HITECH makes it clear that individuals—hospital employees or others—can be held liable, Gallagher says.

"There are some real teeth in there," Symantec's Finn says.

In addition, the new law broadens the number of potential HIPAA enforcers. It allows state attorney generals to file a federal civil action on behalf of residents of their states who they believe were adversely affected by a HIPAA violation, Gallagher says. Already, one such lawsuit has been filed: In January, Connecticut Attorney General Richard Blumenthal sued Health Net of Connecticut [http://www.ct.gov/ag/cwp/view.asp?Q=453916&A=3869], alleging the company violated HIPAA when it lost a portable disk drive containing health and financial information of about 446,000 enrollees last May.

PRIVACY

New disclosure rules

Organizations will need to provide three-year histories of disclosures of protected health data.

AMONG THE Health Information Technology for Economic and Clinical Health (HITECH) Act's expanded privacy requirements are new rules for disclosure of protected health information (PHI).

Organizations using electronic health record (EHR) technology must be able to provide a patient with a three-year history of PHI disclosures, including disclosures previously considered exempt, such as those for treatment like lab work, and those made for payment purposes.

"That will require logging of all those disclosures and creation of a process to prepare a disclosures list," says Lisa Gallagher, senior director of privacy and security at the Healthcare Information and Management Systems Society (HIMSS).

"The volume of audit logging that is going to is kind of mind numbing," says David Finn, health IT officer at Symantec and former CIO at Texas Children's Hospital. "No human could comb through all that, so at some point it has to be automated."

Also, if a company keeps a patient's data in electronic format, it must provide an electronic copy if the patient requests one. "You can't just print something on paper," Gallagher says.

Federal guidance on accounting of disclosures is expected June 30.›

–MARCIA SAVAGE

"There's a bigger army coming after you now," Finn says of the new state-level authority to enforce HIPAA.

Having enforcement at the state level increases the chances that a health care organization's HIPAA compliance might be examined, which could help bolster a security department's ability to win funding, says Jeff Pentz, assistant director of information technology of the University Health Center at the University of Georgia.

"More teeth, more money," he says. "Going to your administrator with details of the HITECH Act may help to get more funds for security or at least reduce the amount that might be cut for security."

HITECH also requires the HHS secretary to provide for periodic audits to ensure covered entities and their business associates comply with HIPAA's security provisions.

THIRD-PARTY SECURITY

Perhaps one of the most far-ranging changes HITECH makes is in its extension of HIPAA's provisions to business associates. Effective Feb. 17, companies that provide services such as claims processing and billing and handle personal health information for health care providers are directly covered by the HIPAA security rule.

"The biggest impact the HITECH Act will have on health care companies are the

THREATS

Study reveals increased attacks on health care

SecureWorks detected doubling of attacks targeting its health care clients last year.

CYBER ATTACKS targeting health care organizations doubled in the fourth quarter of last year, according to a data compiled by Atlanta-based SecureWorks.

The company's findings were based on a 12-month study of 38 of its health care clients using the SecureWorks' Managed Intrusion Detection and Prevention service. Attempted attacks increased from an average of 6,500 per health care customer per day in the first nine months of 2009 to an average of 13,400 per client per day. In other industries, attempted attacks did not increase in the fourth quarter.

From October through December 2009, SecureWorks blocked hundreds of SQL injection and Butterfly/Mariposa bot malware attacks launched at its health care clients, according to Hunter King, SecureWorks security researcher.

Criminals can use SQL injection attacks and the Butterfly/Mariposa malware, which SecureWorks says surfaced last fall, to steal sensitive data. Health care companies often store valuable data and have a large attack surface because of the nature of their business, making them targets for cybercriminals, the company says. ›

–MARCIA SAVAGE

requirements on third-party security," Kark says. That's a challenge, even for companies with mature security programs in other sectors, he adds.

For CIGNA, the expanded requirements for business associates cuts both ways. The health insurer is both a covered entity that works with vendors that handle protected health information and a business associate in cases where it operates as a third-party administrator for clients who fully insure their workforce.

"We are now looking at not just being a covered entity but also a business associate under those enhanced provisions," says Georgia Dodds Foley, chief compliance, ethics and privacy officer at CIGNA."We want to make sure with both of those hats that we're doing what we need to do to evaluate our current processes, programs, and documentation."

That's meant verifying all its business associates, making sure any necessary contractual amendments are made or additional oversight is added. It's also meant dealing with a lot of contract amendments from clients for whom it is a business associate, which is administratively complicated, Dodds Foley says.

Despite the complications, the entire industry is dealing with them at the same time and "there's a certain amount of collegiality and [sense of] community going through the compliance efforts," she adds.

However, Gallagher of HIMSS says many health care business associates aren't aware of their HITECH obligations. A survey by HIMSS Analytics, a HIMSS subsidiary, last fall showed that while many health providers are aware of the new requirements, few business associates are.

ELECTRONIC HEALTH RECORDS

Many health care providers, of course, are focused on HITECH's incentives for "meaningful use" of EHR technology. Some companies have calculated that the combination of federal reimbursements and efficiencies gained in switching to electronic health records would mean a big return on investment, Forrester's Kark said.

In late December, the Centers for Medicare & Medicaid Services (CMS) released proposed provisions for meaningful use of EHR technology [http://edocket.access.gpo.gov/2010/E9-31217.htm] and the Office of the National Coordinator for Health Information Technology (ONC) released an interim final rule [http://edocket.access.gpo.gov/2010/E9-31216.htm] that specifies standards and certification criteria for EHR technology. While ONC's document includes a baseline of security controls such as encryption and authentication, the meaningful use document only cites the need for a security risk assessment, which is what HIPAA requires, Gallagher says.

Catholic Health East is working to fully understand the meaningful use criteria before conducting a gap analysis, Cline says. "Probably every hospital in the country is doing this but apparently working in a silo," he says, adding that industry-wide collaboration would be helpful.

CIGNA's operations include some health care delivery facilities, which are ready to do what is known to be required for EHRs at this point, Dodds Foley says. But like other health care organizations, it's waiting for additional federal guidance on EHR

standards for other types of providers, like pharmacies, which likely won't be released until later this year. The company has project plans and has done some high-level gap assessment work, but has no choice but to take a wait and see approach in that area, she says.

FIRST STEPS

The federal schedule for incentives is accelerated, but compliance with HITECH will be a long-term process, Kark says. In building out compliance programs, organizations should focus on process rather than technology, he says.

"Don't lead with technology," Kark says. "Build a program and use technology to augment it."

Gallagher says meeting HITECH's security requirements require a lot of work and organizations will be preoccupied with establishing meaningful use of EHRs, which involves extensive requirements for quality and efficient health care delivery. But the basic requirement for a security risk assessment is something that companies should have already been doing under HIPAA, she says.

"That's a process that needs to be institutionalized. It's something an organization should be doing on a regular, continual basis," she adds.

According to Coburn of Coburn IT Law, other steps organizations should take to comply with HITECH's security and privacy requirements include: documenting security policies and procedures; workforce training on the procedures; implementing physical safeguards; and restricting disclosures of protected health information to the minimum necessary information.

Faced with either budget or human resource constraints, health care organizations need to realize they can't meet every one of HITECH's security requirements all at once, Symantec's Finn says: "You're going to have to prioritize based on level of risk."

Overall, HITECH escalates the importance of security and privacy in the health care industry, he says. "It's no longer just the CIO's problem."

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

ADVERTISING INDEX

TECHTARGET SECURITY MEDIA GROUP