Plus: CONFUSED OVER CLOUD COMPUTING RISKS? YOU'RE NOT ALONE

INFORMATION SECURITY®

JUNE 2009

SIMs: More than just a pile of logs

ALSO:

A method(ology) to the madness

Convergence an uneasy union

INFOSECURITYMAG.COM

contents

JUNE 2009

VOLUME 11 NUMBER 6

FEATURES

ALSO

VeriSign Secured®

The latest and greatest in online security. Also the greenest.

Get visible site security from the company your customers trust.

It's simple: a green bar means your site is secure. For your customers, this means they can trust their Web experience. It's all done through VeriSign® Extended Validation (EV) SSL Certificates, which verify and visually represent the authenticity and security of Web sites. This protects you and online customers. Combine visitor confidence with the strongest encryption available to each site visitor to maximize your site's overall security profile.

Get your free white paper, *The Latest Advancements in SSL Technology,* at www.verisign.com/is or call 1-866-893-6565 or 1-650-426-5115.

VeriSign®

A Little Ingenuity

BY KELLEY DAMORE

The economy is forcing organizations to be more resourceful and bury the hatchet. And that's a good thing.

BELIEVE IT OR NOT, there is a silver lining to the recession. It forces organizations to think creatively about problems, use tools for tasks beyond their intended purpose, and foster relationships they may not have had in the past. There are two such examples in this month's issue.

The first centers on the integration of physical and logical security. While the benefits have been talked about for years, culture clashes and ownership issues have limited its widespread adoption (see "A Sustainable Relationship" by Michael Mimoso).

But in a world of cost cutting and increased scrutiny on ROI, some organizations are bringing the two groups together successfully. It is worthy to note that physical and logical security people have the same concerns: protecting assets, ferreting out malicious insiders and managing risk. What's more, their worlds are colliding as much of the physical security infrastructure has become IP-based.

Desperation is a powerful tool. It can actually force people to look beyond preconceived notions and topple established silos. Face it, IT and IS managers are overwhelmed by the multitude of technology and operational tasks that they are accountable for. In an environment of reduced budgets and headcount, the task becomes even more untenable.

James Connor, principal of N2N Secure, a consulting company that works with organizations to meld physical and logical security, sees barriers breaking down and people being more receptive to working together these days.

> "Before the downturn we saw a lot of fighting," around ownership issues over processes and responsibilities. "When faced with cost cutting, people are more receptive."
>
> —JAMES CONNOR, principal, N2N Secure

"Before the downturn we saw a lot of fighting," around ownership issues over processes and responsibilities, Connor says. "When faced with cost cutting, people are more receptive."

Connor believes that policy is the most powerful tool. "You need to get the policy right and the stakeholders right. Then the technology comes in," he says. Streamlining processes becomes a powerful argument that can be conveyed to upper management.

Melding processes is what made Greg Jodry successful in his position as director of business and asset protection at Yahoo! As Jodry explained at the RSA conference in April, he just wanted his team to be invited to the table when it came to IT security.

Since much of Yahoo!'s assets reside in servers in data centers, he offered up his security team to do audits of the vaults where the customer information is housed. This offer played on his team's strengths and has allowed him to foster a strong working relationship with the

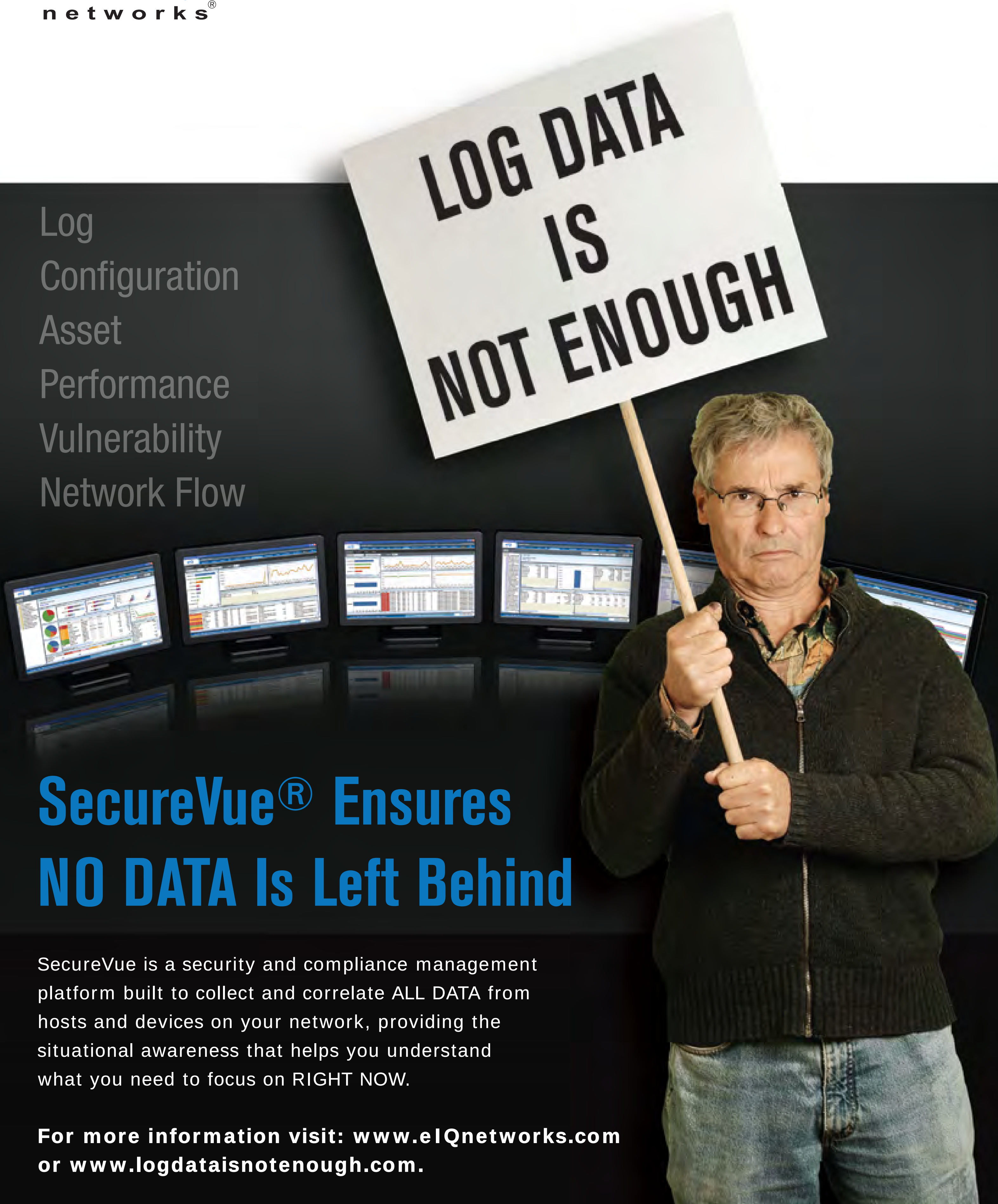
IT security folks. His mission was accomplished: he now has a seat at the table.

These two examples illustrate how partnerships can work. I would encourage you to think about potential allies or former "frienemies" and see how you can work together, combine budgets on certain projects and utilize their talents to help you achieve your goals. It may open doors you never considered before.

A second example of ingenuity comes from our story "A Method[ology] to the Madness" by Cris V. Ewell. This story explains a homegrown risk methodology that had its roots in a Ph.D risk management course at Nova Southeastern University and is now fully implemented at a private corporation and the University of Washington. We are grateful that they wanted to share their framework with others in the information security field.

If you have any success stories or tools that have helped you weather the storm, please send them to us. We're all in this together. ▸

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


LOG DATA
IS
NOT ENOUGH

VIEWPOINT

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

Tabletop post-mortem checklist a must

Good stuff and an interesting read about the value of tabletop exercises ["This is Only a Drill" April 2009] for enterprises and government agencies.

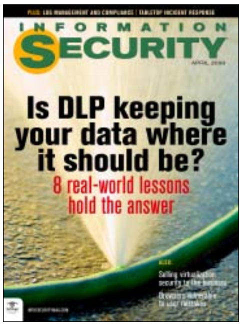
One area where I really see organizations falling short on many tabletop exercises I've observed and participated in is the post-mortem.

This is really where you can learn about the exercise, especially what worked and what didn't work.

You can also identify areas needing improvement that would help in future planning. Unfortunately, there is really no decent checklist on questions to ask and issues to raise during the post-mortem.

Anyway, when an exercise is planned, its planners need to ensure that they have built a robust post-mortem checklist to be sure that they really get the total value out of the exercise.

—Ernie Hayden


INFORMATION SECURITY
Is DLP keeping your data where it should be?
8 real-world lessons hold the answer

Hardcopy 1, Digital 1

I, too, am one who strongly prefers hardcopy over digital when it comes to magazine medium, for the same reasons sited by others in your Viewpoint section.

If the presentation is digital only, I won't read it.

When hardcopy, I'll read the entire magazine over a short period of time—at work, at home, traveling.

Keep the hardcopy!

—Gary Lee, Bank of Oklahoma

I love the new digital format of the magazine. It is much easier to search and archive than it was in print form. Those who insist they will read only magazines that continue to be offered in print form are in denial about the current and future state of the newspaper and magazine business. Offering the magazine in PDF form offers the best of all worlds to your readers.

—David L. Leach, director of information security, Micron Technology

COMING IN JULY/AUGUST

MUST READ!

Must-Have UTM

Unified threat management (UTM) has come a long way since it was known as a turnkey appliance, which was basically a firewall replacement with some added optional capabilities for small businesses. Today, UTM is close to a must-have for mid-market companies, and at the high end, powerful data center and carrier-grade UTMs have emerged. We'll look at what constitutes today's essential features, appropriate use cases, and what to look for based on your needs.

Privileged Access Controls and Strategies

In the wrong hands, privileged accounts represent the biggest threat to enterprises because these accounts can breach personal data, complete unauthorized transactions, cause denial-of-service attacks, and hide activity by deleting audit data. Compliance mandates such as PCI DSS require control of privileged accounts. We will explain the technologies—such as privileged account management tools—and strategies that are available to help organizations get better control over their privileged accounts.

Time for DNSSEC

A year ago, researcher Dan Kaminsky uncovered a critical bug in DNS. Not only was the vulnerability serious enough to draw the major DNS and security companies to the same table for a coordinated patch, but it kick-started discussions on the viability and need for DNSSEC. We'll examine how far discussions have progressed and whether companies should embrace it.

Tread Carefully Into the Cloud

Cloud computing carries risks that enterprises need to weigh before they forge ahead. BY PATRICK CUNNINGHAM

THE "CLOUD" IS OFTEN used as a generic term for any type of Web-based application. It is most commonly used today to refer to the grid or utility computing model, where it replaces local hardware and storage input/output. Organizations are moving to the cloud, some faster than others. However, moving to the cloud presents the enterprise with a number of risks to assess. At the core of these risks is the inability of many cloud/Web 2.0 vendors to meet regulatory and legal requirements. Here are the top three risks:

1. Security: For many organizations, security of information is the most critical risk. This may be driven by a need to protect intellectual property, trade secrets, personally identifiable information, or other sensitive information. Making that sensitive information available on the Internet requires a significant investment in security controls and monitoring of access to the content and the pathways to the information. The logging and auditing controls provided by some vendors are not yet as robust as the logging provided within enterprises and enterprise applications. The challenge here is to ensure that, post incident, the organization has visibility to anyone who had access to the document and what might have been done to the document (edit, download, change access, etc.).

The logging and auditing controls provided by some vendors are not yet as robust as the logging provided within enterprises and enterprise applications.

2. E-discovery: The current climate for e-discovery assumes for the most part that an enterprise knows specifically where its information is being stored, how it's being backed up, and how it's secured. The rules also assume that an enterprise will be able to physically examine storage devices and, when required, examine storage media for evidence of erased and/or deleted files. In the cloud environment, the enterprise may have little or no visibility to storage and backup processes and little or no physical access to storage devices. And, because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of file access and deletion will be a significant challenge.

3. Computer forensics: For many organizations, computer forensics is a critical component of e-discovery efforts and internal investigations, and often requires physical access to the storage device or computing resource. Much can be learned

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

from information stored by a computer's operating system in physical and volatile storage: information that is retained in a computer's random access memory that disappears almost immediately after a computer is turned off. When data and applications are moved off the local personal computer, the forensics investigator may lose the ability to access very critical information for the case. The provenance of a particular file or the time the file was last accessed can often be crucial in determining how the file was used and who had access to it. If the data storage shifts to the cloud, the ability to obtain uncontaminated copies of evidentiary data may be reduced, if not eliminated.

Prepare in Advance

While these concerns may not be absolute barriers to moving data storage and applications to the cloud environment, clearly they are significant obstacles that will require an enterprise to carefully examine its contractual obligations, risk profile, security infrastructure and oversight ability. An enterprise should be prepared to present the vendor with detailed security and legal requirements applicable to their business needs and the nature of the information being stored or transacted.

A major challenge today is that case law involving information stored in the cloud is nearly non-existent. The enterprise must take measures to legally protect intellectual property and secure title over its information. Legal departments may be wary about moving intellectual property, trade secrets and legally privileged information to the cloud due to the lack of relevant case law in this space. In any event, the business must ensure that its security and legal requirements are made part of the contract and that it conducts periodic audits to ensure the vendor is meeting the requirements.

Patrick Cunningham, CRM, was previously a member of the board of directors for ARMA International, a records and information management professional association. Cunningham holds a master's degree in public history from Loyola University of Chicago and has been a Certified Records Manager since 1992. Send comments on this column to feedback@infosecuritymag.com.

Analysis | CLOUD COMPUTING

Cloud Confusion

Vendors are loosely using the term cloud computing, and it's causing confusion for users in the market for buying and securing these services. BY ROBERT WESTERVELT

WRITING IN HIS BLOG RECENTLY, Misha Govshteyn, co-founder and CTO of log management software-as-a-service vendor AlertLogic notes that some vendors at the RSA Conference 2009 were using the term cloud computing rather loosely.

Govshteyn points out that Netgear uses "cloud" to describe its line of unified threat management (UTM) appliances. Netgear says it has a "hybrid-in-the-cloud security architecture." Endpoint security vendor Prevx uses "cloud" to describe its endpoint agents using the "power of the cloud."

"Those are some of the more absurd examples," Govshteyn says. "Cloud is really about moving complex computing workloads off premise and delivering them as a service. At the end of the day, cloud at its core is cost effective and simple."

Even IBM is coining the term for what it isn't. Big Blue describes its new WebSphere SOA appliance as the WebSphere CloudBurst Appliance. It's deployed in-house, but that doesn't stop IBM from calling it an SOA appliance that deploys and manages SOA in a private cloud.

Like Govshteyn, other security experts and industry observers agree that the loose use of the term cloud has fueled some confusion about what it really comprises.

"I've heard from a lot of end users saying that they are sick of the word cloud because it's used in every conversation they have with vendors," says Chenxi Wang, a principal analyst at Forrester Research. "The industry is sick of getting another buzzword, but cloud computing and cloud services are here to stay."

Web-based service offerings are what primarily make up the cloud. In a recent Forrester report, Wang describes three markets associated with cloud computing: App-components-as-a-service, software-platform-as-a-service and virtual-infrastructure-as-a-service.

The app-components-as-a-service market includes Web-based email and other social networking applications where the application is owned by the provider. Google's Web-based word processing and spreadsheet applications fall into this market.

Salesforce.com and other vendors that sell their software via the Web would qualify for the software-platform-as-a-service market. Microsoft Azure Services Platform and Amazon's S3 data storage services also make up this market, according to Wang.

The third and final piece of the cloud-based services market includes the virtual-infrastructure-as-a-service market. The space is made up of traditional outsourcing services, such as when a company hosts a Web server at a remote data center where a service provider provides maintenance and upgrades.

Having a firm grasp of what really makes up the cloud is mixed among different organizations, Wang says. In fact, some companies may not realize that a small division is using cloud computing for a certain business process, she says.

"Many are just starting to get their feet wet and those companies tend to be less versed in the benefits and risks, and even the functionality," Wang says.

> "Many are just starting to get their feet wet and those companies tend to be less versed in the benefits and risks, and even the functionality."
>
> CHENXI WANG, principal analyst, Forrester Research

Even the National Institute of Standards in Technology (NIST) is weighing in on an official definition. In a working definition released in April, NIST called cloud computing an "evolving paradigm." The organization narrows the term down to five key characteristics, three delivery models and four deployment models.

"Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction," NIST says.

Jim Reavis, a security consultant and director of the Cloud Security Alliance, a non-profit organization seeking ways to better secure cloud-based services, says the term "cloud" should be simplified for the average customer to understand.

"Cloud computing is in my view an on-demand usage of information technology delivered to the customer as a subscription-based service," Reavis says. "The customer is not aware of a lot of the interworkings of these shared resources."

And according to AlertLogic's Govshteyn, if customers aren't aware of the interworkings of the shared resources, they probably shouldn't worry about the definition of the cloud.

"Understanding the definition of cloud isn't really going to have any bearing on how you make your buying decision," Govshteyn says.▸

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

National Cybersecurity

CYBERSECURITY AND NATIONAL SECURITY are finding their way into the same sentences an awful lot lately. Now that the Obama administration's 60-day review of federal cybersecurity processes is complete and details slowly trickle out, it will be interesting to see which squeaky wheel gets the grease. —*Information Security* staff

2 ATTACKS

Electric Grid Takedown(?) The government reveals that Russian and Chinese hackers have penetrated the country's electric grid and possibly have left behind backdoors that would enable the attackers arbitrary access to critical infrastructure.

Fighter Jet Plans Stolen *The Wall Street Journal* quotes anonymous former government officials who said the Pentagon's $300B Joint Strike Fighter project was hacked, and terabytes of data on the fighter jet were stolen.

0 SOLUTIONS

Hathaway Swings and Misses Attendees had high hopes for Melissa Hathaway's RSA keynote, but the acting senior director for cyberspace for the National Security and Homeland Security Councils whiffed badly during her awkward 30-minute speech, which harkened back to past calls for public-private sector cooperation and White House leadership for cybersecurity. Anyone seen that copy of the National Strategy to Secure Cyberspace?

BUT WAIT...

S.773 The Cybersecurity Act of 2009 would give the president unprecedented power to disconnect critical infrastructure networks from the Internet in time of national emergency. The bill—also known as Senate Bill 773, or the Killswitch Bill—fails to define a critical network, nor does it limit the president's power to just federal networks. Another section of the bill establishes the Commerce Dept., as the clearinghouse for threat and vulnerability information and gives them unfettered access to relevant data on critical networks. And don't skip the provision that could lead to a national ID program. Anyone have the EFF on speed dial?

OVER-HEARD

> **"The White House must lead the way forward with leadership that draws upon the strength, advice and ideas of the entire nation."**
>
> –MELISSA HATHAWAY, acting senior director for cyberspace for the National Security and Homeland Security Councils

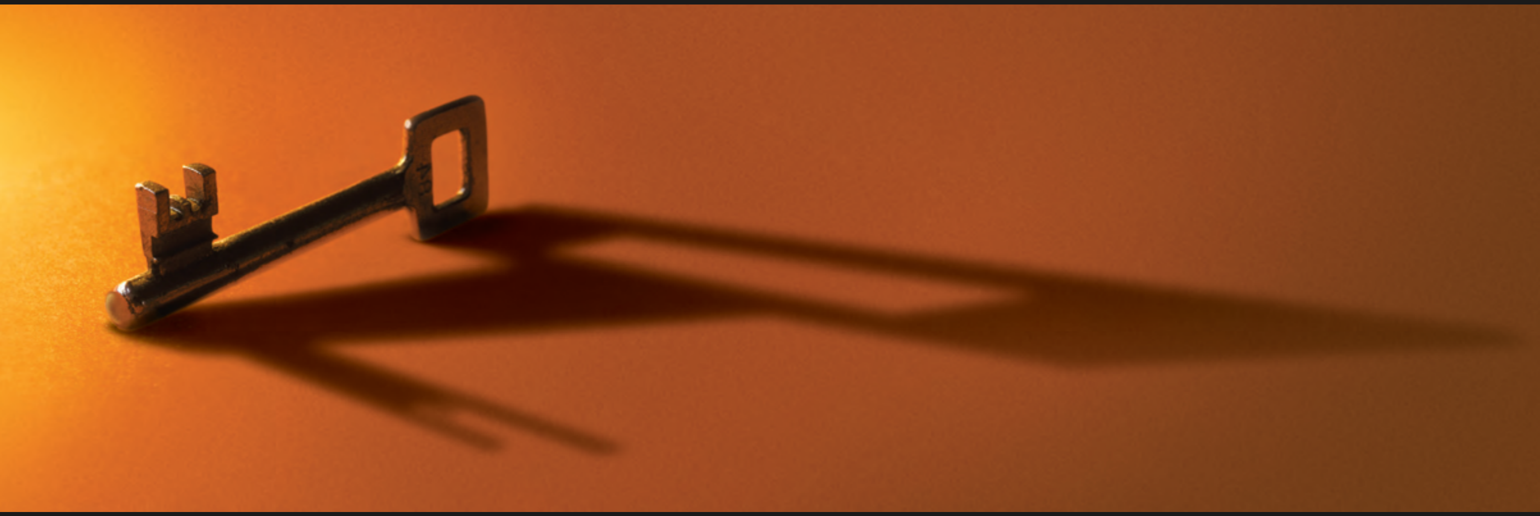


TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

SIMs: More than just a pile of logs

They've come a long way from the early days of log aggregation and correlation; enterprises now glean value from SIMs for compliance, visualization and even overall business intelligence. By DIANA KELLEY

IT'S BEEN ALMOST A DECADE since security information management (SIM) systems were introduced. During that time, SIM products have evolved from relatively immature log aggregation products that were too expensive for all but the largest enterprises, to mature aggregation and management solutions that provide network and security insight to organizations of all sizes. But SIM solutions aren't done evolving.

As SIM use increases, enterprises are asking vendors for additional functionality, including deeper compliance intelligence and reporting, better visualization, improved incident response and integration of identity awareness. Many companies are leveraging SIMs to increase efficiency and cost savings in their security programs. And some businesses are going beyond security awareness and exploring how the comprehensive view of network and user activity that is collected and parsed by the SIM can be used for proactive risk management and business intelligence.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

A CONFUSING BEGINNING

Early on, the SIM space suffered from a number of identity crises. To start with, there wasn't even consensus about what to call the products, and vendors used a variety of acronyms. Part of the problem stemmed from the fact that vendors and their customers approach functionality in different ways. For some, the great promise of SIM was bi-directional management of heterogeneous security devices (also known as MoM—the manager of managers). Others saw the consoles as a hyper-intelligent processor of complex correlation rules and predictive attack analysis. And some enterprises found simple, but effective, centralized log aggregation to be the core business justification for installation.

In early deployments, SIMs were installed in large enterprises and used primarily as log aggregation tools. Although some enterprises spent a significant amount of time and resources crafting custom correlation rules, most gained the greatest value from the ability to collect critical log information from multiple sites and sources in a single, searchable repository using pre-set rules and templates for alerts management. But the landscape changed and the products matured. SIMs became more user friendly and compliance aware. New offerings emerged that were scaled for small and midmarket companies [http://searchmidmarketsecurity.techtarget.com/tip/0,289483,sid198_gci1354209,00.html]. And most SIM users realized that, although deeply complex correlation rules were not always cost-effective, there were many efficiencies to be gleaned from the powerful log aggregation and reporting that enterprise-ready SIM solutions offered.

MEETING COMPLIANCE DEMANDS

Compliance requirements for protection of personal information and industry standards such as PCI DSS drove many initial SIM purchases and still do today. Trent Henry, principal analyst for research firm Burton Group, says, "Companies that were only monitoring the perimeter devices are moving toward complete log and event aggregation" to meet audit and regulatory requirements. SIM solutions are, at heart, log aggregation engines because the information and events need to be collected and parsed at a central point before prioritized event reporting or correlation rules can be applied.

Most companies using SIM report that centralized log aggregation is the baseline function; without it, the product would not even be installed [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257083,00.html]. But centralized logs and reporting comprise only a portion of the overall compliance landscape. For example, while requirement 10 of PCI explicitly mandates log aggregation, other portions of PCI could be supported with SIM such as the ability to report on who accessed data stores of credit card numbers.

Compliance requirements for protection of personal information and industry standards such as PCI DSS drove many initial SIM purchases and still do today.

Similarly, properly tuned SIMs can provide reporting and alerting that ease compliance with privacy related regulations such as HIPAA and the new Nevada and upcoming Massachusetts protection standards for personal information.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

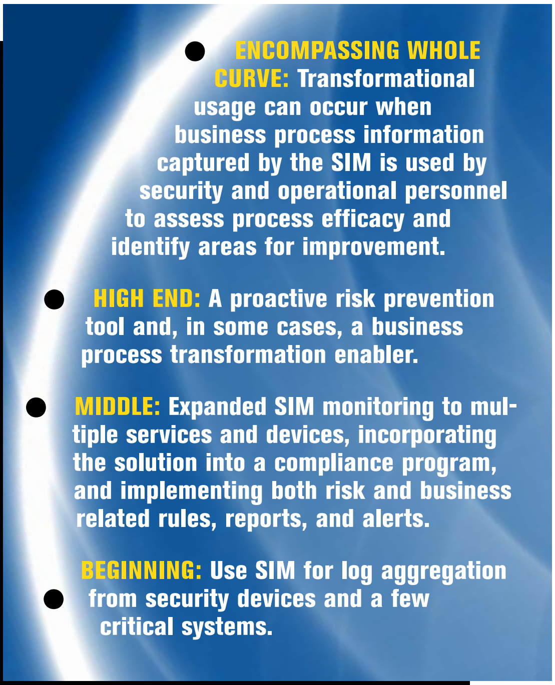
SPONSOR RESOURCES

Section 17.04 of the Massachusetts law requires secure authentication, secure access control to records, and periodic reviews of audit trails. While log aggregation helps with the audit trail reviews by centralizing the information, a SIM tuned to monitor for access control or one that is integrated with a database monitoring tool from vendors such as Application Security, Guardium or IPLocks, will provide deeper coverage for compliance monitoring and reporting.

SIM tools come with a variety of templates for compliance reporting and basic correlation rules for alerting on access violations. Organizations can use the default

Where are you on the curve?

SIM has evolved from a security only solution sitting on the periphery of network operations to an integrated part of the business. Here's a look at the different stages of implementation for organizations. ►



● **ENCOMPASSING WHOLE CURVE:** Transformational usage can occur when business process information captured by the SIM is used by security and operational personnel to assess process efficacy and identify areas for improvement.

● **HIGH END:** A proactive risk prevention tool and, in some cases, a business process transformation enabler.

● **MIDDLE:** Expanded SIM monitoring to multiple services and devices, incorporating the solution into a compliance program, and implementing both risk and business related rules, reports, and alerts.

● **BEGINNING:** Use SIM for log aggregation from security devices and a few critical systems.

One of the most interesting aspects of how SIM has evolved is the move from a security only solution sitting on the periphery of network operations to an integrated part of the business. While this trend is a natural evolution, it is not yet the norm. Companies that are at the beginning of the curve are using SIM only for log aggregation from security devices and a few critical systems. In the middle of the curve are companies that have expanded SIM monitoring to multiple services and devices, incorporating the solution into their compliance program, and implementing both risk and business related rules, reports and alerts. At the other end of the curve are the organizations that see SIM as a proactive risk prevention tool and, in some cases, a business process transformation enabler. Transformational usage can occur when business process information captured by the SIM is used by security and operational personnel to assess process efficacy and identify areas for improvement. ▸

—DIANA KELLEY

templates and reports or customize them as needed. Alberto Cardona, CISO for a large New York newspaper that uses a SIM from eIQnetworks, says the newspaper was able to use the templates included with the SIM, for the most part, "out of the box." Although some customization was required, it wasn't labor intensive and was mostly due to legacy applications with older login mechanisms, he adds.

Now that companies have learned to "walk" through compliance with SIM log aggregation, many of them are breaking into a run and integrating the solutions into a broader compliance program.

CLOSING THE RESPONSE WINDOW

Enterprises also are using SIMs to get a better view of their security posture and to improve their incident response. What separates a security event from a user error can be difficult to assess in a limited-view analysis, but becomes clear when understanding the context of the larger system as a whole. A SIM consolidates information from multiple sources including applications, servers, security and perimeter devices, making it possible to determine root causes.

Enterprises also are using SIMs to get a better view of their security posture and to improve their incident response.

At the newspaper, the layered data inputs are used to hone responses. As Cardeno explains, in a narrow view, an event such as a spike in CPU usage on a server, the root cause might not be apparent. An administrator could attribute the usage increase to a bad patch while an application developer might fear it was a memory leak in the code written for the application running on the server. And a security administrator might assume the spike was caused by a malicious denial-of-service (DoS) attack. With the consolidated view provided by the SIM, an administrator could see that the application log and event data is normal, no recent patches have been applied, and the IDS or IPS is reporting a huge increase in attempted connections to the server, making it likely that the company is experiencing a DoS.

John Menezes, president and CEO of Cyberklix, a managed security service provider (MSSP) that uses RSA's enVision SIM, calls this consolidation "the holistic view of security." [http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1327864,00.html] Burton Group's Henry agrees, observing that many Burton customers are tweaking their SIMs to get better value out of their IDSes and other security devices. At Ontario, Canada-based Cyberklix, vulnerability management tool information is cross-checked with IDS or IPS events at the SIM console. For example, while an IDS or IPS may report that an exploit is being launched against a target, the vulnerability manager reports "show the target device was patched, so the IDS scan information is a false positive," Menezes says

Of course there's always a possible downside to too much information. And enterprises that suffered through multiyear roll-outs of SIMs slowed by extremely complex correlation rules may read the above with a world-weary sigh. To be effective with a holistic approach, be selective with what is monitored. Start slowly, focus on the highest priority systems, and a limited number rules. Grow the rule-set only when the processes are well understood and the existing rules are functioning smoothly.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

In addition to helping sort out the root case of an event, organizations are using SIMs to proactively stop attacks or fix improper changes to systems. At TruMark Financial Credit Union in Pennsylvania, Matt Roedell, vice president of information security and infrastructure, has configured a TriGeo Network Security SIM to monitor and alert on configuration changes such as add a user, add a firewall, and AD [Active Directory] reassignment. The SIM automatically emails the change control committee inbox when a change is made. If any process or service works improperly after the change occurs, the team "can immediately call who made the change and ask them what they did and have them back it out," he says.

SIM Vendors

A sample of SIM vendors.

ArcSight (www.arcsight.com)
CA (www.ca.com)
Cisco Systems (www.cisco.com)
eIQnetworks (www.eiqnetworks.com)
IBM (www.ibm.com)
Intellitactics (www.intellitactics.com)
LogLogic (www.loglogic.com)
netForensics (www.netforensics.com)
NetIQ, an Attachmate business (www.netiq.com)
NitroSecurity (www.nitrosecurity.com)
Novell (www.novell.com)
OpenService (www.openservice.com)
Q1 Labs (www.q1labs.com)
Quest Software (www.quest.com)
RSA, a division of EMC (www.rsa.com)
SenSage (www.sensage.com)
Symantec (www.symantec.com)
Tenable Network Security (www.tenablesecurity.com)
TriGeo Network Security (www.trigeo.com)

WHAT'S IDENTITY GOT TO DO WITH IT?

Managing events and logs from security devices is common practice in the SIM world. But what about identity related information? [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1351973,00.html] Login information is closely tied to security and risk and SIMs have correlation engines that could use this information to improve the company's security posture. Henry calls identity information the "classic example" of SIM intelligence gathered from devices that are not deployed for security only purposes such as firewalls, vulnerability management, and IDS. Vendors with robust identity management offerings, such as CA, IBM, and Novell, have focused on this issue, offering close integration between their identity management solutions and SIM products.

With this integration, a SIM could report a successful login, alerting a company that thought the user was de-provisioned, according to Henry. The login itself is significant but this could also trigger a call to the identity management team to ascertain whether the de-provisioning system is mal-

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

functioning or perhaps not configured to properly deactivate all of a user's accounts. In this way, a SIM could help close the audit loop for identity management systems that don't have mechanisms for monitoring themselves or function as a separate channel for audit monitoring and control.

Companies are reporting that some or all logins to sensitive servers and applications are being monitored by a SIM. This information is used for data protection purposes, ensuring that only legitimate, approved users are accessing protected information, and for compliance reporting of the access. For one business, a SIM helped flag a problem with a new password policy. An auditor had recommended a very strict policy with more than eight characters, no dictionary words, and a password time-to-live (TTL) of two weeks. Because the company had a single sign-on (SSO) solution in place, users only needed to remember one password, but with the new rules, even that one password was too much. Lock-outs shot up and the help desk was overwhelmed with reset calls. While help desk records would have eventually shown the new policy was causing problems with users, the SIM alerts indicated a problem within a couple of days.

Companies are reporting that some or all logins to sensitive servers and applications are being monitored by a SIM.

At the newspaper, Cardona saw a corollary usage. By using the SIM to monitor key systems, each with a different password, and correlating them with logs, alerts, lock outs and help desk calls, the security team was able to use this information as business justification for investing in an SSO solution.

Perhaps one of the more complex identity options for integrating a SIM with identity management is to create comprehensive user activity profiles that follow a user's activities through the network. This information can be used to track anomalies and possible misuse. An example of this is limiting access to a database using location information. The database administrators may have access to the database from inside the data center or using an approved remote access solution, such as an IPSec VPN, from an approved remote device. If access is granted to a legitimate user from an unapproved network or device, the SIM could issue an alert or possibly trigger an automatic shutdown of the session through communication with network management systems. Though these usage scenarios require more integration and customization work, the pay-offs could be significant depending on your business.

CONTINUOUS IMPROVEMENT

Better integration with operational consoles is one feature of the SIM evolution *[see chart, p. 15]*. The days of a separate SOC and NOC may be numbered for many companies that simply can't afford the costs. But the importance of the security information doesn't disappear. And, for some entities, not having some sort of separate audit channel and monitoring solution in place is not an option. To make this work in the enterprise, operation teams are consuming the information from the SIM console into the large meta-consoles such as HP OpenView, IBM's Tivoli, and CA's NSM (formerly Unicenter). The security team still maintains administrative control of the SIM, but the operations team can use the information as well. For example, if a slowdown is detected in an area of the network, the operations team may discover that the root cause is a security event such as a DoS attack or a bandwidth-intensive worm.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

Menezes says the architecture of the SIM solution can be a contributing factor to whether or not the SIM can be more widely deployed throughout the infrastructure. In his experience, agent-based solutions created "all sorts of political issues with whether the tool could be installed." Also, he found that the administrator uninstalled the agent if anything unexpected happened on the device. Agent-based solutions, on the other hand, may be preferred by companies that want a separate monitor agent on a server.

To make a SIM more valuable to the business, Cardona advises answering some questions up front: What is your core requirement? What is the main objective that you want to accomplish? What reports will you generate and give to the CIO and other stakeholders? And how can you make this information valuable to them? Armed with the knowledge of what information will be of value to the stakeholders, security administrators can customize the standard reports that come with a SIM for their own business needs.

Out of the box, a SIM delivers meaningful solutions that satisfy auditors, Roedell at TruMark says. But to get business value from a SIM, he adds, "You have to spend time to tailor it to your business and your network. Risk mitigation strategies are only effective when they're implemented and managed by IT professionals who understand your business." In SIM parlance, that can mean identifying when a password policy has gone bad, finding the root cause of a CPU usage spike, or even justifying additional hardware resources because a critical server is overloaded.

Long-term, SIM alerts can be quantified into metrics-based assessments. Again, this is a fairly advanced use of the tools, but it is one that some end-users are exploring and a few are already adopting. At TruMark, using a SIM means "residual risk scores will be reduced," Roedell says. To make that matter to the business, security experts will "have to do a better job showing what they're going to do and how these tools are going to reduce risk in a dollars and cents way," he says. For another organization, repetitive alert suppression rules reduced redundancy so what was effectively a full-time job for three people was reduced to a part-time job for one.

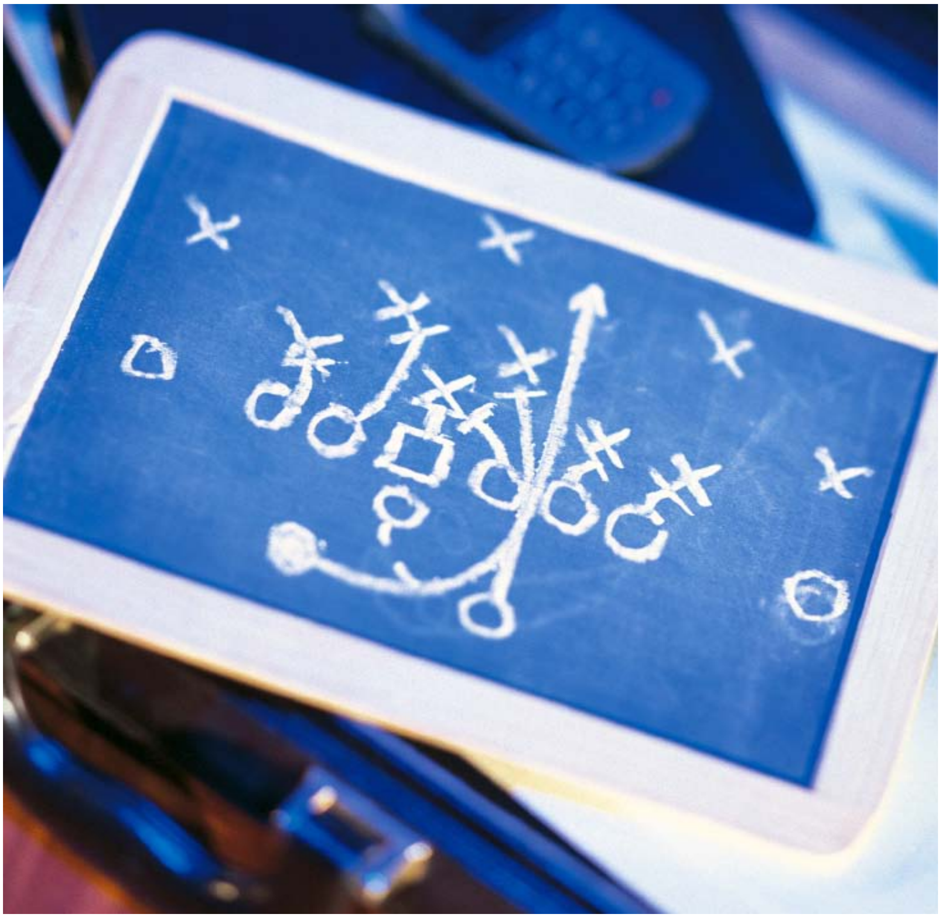
EXPANDED OPPORTUNITIES

For many, SIM is the Holy Grail for log aggregation compliance, but a number are looking beyond compliance to business improvement. SIM can be "used as a foundation for making the organization more compliant while being leveraged in the long run for continuous improvement," Menezes says. Compliance is a starting point for SIM use but by reviewing the information captured by the SIM, companies can begin to make process improvements such as understanding which devices or areas of the network are more prone to malware attacks and then shoring up controls or fine-tuning a password policy to reduce help-desk calls, he says. Cardona echoes this view: "Start with compliance but tune the SIM in the long run to make it a tool for business enablement."

It's been an interesting decade for SIM. SIM has evolved from the confusion of the early days, through the toehold of log aggregation for compliance, to its current emerging usage as a risk and business tool. If you're using SIM for basic log aggregation and you're happy with it, that's great. If you think it can do more, you're right. Some of your peers are expanding usage for increased business intelligence and better risk awareness. ▸

Diana Kelley is founder and partner at consulting firm SecurityCurve [http://www.securitycurve.com/]. She has worked in computer and network security for 19 years. Send comments on this article to feedback@infosecuritymag.com.

CGEIT®
Certified in the Governance of Enterprise IT®
CISA®
Certified Information Systems Auditor™
CISM®
Certified Information Security Manager®



A METHOD[OLOGY] TO THE MADNESS

One security professional describes a homegrown risk methodology currently being used by a large university and a private corporation. BY CRIS V. EWELL

PROTECTING INFORMATION ASSETS is the information security program's primary directive. But the industry's inadequate strategies are partly to blame for its failures to do so; the industry seems satisfied with its current game plan. We allow vendors and compliance to direct how we should protect assets without regard to analyzing what risks would be minimized by implementing the proposed technology. If we truly believe in protecting the confidentiality, integrity, and availability (CIA) of our information assets then we must think outside the box and take the time to analyze risk, and design security systems that can reduce residual risk.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

Security breaches (more than 261 million records lost since ChoicePoint; more than 30 million in 2008) are happening despite substantial investment in perimeter security defenses and compliance. The current standards and compliance efforts used to help protect our information assets are disproportionately technical and do not adequately address the current threats and security risks. It is clear that spending additional money on technology is not the answer to the problem; nor is spending money on compliance or program development, without addressing root causes.

The risk process must be rooted in the principles of security and integrated into a security program that blends business needs, due care, current attack vectors as well as addressing contractual and regulatory requirements. Compliance with standards and regulations help to show due care, but should not be the driving force in a security program. It is not possible to address all of the threats and vulnerabilities. Instead of prescriptive controls, reduction of residual risk should be the driving force for the direction of development, assessment, and improvement of information security practices within the organization.

Compliance with standards and regulations help to show due care, but should not be the driving force in a security program.

Organizations need to follow a risk methodology; we'll describe one here that was developed as part of a Ph.D. risk management course requirement at Nova Southeastern University. Risk research from James F. Broder, George L. Head and Stephen Horn, Elaine M. Hall, and Thomas Peltier was also reviewed as part of the risk methodology development.

Over the past two years, the risk methodology has been revised and implemented

TABLE 1

Framework Categories

STRATEGIC CATEGORY

(1) organization and authority

TACTICAL CATEGORY

(2) policy **(3)** audit and compliance **(4)** risk management and intelligence **(5)** privacy **(6)** incident management **(7)** education and awareness

OPERATIONAL CATEGORY

(8) operational management **(9)** technical security and access controls **(10)** monitoring, measurement, and reporting **(11)** physical and environmental security **(12)** asset identification and classification **(13)** account management and outsourcing

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

at a private corporation and the University of Washington (UW). The risk methodology is now fully integrated in UW's information security program. The risk methodology was recently presented to the UW President's Advisory Committee on Enterprise Risk Management (PACERM) as a successful example of integrating business values, strategy, and operations into UW's ERM program.

The methodology is based on a security framework we developed four years ago. The framework accounts for all aspects of information security, addresses required security standards and regulations, and integrates information security into the business strategy. The initial concept of the framework came after talking to several security professionals; reviewing current regulations such as PCI-DSS, HIPAA, Gramm-Leach Bliley, and standards from ISO and NIST; auditing information security programs and practices of more than a dozen public, private, and government organizations; and researching security frameworks as part of a master of science information security program.

The goal of the project was to develop a framework that could be integrated into an information security program that would help defend the organization's information security practices, show performance at or above the due-care principle, and meet the organization's strategic security needs.

The framework is divided into 13 security elements within the strategic, tactical, and operational categories [*see chart, p. 22*] . The framework is integral to the security program because of the need to view the entire organization holistically for risk components. The framework gives the organization the ability to modify or add controls and objectives to meet the acceptable risk tolerance level for the organization. It also provides the direction for the development, assessment and improvement of informa-

TABLE 2

Capability Scale

LEVEL 1	Best practices are not performed and informal process is disorganized
LEVEL 2	The organization has some policies and procedures, best practices are being performed, and the process is organized but not repeatable across the entire organization
LEVEL 3	Policies and procedures are well defined and are implemented across the entire organization
LEVEL 4	Security practices and processes are being managed and controlled through data collection and analysis
LEVEL 5	Security practices and processes are being improved and are integrated into strategic business decisions

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

tion security practices within the organization. The security program must concentrate security protection efforts across the entire spectrum of the organization and be nimble enough to adapt to new threats. Compliance with standards and regulations are important, but compliance alone does not mean that the residual risk is reduced in an organization.

INTEGRATED RISK METHODOLOGY

The risk methodology consists of a self-directed, qualitative assessment process that is repeated several times during each year. As an example, UW completes quarterly risk assessments and reports the outcome to the security steering committee

FIGURE 1

Framework Elements

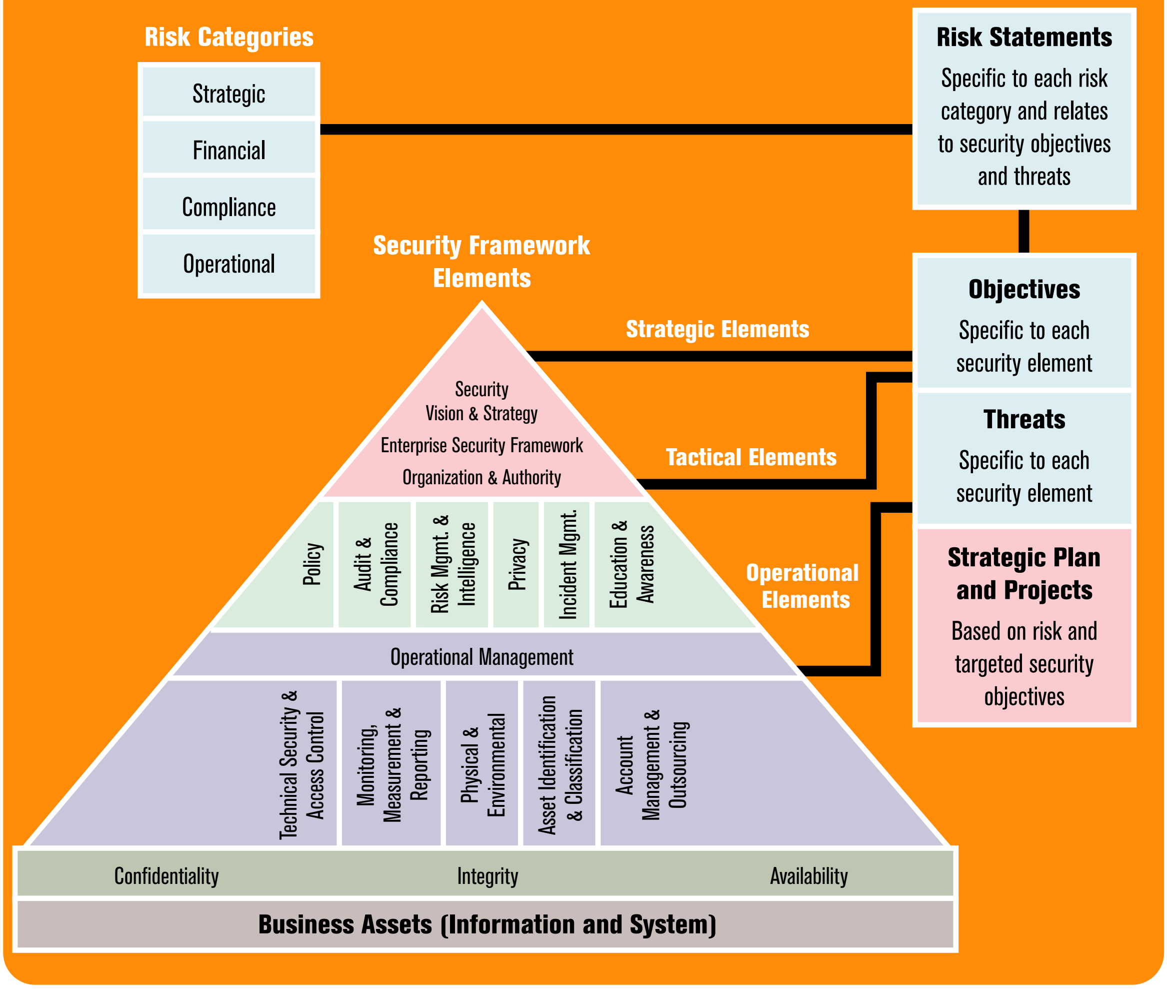

Risk Categories
Strategic
Financial
Compliance
Operational
Risk Statements
Specific to each risk category and relates to security objectives and threats
Security Framework Elements
Strategic Elements
Tactical Elements
Operational Elements
Security Vision & Strategy
Enterprise Security Framework
Organization & Authority
Policy
Audit & Compliance
Risk Mgmt. & Intelligence
Privacy
Incident Mgmt.
Education & Awareness
Operational Management
Technical Security & Access Control
Monitoring, Measurement & Reporting
Physical & Environmental
Asset Identification & Classification
Account Management & Outsourcing
Confidentiality
Integrity
Availability
Business Assets (Information and System)
Objectives
Specific to each security element
Threats
Specific to each security element
Strategic Plan and Projects
Based on risk and targeted security objectives

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

[http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1344606,00.html].

Without a practical and easy-to-use method, individuals will tend to postpone or not complete the assessment, take a reactive posture, or incorrectly apply the risk process. Risk assessments are a point-in-time evaluation that can quickly become outdated. To be effective in reducing risk, security professionals need to complete periodic assessments of their organization's security and risk posture.

Jan Emblemsvag and Lars Endre Kjolstad, in "Qualitative Risk Analysis: Some Problems and Remedies," showed how qualitative security risk assessments depend on a consistent analysis of the organizational capabilities and information quality conducted by knowledgeable and credentialed security professionals. Without a consistent approach, analysis of the capabilities of the organization, and critical analysis of the quality of assessment information, the results of the qualitative assessment should be questioned. According to Ruth Hauser, Eric Breidenbach, and Katharina Stark, who wrote "Advances in Statistical Methods for the Health Sciences," even with the limitations of qualitative assessments, they can provide the business with adequate information for risk decisions not obtainable by other methods.

> Without a practical and easy to use method, individuals will tend to postpone or not complete the assessment, take a reactive posture, or incorrectly apply the risk process.

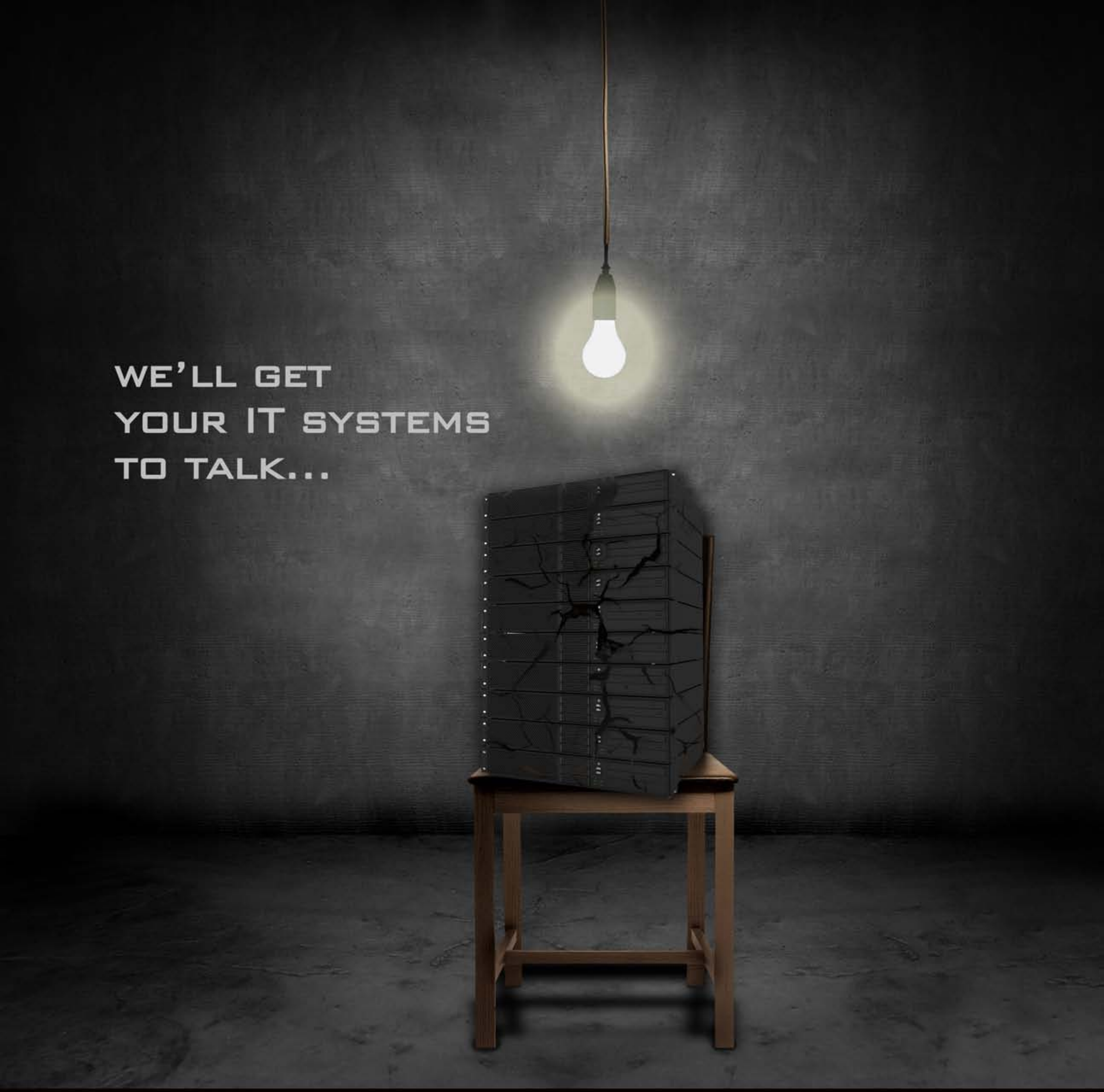
The assessment methodology is based on the premise that the amount of risk to the organization is dependent on the capability of the organization to protect its assets against enterprise threats. This is shown by the following formula:

$$\textit{Risk score} = \frac{\textit{Threat score}}{\textit{Compatibility score}}$$

As the capability of the organization to protect the assets increases or the threats to the organization decreases, the overall risk score should decrease. Calculating the risk score requires an organization to evaluate its capability and threats based on a comprehensive framework of security elements. Key objectives and threats need to be defined in each security element to enable the evaluation of capability and the likelihood and impact of threats.

The risk methodology accommodates the integration of the information security program into the organization's enterprise risk management (ERM) program. This is accomplished by identifying the relationship between the risk statements and objectives and threats within each security element. The risk statements are categorized within four areas and include:

- Compliance (failing to follow laws, regulations, contractual agreements, standards, or organization policy);
- Financial (loss of physical assets or financial resources);


We'll get
your IT systems
to talk...

- Operational (affect ongoing management processes), and;
- Strategic (affect ability to achieve goals or objectives).

The relationship between the objectives, threats, and risk statements allows the organization to assess and check the risk from both the security element perspective and the ERM perspective. This ensures a top-down or bottom-up consistency check that is needed for qualitative risk assessments. Figure 1 *(p. 24)* shows the relationship between ERM and the framework.

HOW TO IDENTIFY RISK

Identification of security risks, objectives and threats is critical to the success of the security risk process and is the first phase that should be completed by the organization. The risk identification phase should not be taken lightly and will require a concerted effort led by a knowledgeable and credentialed security professional team. The team must be familiar with the business environment, security standards, business needs, regulatory requirements and current threat spectrum. During this phase, the team will determine and validate the key objectives and the current threats for the environment. It is important to discuss each objective and threat to ensure they are representative of each security element as well as not being too granular.

The risk statements can be created as part of the organization's ERM process, or separate, if the organization does not have a coordinated risk process. The team must consider the root cause and not focus on the effects of the risk or mitigation steps. After the team completes the definition of the objectives, threats, and risk statements, each objective and threat will be correlated to one or more of the risk statements. The relationships between the risk statements, objectives, and threats allow the organization to analyze the impacts to risk due to changes in capability and threats. It is not uncommon to complete several iterations during this phase. After the team completes defining the objectives and threats for each security element, the threat relationship to the CIA triad should be completed. The objective of the risk identification phase is to have an overall balance of objectives and threats between all security elements and correctly identify the relationships with the risk statements.

HOW TO EVALUATE RISK

During the risk assessment phase, the team will use the key objectives and threats to make the scoring decisions. It is important to remember that the consistency of the methods used to determine the outcome and the security expertise of the team is more important than the scoring definitions. The team must document their decision process to ensure this consistency. The benefit of consistency is the ability to compare past and current assessments and analyze trends.

The first step in this phase is to define the level of capability the organization has reached in developing its comprehensive security program for each security element. A five-level capability scale was developed to aid in this process [*see chart, p. 23*].

The team will also evaluate the likelihood and impact of each threat within each security element. Along with data assets, threat agents should be considered during this part of the scoring. Threat agents are individuals who could use various threat

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

sources to exploit vulnerabilities. Intentions, capabilities, and opportunities for carrying out an attack make people dangerous threat agents. Potential threat agents may include employees, contractors, former contractors and subcontractors, maintenance staff, former employees, and unauthorized external users.

Likelihood and impact are scored on a three-point scale (low, medium or high). The likelihood score is influenced by the capability of the threat agent, the controls currently in place and the frequency and type of attacks. The impact is determined by the damage caused to the asset or organization by the vulnerability exploitation. The damage is measured in terms of disruption, loss of competitive advantage, capability, reputational loss, and replacement cost of the asset.

The final threat index score is calculated by adding the likelihood score, impact score, and one point for each CIA relationship to the threat. If the threat is only related to availability, one point will be added to the likelihood and impact scores. Three points will be added if the threat is related to the entire CIA triad. The maximum base threat index score is nine and the minimum base score is three. The threat score is calculated by the following for threats within each security element.

$${}^{1}\Sigma_{t=1}^{n}(CIA + ((Threat\ Likelihood + Threat\ Impact) * Risk\ Factor)_{t}$$

The capability score is calculated by the following for objectives within each security element.

$$\frac{1}{n}\Sigma_{c=1}^{n}(Objective\ Capability)_{c}$$

The risk factor for the threat score is initially set to 1.0 unless the organization feels that certain risks have a greater weight, in which case an additional risk factor of 0.1 to 0.5 can be added.

HOW TO ANALYZE AND MITIGATE RISK

This phase evaluates the information gathered throughout risk identification and evaluation. The analysis starts with looking at the overall security process capability scores and threat index scores for the current and previous periods. Over time, trends can be established that can aid in the analysis. The trends will help the organization determine what steps need to be accomplished to increase the overall security posture, decrease the impact and likelihood of the threats, and decrease the risk to the organization. Specific attention should be given to security elements where the threat index scores are high and the capability is low. This gap creates additional business risk that should be mitigated.

The last step is to develop a risk mitigation plan and ensure that the plan is tied to the security strategic plan. As shown in Figure 1, the strategic plan and projects are based on the risk and targeted security objectives. Conflicts between risk mitigation projects and compliance efforts may be uncovered during the analysis. Management will need to reconcile these differences and decide on a course of action. When allocating resources, top priority should be given to items with unacceptably high-risk rankings. These areas will require immediate risk mitigation to protect an organization's interest and mission. The objective is to minimize the overall risks to the organization.

The risk mitigation plan should include capability risk level, recommended control to be implemented, prioritization of controls, resources needed for implementation,

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

start and projected end dates, and ongoing maintenance and operation requirements. Ideally, the risk assessment will be repeated quarterly to track progress with the risk mitigation plan. Figure 2 [http://media.techtarget.com/digitalguide/images/Misc/June_ISM_risk_report1.jpg] shows one of the risk statements with the trends for the objective capability and threats. The colors under the element column indicate the current risk level for the specific element.

The color (red, yellow, or green) under the goal column indicates the gap between the current capability and the capability goal for the current budget period. The red arrows correspond to a negative change (decreased capability or increased threat) and the white arrows correspond to a positive change. Discussion should take place with the security team to evaluate if the risk can be reduced with the current projects or if a change is required.

RISK COMMUNICATION AND MONITORING

Knowledgeable and credentialed security professionals need to discuss information security risks issues on a regular basis. With limited resources and budgets, it is important to determine risk and compensating controls that reduce risk. Figure 3 is a sample quarterly risk report [http://media.techtarget.com/digitalguide/images/Misc/June_ISM_riskreport2.jpg] that shows the changes in risk and communicates these changes to senior management. The capability level has three lines. The inner line (blue) shows the current capabilities, the middle line (red) shows the estimated growth in capability for the current budget year, and the outer line (black) shows the desired long term capability goal for each security element. The threat index score shows the current threats for each security element. These graphs are calculated after the team enters the capability and threat scores. Each risk statement (identified by O1, C1, F1, S1, etc.) and security element are plotted on the risk chart based on their individual risk score. The security element lines use the same key as the capability level. The changes in the capability level, threat index score, and risk score from the past period are shown in the middle box. This report gives management an overview of current risks, trends, and gaps in the security program and should be used for strategy and risk mitigation discussion.

BE COMPREHENSIVE ABOUT RISK MANAGEMENT

The security industry needs to begin thinking outside the box and selecting different security strategies directed at mitigating information security risks and directly identifying risk mitigation methods that will be successful against current adversaries. Enterprise information security cannot be solved by technology alone or the dependence on perimeter defenses that assumes the adversary can be kept out of the enterprise. The resolution to the problem will require a comprehensive security program that incorporates risk management as the driving force for the strategy. The status quo is no longer acceptable, and our industry must change their practices and adopt concepts such as assumption of breach, active response, capability and attack intelligence analysis, as well as targeted discussions about attack vectors and patterns used by our adversaries as part of their risk management strategy.

Cris V. Ewell is director of information security operations, Office of the CISO, University of Washington. Send comments on this article to feedback@infosecuritymag.com.

A Sustainable Relationship

If your organization is serious about managing risk and total asset protection, then physical-logical convergence is a necessary step.

BY MICHAEL S. MIMOSO

RICH GRASSIE IS IT'S VERSION OF A MATCHMAKER. Many times he's united people you'd think on the surface would have no shot at a sustainable relationship. But Grassie knows how to connect disparate entities, especially when he hitches those guys with guns guarding the gates, to the geeks guarding the GUIs.

Converging physical security with IT security inside the enterprise isn't easy, but it's a labor that Grassie, principal consultant with TECHMARK Security Integration of Massachusetts, says is worth the bother, especially for large companies branching out globally with new services. Convergence affords organizations the opportunity to align security with overall business goals, streamline business processes such as provisioning and investigations, and centralize security operations and policies under one office. There are significant barriers to these unions; political and cultural disputes are often the tallest to hurdle, and companies cannot ignore the integration required to get a central view of physical and logical systems.

"We look at it as a holistic approach to managing security across an enterprise. It becomes a formal cooperation between two functions in the organization that previously never worked together," Grassie says. "They operate on their own budgets. They are two kinds of people. Now by integrating a holistic approach to information, logical and physical security, into one function under the CSO, we actually protect the enterprise much better than if we had three different silos."

> "Now by integrating a holistic approach to information, logical and physical security, into one function under the CSO, we actually protect the enterprise much better than if we had three different silos."
>
> RICH GRASSIE , principal consultant, TECHMARK Security Integration of Massachusetts

OF CULTURE CLASHES AND CONVERGENCE

Enterprises have been talking tough for years about transforming their security functions into more of a risk management exercise, yet few on the IT side have thought enough to include their physical security brethren to help make it happen.

"If organizations take a step back from the myopic IT-centric approach and really look at the security of an organization, they'll realize physical and logical security are perhaps equally important," says Brian Contos, chief security strategist with database and application security company, Imperva. "Understanding risk is more inclusive than IT-centric security."

Convergence, ultimately, isn't a grassroots campaign; it has to start from the top-down. That means executive management has to have the forethought to establish a chief security officer or chief risk officer and have that person oversee both operations. The CSO must massage conflicting people, business and technology issues, to ultimately gain an overall vision of risk to the business beyond information security.

"You need a central figure to carry the flag," says Contos, coauthor of *Physical and Logical Convergence*. "It can't happen from the bottom up simply because there does need to be an investment in new technology to make it work. I've seen grassroots campaigns try to start, but they only have a sliver of an organization covered. When they have a champion, they're able to run out an organization-wide solution quickly."

A CSO can mandate a risk assessment that identifies critical assets, their location and what they contain. He can also evaluate whether these assets are protected by the proper IT and physical controls, and then high-value assets, such as critical data centers, can be prioritized as the first targets for convergence. The end result should be that risk is lessened around fraud, business continuity, compliance and reputational risk.

"If you don't look at it from just a logical or physical standpoint, but as total asset protection," says Ron Woerner, president of the Nebraska InfraGard chapter and a security professional at a financial services firm, "it helps you better manage risks versus having a segmented view."

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

While risk assessments and asset classification might naturally be within the purview of CISO, the CSO also has to be part mediator, part politician. Nothing stands up convergence initiatives more than a culture clash. Not only have these two groups been segmented, but they're often separated by experience, pay scale and interests.

"[Political] battles are huge—monumental," Grassie says. Grassie recalls a consulting job in on the West coast with a major corporation, sitting with physical and logical security management, and bringing up the notion of the two entities working together because more physical security tools and systems were IP-enabled and creating network bandwidth issues.

"You should have seen the look on their faces; they turned purple," Grassie says. "A lot of physical security guys, especially the older ones, don't want to venture into the IT space. They see those IT folks as competing for the same dollars and space."

Staff on the physical security side of the house usually have a law enforcement background, or are retired military supplementing their pay. The CSO not only has to bring these groups together, but weed out those who are just along for the ride from those who can recognize the benefits of a converged operation.

"Someone told me that going out for a couple of beers did more for the convergence practice than any number of meetings," Contos says. "Once they start talking and sharing best practices about how IT can help physical security and, where physical security guys share information with IT, the use cases and value propositions became very apparent."

VIDEO ANALYTICS

Cameras = Computers

Modern video surveillance cameras are IP-enabled devices that take up bandwidth and must be secured.

IP-enabled physical security tools such as video surveillance are easing physical and logical convergence pains, experts and practitioners say.

Analog cameras are slowly being phased out as network cameras are introduced with advanced functionality and logging capabilities, says Ron Woerner, president of the Nebraska InfraGard chapter and a security professional at a financial services firm.

Woerner said during a presentation at the RSA Conference 2009 that network cameras enable video to be stored locally or remotely, and include video motion detection, audio and digital inputs and outputs and serial ports for data or control-pan-tilt capabilities.

They communicate, Woerner said, either via built-in Web servers or FTP servers.

"Many of the technologies in place today on the physical side are really client-server," Woerner says. "Cameras are really getting to be computers; digital cameras have digital analytics. So the IT side realizes this traffic is flowing over network, they prepare for it and realize it can take up some bandwidth. It needs to be protected and segmented on the network." ›

–MICHAEL S. MIMOSO

CONVERGENCE USE CASES

The most typical use case right now involves some sort of badge reader integrated with an identity management or directory system such as Active Directory or LDAP. Users swipe an access card at the door and use that same access card to log on to network resources. Activities are monitored and correlated centrally.

But increasingly, video surveillance is entering the picture as analog cameras are replaced with network-aware cameras that allow users to view locations remotely, store video digitally and manage it remotely over an IP network. Some are able to do video motion detection and capture audio as well. Some also include built-in Web and FTP servers, email clients and allow users to program alarms.

Woerner notes that some cameras also feature video analytics capabilities that can do object or people tracking, facial recognition, and much more. He cautions that some companies do run into bandwidth issues transmitting video, but compression technology has improved, easing this challenge. This could lead to discussions about whether to store video—locally or in a central repository—and whether more storage must be allocated or purchased.

Contos says some industries such as the government and pharmaceuticals and other health care facilities are using badge readers and video extensively. He relays one specific use case from an Asia-Pacific enterprise where a network analyst noticed an anomaly on a critical server—events such as brute-force logins or unauthorized copying of data to a USB stick would trigger an event. The video analytics system this company had installed not only streams video on demand, but takes snapshots of certain high-value locations, such as a data center, based on a trigger from an analyst. Within seconds, the analyst had an image of a user inside the data center, could correlate that against an access log and determine whether that individual belonged inside the data center. If this were determined to be a malicious and unauthorized user, physical security could be notified.

Video surveillance is entering the picture as analog cameras are replaced with network-aware cameras that allow users to view locations remotely, store video digitally and manage it remotely over an IP network.

"Now with the advent of IP-ready physical security systems, it makes the transition easier," Contos says. "It used to be that if you wanted to upgrade physical security systems, you'd wait a couple of decades. With, IT things get upgraded quickly; every 18 months. With wireless and IP-centric solutions, you slap up a couple hundred IP-centric video cameras around your facility and you don't have lay cable or drill through concrete. You can have a pretty robust system, and to boot, you can use the system over an IP network and bring it all together. The availability and cost with these new technologies are allowing physical security groups to do upgrades on par with how quickly IT does upgrades."

IP-capable cameras and badge readers also ease integration, unlike their predecessors which evolved in a vacuum. Today's video cameras and badge readers not only communicate either wirelessly or on their own segmented VLANs, but they create logs and track events. This enables IT to pull these in centrally, and correlate physical and IT logs via a SIM. And since they're essentially computers, storing information on databases or being accessed often via Web applications, those avenues must be kept secure as well. Organizations especially need to keep the integrity of this data in case it's required in an investigation.

The ability to establish an audit trail is critical, Grassie says.

"For example, in the biotech and biopharma industries, there is a requirement from the Food and Drug Administration (FDA) and Health and Human Services (HHS) to have an audit trail to determine how batches [of drugs] spoiled," he says. "By utilizing converged security, this assists investigations further. There are cameras to monitor pill finish lines at pharmaceuticals. If a problem arises, they go to the database, identify where the lot is contaminated. This saves them a lot of money, rather than throwing the output for a day away."

CONVERGENCE STREAMLINES BUSINESS PROCESSES

Cost savings are a huge business driver for convergence. Enterprises quickly realize the similarities between the two operations and see opportunities to consolidate security processes and policies. For example, security operations can be combined to have one team trained to monitor logs and systems, eliminating a duplication of efforts and cross-staffing. Also, information sharing between the disparate groups improves, and a centralized operation no longer competes for budget dollars the same way separate entities would.

> "Once a process is in place and the boundaries are known, IT looks at events on the network making sure they are keeping these physical systems up and running and operational."
>
> –BRIAN CONTOS, chief security strategist, Imperva

"There are certainly some coordination issues: 'Who does what? Who am I supposed to notify?' I wouldn't say it requires more people power, but it does require more process" Contos says. "These are very different groups, with different perspectives on what they are trying to do and trying to protect. So a lot of times, it's really the direct managers each of the groups making sure processes are well coordinated."

Contos says, however, that the process moves a lot smoother than, for example, the convergence of application and data security with network security.

"Once a process is in place and the boundaries are known, IT looks at events on the network, and making sure they are keeping these physical systems up and running and operational," Contos says. "The physical security guys are the ones who ultimately respond to incidents. They become the response leg of the IT department when it comes to a physical security event. Once a process is in place, no additional manpower is necessary. It can be taken care of by opening lines of communication."

No business process benefits more from convergence than provisioning, experts say. Being able to combine on-boarding and off-boarding of employee access in one process is invaluable. Insider threats have been well documented; a 2007 Carnegie Mellon University study on insider threats said that critical system disruptions, loss of confidential intellectual property, fraud, reputational risk, and loss of customers, partners and future revenue were attributed to actions by disgruntled insiders. Often, problems arise from an insider retaining his system and/or physical access long after termination of employment.

By converging the assignment of proximity badges for door access, for example with network access control processes, one central entity can be responsible for terminating every avenue of access.

"In a previous life, eight or nine years ago, I had to go out to each group for access," Woerner recalls. "Having a single point of focus for access control not only manages on-boarding and off-boarding, but ensures whether access is appropriate."

"Nothing is more important than terminating access," Grassie adds.

Convergence is within reach of many large enterprises, especially as vendors such as Cisco, General Electric, Symantec, McAfee and Check Point continue to invest in information technology products that support traditional physical security.

Companies with global operations will continue to explore convergence, especially IP-based physical systems that integrate well with open network and application platforms and Web services. Organizations will be able to reduce risk, unify management, and centralize asset protection, provisioning and access control

"Convergence offers the opportunity for an enterprise to develop a comprehensive security strategy that aligns security goals with corporate goals," Grassie says. "If information is king, I think IT folks have a greater opportunity to converge physical and logical security. The less information-dependent a company is, the more the physical security guy can survive."▸

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SIMs

RISK METHODOLOGY

PHYSICAL-LOGICAL CONVERGENCE

SPONSOR RESOURCES

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.