

SPECIAL ISSUE

INFORMATION  
**SECURITY**<sup>®</sup>

**Look who's  
coming  
to dinner**

**INTERNAL AUDIT + FINANCE + HR + IT**

*Security Steering  
Committee*



In this  
SPECIAL ISSUE,  
we explore the  
importance and  
effectiveness of security  
steering committees  
and how these groups  
help integrate  
information security  
into the business.

## FEATURES

### 12 The Company You Keep

**SECURITY STEERING COMMITTEE** What better way to facilitate the integration of security and business than to bring all interested parties to the same table. *By Michael S. Mimoso*

### 20 Not So Different

**INTERNAL AUDIT** Internal audit and information security may often find themselves at odds, but in the end, their respective goals are the same. *By Michael S. Mimoso*

### 24 Necessary Cooperation

**HR** The teaming of human resources and security pros is mission critical for protecting corporate data. *By Marcia Savage*

### 30 Risk Spoken Here

**FINANCE** CFOs live in a world where risk management is the lingua franca. CISOs have to join the conversation. *By Neil Roiter*

### 36 Appropriate Urgency

**IT** Technology executives focus on elevating information security in the enterprise. *By Amy Rogers Nazarov*

### 42 Rising Profile

**SMBs** Security has the attention of SMB execs; the time for facilitating integration is at hand. *By George V. Hulme*



## COLUMNS

### 6 EDITOR'S DESK

#### A Great Way to Integrate

Driving security into lines of business takes dedication, effort and a steering committee.

By Michael S. Mimoso

### 7 PERSPECTIVES

#### A New Recipe for Fraud

In making risk decisions, security pros should consider three factors that fuel insider fraud.

By Ron Woerner

### 8 FACE-OFF

#### State Data Breach Notification Laws: Have They Helped?

There are more than 40 state notification laws, but how have they impacted the security of sensitive data? Our two experts debate the issue.

By Marcus Ranum and Bruce Schneier

### 54 PING

#### Anthony Meholic

The Republic First Bank information security officer offers guidance on maintaining a security program in lean economic times.

By Marcia Savage

## DEPARTMENTS

### Product Reviews

#### 47 ENDPOINT SECURITY

Trend Micro's Trend Micro Worry-Free Business Security 5.0

#### 48 WEB APPLICATION SECURITY

Cenzic's Cenzic Hailstorm Enterprise ARC 5.7

#### 49 DATABASE SECURITY

Sentriigo's Hedgehog Enterprise 2.2

#### 50 MOBILE SECURITY

GoldKey's GoldKey Secure USB Token

#### 51 TECH FOCUS

Sour Note on Endpoint Suites

Tests suggest AV products need more than a little tuning.

By Neil Roiter

#### 51 AT YOUR SERVICE

Mimecast's Unified Email Management

By Neil Roiter

#### 52 Advertising Index

# SEARCHSECURITY.COM online now

The Web's best security-specific information resource for enterprise IT professionals, and home of *Information Security*.



## SPOTLIGHT: SNYDER ON WIRELESS SECURITY

### Video: Setting Up a Secure Wireless Network

Providing secure wireless access to employees requires careful consideration. A proper enterprise wireless network must incorporate Wi-Fi standards such as 802.11i and WPA. Inbound and outbound security policies must be created to handle unauthenticated guest user access, and security teams have to invest in the appropriate technology, such as WLAN switches, firewalls and intrusion detection systems.

In an exclusive video presentation, network security expert Joel Snyder goes beyond the basics and carefully walks viewers through all the key phases of a secure wireless setup. Get the same topnotch instruction offered at our in-person seminars—without having to leave your office.

[/video](#)



## WEBCAST

### Compliance and NBA

In this presentation, compliance expert Ed Moyle details network behavior analysis (NBA) technology and how it can be used to advance compliance for mandates such as HIPAA, SOX and PCI DSS.

[/webcast](#)

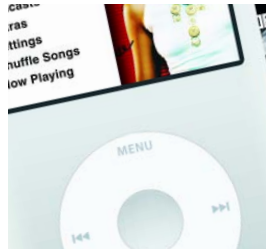


## EXPERT ADVICE

### New Threats Expert

Have you visited SearchSecurity.com's Ask the Experts section recently? If not, you're missing out on advice from the industry's leading practitioners. Plus meet our newest expert, John Strand.

[searchsecurity.com](#)  
click: [Advice](#)



## PODCASTS

### Sounds of the Season

Join the thousands who are downloading SearchSecurity.com's information security podcasts. This month's theme focuses on recapping the best interviews analysis and advice of 2008. New shows are added weekly.

[/podcast](#)

# INFORMATION SECURITY®

## EDITORIAL

**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

**EXECUTIVE EDITOR** Dennis Fisher

**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

## HOW TO REACH US

**SUBSCRIPTIONS: 888-804-5501**

117 Kendrick St., Suite 800, Needham, MA 02494  
Phone 781-657-1000 Fax 781-657-1100  
[www.infosecuritymag.com](#)



**always online**

Daily News, IT Knowledge Exchange, Tips, Ask the Experts, Webcasts, Podcasts, White Papers, Downloads, Careers, Security Bytes Blog and more.



Copyright © 2009 Information Security and TechTarget. All rights reserved. No part of this magazine may be republished or redistributed in any form, including electronic, without the express consent of TechTarget or Information Security.





**“It seems that the security community is unaware of the massive smart card migration that has begun across the border in Canada.”**

—FABIAN SOLER,  
on “Cracking Smart Cards,” October 2008

## Canada Ahead of Smart Card Curve

I found Neil Roiter’s technical article on differential power analysis in chip technology (“Cracking Smart Cards,” October 2008) very interesting. The existence of this threat, and also the effective countermeasures licensed by CRI, are an important addition to the security community’s knowledge. There was something else caught my interest in that article.

The article mentions smart card use in Europe, and the fledgling use of smart cards in the U.S. Based on that brief description, it seems that the security community is unaware of the massive smart card migration that has begun across the border in Canada.

In a nationally coordinated effort, all Canadian financial institutions and acquirers are poised to replace at least 55,000 ATMs, 450,000 payment terminals, and 33 million plastic cards between now and 2015 with CHIP-based terminals and cards. The effect it will have on fraud and identity theft in Canada will be significant.

It is also expected to drive away fraudsters, but they may simply refocus their efforts on markets that lack these stronger controls. It’s important that security professionals educate themselves about these plans in order to have a clear view of the threats and trends in the North American payments marketplace over the next decade.

FABIAN SOLER

## How to Make Friends and Influence Colleagues

Ron Woerner’s column about Dale Carnegie (“Required Reading,” October 2008) is outstanding advice, absolutely on target. I am keeping Ron’s suggestions very close at hand and will use them daily.

PETER HAWLEY  
system analyst, Hartford Technologies

## Active Directory is Not an OS Melting Pot

Neil Roiter’s article (“Central Control,” September 2008) suggests you bring Unix, Linux and Mac under the Active Directory umbrella. Who would want to?

Novell’s eDirectory already can, and with eDir’s superior granularity you can do things that AD can’t even dream about. Besides how a security magazine can say Microsoft and “security” in the same sentence is beyond me (maybe it’s just tongue in cheek then.)

TIM R. HAUZINGER  
Canadian Western Bank Group

CONNECT  
TO US >>>

<<< Send your comments to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).

We reserve the right to edit letters for clarity and space.

# A Great Way to Integrate



Driving security into lines of business takes dedication, effort and a steering committee.

BY MICHAEL S. MIMOSO

Not long ago, the smart people at Carnegie Mellon University's CyLab security research and education center wrote a report on the disconnect between senior management, boards of directors, and those responsible for information security in the enterprise. The results were disturbing because they pointed out how little oversight executives and board members have over security, and how unaware directors are of security and privacy budgets, and roles and responsibilities.

Among a long list of recommendations coming out of the CyLab Governance and Enterprise Security report was the need to include IT risk in an enterprise risk management program, segregate responsibility for security oversight away from audit committees, and establish a separate risk committee that assesses enterprise risks, including IT risks.

Also tucked away on the list was the suggestion to establish a cross-organizational entity that meets regularly to discuss security and privacy issues and include on that team, among others, legal, finance, HR, public relations, the CIO and security and privacy management.

Way ahead of ya.

Our annual year-end, new-year kickoff issue looks at exactly that. Starting on p. 10, we look at what it takes to establish what we're calling a security steering committee, and how those committee members view their roles on the committee and how they view you. Read on if you dare.

For some it will be an interesting reality check; for others, affirmation that you're on the right track.

One thing should stay with you: A well-orchestrated committee can do more for the integration of security into lines of business than most policies or processes you can develop.

Not only do these committees afford you the opportunity to talk out security and privacy issues and explore compliance implications of new projects and technology purchases, but they provide an important forum for business line managers, security officers and executives to get on the same page. They will simplify procurement processes, ease anxiety over budget requests and cut hassle and haggle next time someone in a particular business unit gripes over a new security mandate.

Steering committees aren't easy ventures to pull

off. Kirk Bailey, University of Washington CISO, dedicates significant time to the committee to keep it vital. Kirk says it takes "a lot of coffee and a lot of side conversations," but the payoff is enormous.

Connect with management and encourage them to participate, and don't sweat the type of executive you recruit at first; VPs aren't always the best conduit to get your objectives accomplished. Business unit liaisons need only to be interested in security and be willing to evangelize for you. Don't miss out on the opportunity you have to educate your HR and PR people about security. Spend the first few meetings talking about how risk impacts business; this groundwork will help them make informed decisions about security later on.

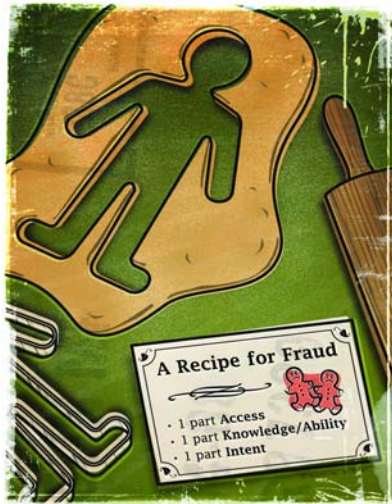
But it's not all roses. There are common mistakes.

Whatever your do, don't make it a status meeting. Forrester Research principal analyst Khalid Kark implores you: Don't talk about the latest round of critical Patch Tuesday fixes or the latest spammer techniques. You set the agenda; make sure it's strategic and use it to guide decisions based on risks that are acceptable to the company. Otherwise, before you know it, your VPs will drop off, and they'll start sending their reps, and pretty soon their reps will start sending their reps, and your committee is just another Outlook invite.

"It's a great idea to get conversations about security going," Kark says. "You've got to know what you're doing and be savvy about a steering committee. It sounds simple to do one of these, but it requires a lot of backend effort and a lot of framing up front to succeed." •

*Michael S. Mimoso is editor of Information Security. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

# A New Recipe for Fraud



In making risk decisions, security pros should consider three factors that fuel insider fraud. **BY RON WOERNER**

On almost any given day you can find a news story about an employee who has gone bad and committed a crime or damaged an organization. Insider threat is a timeless problem. It's always been there and it always will be there. Why? Because companies need to trust their employees in order to stay in business.

The most widely accepted model for explaining why good people go bad is the fraud triangle created by noted criminologist and sociologist Dr. Donald Cressey in the early 1950s. According to Cressey, three factors

must be present at the same time in order for someone to commit a security breach: pressure or motivation, rationalization and opportunity.

Today's electronic society has changed this model. In Cressey's time the incentive was mostly financial, but now there are many other reasons why a person may bypass security or commit fraud. In the early days of IT, hackers wanted fame or were just curious to see if they could pull off an exploit. These days the motive may be revenge against the company or an employee, which is not financially related. Pressure to get the job done no matter what may also cause someone to skirt security.

Therefore, I postulate that there is a new fraud model to consider. To commit fraud, or any other improper action, a person needs the following three elements: access, knowledge/ability and intent.

**Access:** Physical or logical ability to enter, touch or reach a resource. In computers, this is often controlled by network rules, access control lists (ACLs) and a user ID and password.

**Knowledge/Ability:** Familiarity or experience with an object or resource. This means knowing what to do after accessing the resource.

**Intent:** The purpose or an anticipated outcome that guides a person's planned actions; knowingly causing damage to the resource.

Here's an example of how these elements fit together. Suppose I have a logon ID and password to our mainframe computer, therefore I have access. Not only that, but I am given full administrator rights to it. The problem is I'm a neophyte on the mainframe—I barely know how to log on. Plus, I like my organization and don't want to cause it harm. Therefore, I'm missing two of the three requirements for fraud: knowledge and intent. Even though I have access, there is little risk of my caus-

ing intentional harm.

Access and knowledge are the elements most under our control (it's impossible to audit intent). If you can reduce a user's access/authority or increase the controls (which requires the attacker have more knowledge), then you reduce the risk. You must also ascertain what is required for the exploit. Many vulnerabilities require uber-hacker abilities to exploit them, like freezing the memory chips to bypass disk encryption. However, while only a minute percentage of people can normally exploit such vulnerabilities, there are increasingly more script kiddie tools available to reduce the knowledge level required.

Keeping the new fraud triangle in mind, an organization can reduce inappropriate behavior and fraud by having the following processes in place:

- Separation of duties
- Background checks, including a financial records check
- Job rotation/cross-training
- Protecting and limiting access to administrator accounts
- Role-based access control (RBAC)

By considering the access, knowledge and intent required to compromise a system, you can make more intelligent risk decisions. Furthermore, using these concepts promotes the proper balance of security within an organization, thereby reducing costs while improving security. ▸

*Ron Woerner is a security officer at a large financial services firm. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*



# State data breach notification laws: Have they helped?

POINT by **MARCUS RANUM**

THERE'S AN OLD SAYING, "Sometimes things have to get a lot worse before they can get better." If that's true, then breach notification laws offer the chance of eventual improvements in security, years hence.

For now? They're a huge distraction that has more to do with butt-covering and paperwork than improving systems security.

Somehow, the security world has managed to ignore the effect voluntary (?) notification and notification laws have had in other fields—namely, none. We regularly get bank disclosure statements, stock plan announcements, HIPAA disclosures, etc.—and they all go immediately in the wastebasket, unread. When I got my personal information breach notification from the Department of Veterans Affairs, it went in the trash too. "Your personal information has been disclosed...yadda, yadda, yadda"—annoying stuff that's my responsibility to deal with because someone, someplace else, didn't handle data about me responsibly. We are deluged with fine-printed disclosures and warnings, and

"Breach notification laws don't actually do anything to encourage good behavior; they just make bad behavior more obvious and expensive."

—MARCUS RANUM

eventually they're all as empty of meaning as the Department of Homeland Security's color-coded terrorism threat warning level.

Aside from causing numbness in customers' minds, breach notification laws don't actually do anything to encourage good behavior; they just make bad behavior more obvious and expensive. The theory, I suppose, is that businesses will improve their security out of fear of losing customers due to a breach. There are three problems with this theory:

- Most customers seem to assume that if one bank/brokerage/hospital/whatever can't keep its data secure, it's likely that *none* of them can, and there's zero incentive to switch.
- It's already too late. You might be able to motivate a customer to switch providers *before* there is a problem, but after there's a problem, they're going to be more

likely to spend their time calling in fraud alerts and looking at their bank statements than complicating things further by switching providers.

- It assumes there is actually a free market. My Social Security number was leaked by the U.S. government. As much as I'd like to fire *them*, I can't.

All I see breach notification laws doing is informing customers that they need to pay attention to their horses after they've left the barn via an unlocked door in someone else's barn. Not to over-stretch an analogy, but if you let my horse out of your barn, it's your problem to catch him safely and if anything bad happens to him while he's gone walkabout, it's your responsibility. What these data breach laws are really saying to the consumer is "our mistake is your problem and we're bending over backwards to make sure you know that...it's your problem."

We know that's silly.

But breach notification laws encourage businesses and government agencies to worry about entirely the wrong thing—they should be worrying about the barn door. Most importantly, it shouldn't be the customer's problem.

A lot of personal information is at risk because it is stored in systems that are not well designed to separate information within the organization. Some of us were warning about this back in the late 1980s; it's a bad idea to have your database configured so every secretary and contractor can access any record it contains.

As long as systems are built that way, there will be news stories such as "Bored contractors examine presidential candidates' medical records" or "Customer database sold by ex-employee." This is not rocket science; it's just common sense. I'd rather have my government agencies and commercial providers worrying about how to fix their poorly designed systems than having their lawyers word-smithing breach notices. •

*Marcus Ranum is the CSO of Tenable Network Security and is a well-known security technology innovator, teacher and speaker. For more information, visit his website at [www.ranum.com](http://www.ranum.com).*





Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).

## COUNTERPOINT by **BRUCE SCHNEIER**

THERE ARE THREE REASONS for breach notification laws. One, it's common politeness that when you lose something of someone else's, you tell him. The prevailing corporate attitude before the law—"They won't notice, and if they do notice they won't know it's us, so we are better off keeping quiet about the whole thing"—is just wrong. Two, it provides statistics to security researchers as to how pervasive the problem really is. And three, it forces companies to improve their security.

That last point needs a bit of explanation. The problem with companies protecting your data is that it isn't in their financial best interest to do so. That is, the companies are responsible for protecting your data, but bear none of the costs if your data is compromised. You suffer the harm, but you have no control—or even knowledge—of the company's security practices. The idea behind such laws, and how they were sold to legislators, is that they would increase the cost—both in bad publicity and the actual notification—of security breaches, motivating companies to spend more to prevent them. In economic terms, the law reduces the externalities and forces companies to deal with the true costs of these data breaches.

So how has it worked?

Earlier this year, three researchers at the Heinz School of Public Policy and Management at Carnegie Mellon University—Sasha Romanosky, Rahul Telang and Alessandro Acquisti—tried to answer that question. They looked at reported data breaches and rates of identity theft from 2002 to 2007, comparing states with a law to states without one. If these laws had their desired effects, people in states with notification laws should experience fewer incidences of identity theft. The result: not so much. The researchers found data breach notification laws reduced identity theft by just 2 percent on average.

I think there's a combination of things going on. Identity theft is being reported far more today than five years ago, so it's difficult to compare identity theft rates before and after the state laws were enacted. Most identity theft occurs when someone's home or work computer is compromised, not from theft of large corporate data-

bases, so the effect of these laws is small. Most of the security improvements companies made didn't make much of a difference, reducing the effect of these laws.

The laws rely on public shaming. It's embarrassing to have to admit to a data breach, and companies should be willing to spend to avoid this PR expense. The problem is, in order for this to work well, public shaming needs the cooperation of the press. And there's an attenuation effect going on. The first major breach after the first state disclosure law was in February 2005 in California, when ChoicePoint sold personal data on 145,000 people to criminals. The event was big news, ChoicePoint's stock tanked, and it was shamed into improving its security.

Next, LexisNexis exposed personal data on 300,000 individuals, and then Citigroup lost data on 3.9 million. The law worked; the only reason we knew about these security breaches was because of the law. But the breaches came in increasing numbers, and in larger quantities. Data breach stories felt more like "crying wolf" and soon, data breaches were no longer news.

Today, the remaining cost is that of the direct mail campaign to notify customers, which often turns into a marketing opportunity.

I'm still a fan of these laws, if only for the first two reasons I listed. Disclosure is important, but it's not going to solve identity theft. As I've written previously, the reason theft of personal information is common is that the data is valuable once stolen. The way to mitigate the risk of fraud due to impersonation is not to make personal information difficult to steal, it's to make it difficult to use.

Disclosure laws only deal with the economic externality of data owners protecting your personal information. What we really need are laws prohibiting financial institutions from granting credit to someone using your name with only a minimum of authentication. •

**"In economic terms, the law reduces the externalities and forces companies to deal with the true costs of these data breaches."**

**—BRUCE SCHNEIER**

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



# Set your own table



## *Internal Audit*

SOOTHE SOMETIMES CONTENTIOUS RELATIONSHIPS;  
REALIZE YOUR RESPECTIVE GOALS ARE THE SAME.

PAGE 20

## *Finance*

JUSTIFY SECURITY'S WORTH TO THE BUSINESS,  
AND THE MONEY WILL FOLLOW.

PAGE 30

## *HR*

SOLVE THE PEOPLE PROBLEM ARM IN ARM  
WITH HUMAN RESOURCES.

PAGE 24

## *SMBs*

FORGING RELATIONSHIPS TAKES ON GREATER IMPORTANCE  
IN SMALLER COMPANIES.

PAGE 42

## *IT*

ALIGN WITH YOUR CIO, DEMONSTRATE THE  
VALUE OF SECURITY TECHNOLOGY.

PAGE 36

## *Security Steering Committee*

LEARN FROM OTHERS BEFORE EMBARKING  
ON YOUR OWN TABLE SETTING.

PAGE 12

**CISOs HAVE PERENNIALY CLAMORED** for a seat at the boardroom table in order to integrate information security into business processes. But those invitations have been few and far between. One alternative is for security to set its own table via security steering committees, and initiate the process themselves. »

**What better way  
to facilitate the  
integration of  
security and  
business than  
to bring all  
interested parties  
to the same table.**



**BY MICHAEL S. MIMOSO**

**the  
you**



### **A PICTURESQUE TABLE SETTING**

may gleam a mix of polished silver and crystal, but it's nowhere near perfect without the right guest list. People make a party, and this particular table is adorned with ornate place cards pointing your invitees to their spots: internal audit to the right, HR and finance across the table, IT to the left. No, this isn't your boss' board meeting; it's the regular gathering of the security steering committee, and it's the CISO who is writing out the invitations and setting the table.

Security steering committees aren't a new concept, but they are popping up in more corporate settings and allowing security management to better facilitate the integration of security into business processes. If you're a CISO with internal, industry or federal compliance mandates, it's becoming increasingly difficult to do business without establishing such a body.

But be forewarned: these aren't foolproof exercises. Before your gathering has muscle, before it formulates policies, debates liability and risk, and manages compliance obligations, it needs a sense of formality built on a legion of legwork usually done by a security manager eager to set his own table.

# company keep

## PASS GO

It may be sacrilege to hold an administrative meeting in the city of Seattle without serving coffee, but University of Washington CISO Kirk Bailey cannot afford caffeinated distractions when it comes to the institution's Privacy Assurance and Systems Security Council. The PASS Council is the epitome of a successful and influential security steering committee within an enterprise, one with a long reach into important decision-making entities.

Besides, if someone really wants coffee, there's a Starbucks on every corner.

The PASS Council is a chartered organization at UW, and has administrative authority, oversees system security and privacy assurance, and is responsible for the university's risk and compliance strategy for system security and privacy.

It meets monthly, and is likely Bailey's most indispensable tool when it comes to risk mitigation, policy development and the execution of compliance-related activities. Among the 16 regular invitees (14 voting and two advisory) are what would be considered

business-unit leaders in an education setting: an assistant VP of human resources; executive director of risk management; lab director, computer science and engineering; HIPAA compliance officer; associate vice provost of enterprise information services; a facility security officer; executive director of internal audit; the campus police chief; and an assistant Attorney General, UW Division of the AG's office.

"It's just been a wonderful benefit to have that regularly scheduled, officially chartered body to throw ideas and issues around," Bailey says. "It's just been a delightful forum, an enormous benefit. And not just that it is supporting an institutional security and risk-control program; it's a powerful and persuasive group for you to act as a CISO with."

By gathering these important institutional people, Bailey, who chairs the PASS Council, has a one-stop forum to air out legal, compliance or privacy issues as they pertain to the security of systems. Risks associated with new initiatives are identified and hashed out in committee meetings, and budget arguments are formulated—all with the goal of developing a

strategic plan for information security at UW. Overall, the visibility of security is elevated to unprecedented heights.

"The PASS Council serves to promote security in very advantageous ways, especially if you're doing it in language [business leaders] understand," Bailey says. "PASS helped me produce, as a product, a risk picture, a strategic plan associated with the risk picture, a budget associated with the strategic plan, and ongoing reporting to management with their approval and endorsement. It's hard for anybody not to listen to what I'm asking for when it represents the institutional risk officers behind it. How could you operate without it?"

It's crucial too to keep these meetings strategic and about mitigating risk to individual business units or the enterprise overall, otherwise interest and attendance will wane and the effectiveness of the group ends (*see "Failure is Not an Option," left*).

"Don't let it be a status or operational meeting. Make it strategic where senior-level people are able to make decisions based on information being shared with them," says Forrester Research principal analyst Khalid Kark. "What often can happen is that senior executives come in to the first

## Failure is not an option

### HERE ARE EIGHT THINGS TO REMEMBER TO KEEP YOUR SECURITY STEERING COMMITTEE AFLOAT FOR THE LONG HAUL.

1. **get** the right buy-in from security, executives and business leaders that they will participate.
2. **don't** get hung up on titles. Look for those who are interested in and could evangelize security or act as a liaison between security and the business.
3. **educate** your committee members on how to think about risk and how it applies to their business; in turn they'll be able to make useful decisions.
4. **stay** on topic. Don't talk about spam, vulnerabilities or patching. Keep meetings strategic and think about how you can steer the risk appetite of an organization.
5. **bring** metrics to the table. This can't be a status meeting; you need metrics to be able to answer questions and make decisions based on historical data.
6. **charter** the committee. Get formal sign-off from executive management and formalize roles and responsibilities for committee members.
7. **keep** membership consistent and meet regularly.
8. **set** the agenda and send out materials in advance. ▸

SOURCES: Khalid Kark, Forrester Research; Kirk Bailey, Timothy McKnight, Jerry Freese.

few meetings and talk about security. But over the course of a few months, things die down, and they start sending representatives, and then their representatives send their representatives, and the effort is not at the level where it initially started. It ends up being a logistical or operational type of effort where you're either going through status or going through information that does not mean anything to anyone attending—it's either too high level or low level."

The PASS Council's natural intersection of business and security officials facilitates the development and processing of security or privacy policies. Decision makers can expedite funding or approval of policy changes or spending on new security projects knowing that the PASS Council and its wide-ranging representation has already endorsed the initiative.

"This is a group of risk managers an institution would bring together to deal with a response anyway. Having them in place to do preventive discussions and formulate policy to mitigate the liability sets and understand compliance obligations is just powerful," Bailey says. "If an institution doesn't have one, it's missing an opportunity, or you've overlooked a compliance requirement. If you're a security professional operating without such an entity, you're giving yourself a ton of work because you have to run around and talk to these people anyway."

Security steering committees don't have to be strictly advisory. A powerful committee can also assist with incident response, and help minimize reputational risks and costs in the event of a breach. The UW PASS Council, for example, gave Bailey intervention authority to mitigate incidents with the blessing of the institution's risk managers, including the executive director sitting on the PASS Council who is the university's underwriter (UW is self-insuring and all risk questions have an immediate business interest, Bailey says).

"I get to move in without much argument because they know it's done with the consent of the risk manager, auditor and legal—it's hard for anyone to object to our involvement," Bailey says, adding that any complaints would eventually arrive at the desk of a senior manager who is likely associated with the council. "I know security pros are considered a little autocratic, but truth is, in a preemptive action, this council supports that need."

Bailey approaches incident mitigation and response as a service, arriving not only with his expertise, but with the necessary tools and forms required to fend off disaster and appropriately document it. Departments can use that documentation, for example, to make their case for budget changes

### University of Washington Privacy Assurance and Systems Security (PASS) Council

CHAIR BY Kirk Bailey

MEETS every fourth Monday of the month

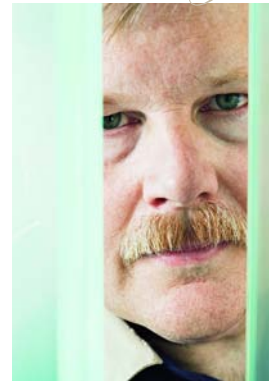
CHARTERED by the university

14 VOTING members

2 ADVISORY non-voting positions

MEMBERS include campus police chief; vice presidents or directors of UW Medicine, Health Sciences, Computer Science and Engineering, Research Information Services and Risk Management (Underwriting); CIO; HIPAA compliance officer; executive director of internal audit and others.

DELIVERABLES include information systems and data security strategic plan; privacy policies, standards, guidelines, risk assessment and risk management program; incident response program; support services for UW compliance requirements. ▶



to prevent future recurrences.

"If the PASS Council becomes involved, people trust it. If you're a department manager who has had a terrible breach, and you're looking at millions of dollars worth of losses and worried about reputation, if I knock at your door and say I'm here to take over this incident with your help, people are relieved," Bailey says. "(Public relations) is in place; we have legal opinions at the ready, risk underwriting ready to answer questions, all congealed into one quick-acting service. If it's planned well, I can't understand living without it."

Bailey says for a security steering committee to flourish it's important that the membership remain fluid and represent an institution's most important risk and administrative areas. Ensure that the committee's interactions meet the needs of its member business units because that helps support its acceptance and effectiveness as an institutional body. And, he says, don't be afraid to expand the group's responsibilities as chartered by providing services in areas that might seem out of its scope, especially in terms of IT policy development.

"If you want this to be well established, you have to dedicate time to it as a security professional. You've got to dedicate resources and energy to make this happen and keep it vital," Bailey says. "I invest an enormous amount of time in it to keep it growing and thriving."

## AUTHORITATIVE ROSTER

Northrop Grumman, similar to UW, has a chartered security steering committee that's been part of the fabric of the defense contractor's information security program for more than a decade. With a roster of internal heavyweights including information and industrial security, lines of business heads of security, as well as representatives of legal and human resources, Northrop Grumman's Corporate Security Council has authority over everything pertaining to information security from buyer contingency planning to investigative issues, says Timothy McKnight, vice president and CISO.

**"WE REALLY DRIVE THESE TEAMS TO EXECUTE AND DRIVE SPECIFIC REQUIREMENTS ACROSS THE COMPANY. WE'RE PRETTY ADVANCED COMPARED TO MOST CORPORATIONS."**

**-TIMOTHY MCKNIGHT, vice president and CISO, Northrop Grumman**

"We really drive these teams to execute and drive specific requirements across the company," McKnight says. "We're pretty advanced compared to most corporations."

How advanced? The structure is deep and complex, beginning with the Corporate Security Council at the top. Under the council is a core group of standing committees including international security, information security, contingency planning, program security, security technology, government

liaisons and personnel security. Under each of those committees are integrated process teams that drive common requirements across the corporation and achieve concurrence from business units on policy and strategy.

"It is a policy-making body for the company," says McKnight, who estimates that 50 percent of its time is devoted to policy creation and maintenance. Further evidence of its importance to the enterprise: Northrop Grumman regularly evaluates the effectiveness and necessity of its internal councils, and the security council is one of 33 such bodies recognized company-wide.

McKnight explains that once the Corporate Security Council has signed off on an initiative, the process moves to the CIO Council for approval from the CIO and eventually business unit leaders. McKnight also relies on what he calls a customer advisory group, a collection of trusted leaders at the VP level who provide a reality check around security priorities.

"That's something I recommend to all my peers; that helps give you a third-party view on things and another check on what your investments are," McKnight says.

Having the ear of influential decision makers helps push through initiatives that have traversed this chain of influencers with minimal resistance.

"If we get to the point that we're presenting something at the sector level, they will ask if it has been reviewed and approved by the security or CIO councils," McKnight says. "Because they're the stakeholders for the company and they're communicating to lines of business, they're helping drive something that may be an enterprise effort."

The Corporate Security Council isn't all about policy setting, but engagement on procurement as well.

"As a collective body, we're spending a significant amount of corporate dollars on security as a whole; a lot of time is spent with key suppliers trying to control, or drive down, costs or improve performance," McKnight says.

An important deliverable coming out of the council in the next 18 months is a smart card deployment that will provide common access to buildings and stronger logical access to systems. The coordination between industrial and information security on such a project is immense, from technology procurement all the way down to badge design.

"I can't imagine, without a body like this, that we would be finally at a point where we're all in agreement and pushing forward on a very large corpo-

ittee by committee



### Northrop Grumman Corporate Security Council

CHAired BY Timothy McKnight

CHARTERED for more than 10 years

QUARTERLY meetings are face-to-face; monthly meetings are teleconferences

MEMBERS include information and industrial security, HR, legal and business unit heads of security

OBJECTIVES: Policy making and procurement. ▶



# deep insight into the network fewer intrusions into the workday

Featuring end-point intelligence with real-time network awareness, Nokia and Sourcefire® combine to create the new standard in network security. You'll maintain accurate, up-to-the-minute visibility into the network and dramatically reduce time chasing false positives. Stop kidding yourself, and start protecting your network.

**Work together. Smarter.**

[nokiaforbusiness.com/security](http://nokiaforbusiness.com/security)



**Nokia IP290**



**Nokia IP690**



**Nokia IP2450**

**NOKIA**

©2008 Nokia. All rights reserved. Nokia is a registered trademark of Nokia Corporation. Use of the word secure is intended to describe the functionality of the product or feature described, and is not intended to extend a warranty to the purchaser or to any end user that the product or feature described is completely secure and invulnerable to random attacks.

**Nokia for Business**

rate-wide program to roll out this capability that will help us tremendously,” McKnight says.

“It’s a good place to be.”

## NO CHARTER, NO PROBLEM

Not all security steering committees are chartered.

American Electric Power of Columbus, Ohio, has an Executive Security Committee that is made up of senior executives from HR, legal and IT, as well as operations and government affairs; reliability officers; and those responsible for federal regulatory compliance and compliance with rigid industry standards set forth by NERC (North American Electric Reliability Corp.).

While the committee has a standing set of members and a regularly scheduled monthly meeting, it is an ad hoc organization, says Jerry Freese, director of enterprise information security and IT engineering security. Freese says the membership can change depending on the issues at hand and who is impacted in the organization.

“The idea of the Executive Security Committee was to provide full disclosure of security for the business side. We’re very aware of the need for integration for security and business,” Freese says. “We can mandate security all we like in a vacuum, but as most companies have found out, that usually meets with a lot of resistance. The business has to be involved in all decisions that are made.”

Having business stakeholders at the table enables security to lay out all the risks to the concerned parties, and, more importantly, provides an opportunity for discourse on the subject.

“The whole idea is to get whoever could be the decision maker on the business unit side apprised of what we’re trying to do, what it means to them, what not doing it means to them from a risk perspective, giving them input from us, and asking them to provide feedback to us,” Freese says.

“We want to provide full disclosure of all events on the security side.”

With stringent NERC cybersecurity rules bearing down on organizations such as Freese’s, bringing all sides to the table via a steering committee takes on greater importance than ever. Freese runs the monthly meetings; he sets the agenda, which runs the gamut from updates on major security initiatives to compliance activities that must be communicated to the enterprise’s commercial operations units, as well as any legislative or regulatory updates.

“It’s quite a lot,” Freese says.

The committee will be invaluable going forward, he adds, because of the new NERC mandates. NERC is demanding that utilities such as AEP identify and protect critical infrastructure assets and ensure reliable operation of the bulk electric system.

“It’s a brand new thing for the electric sector. We have to come up with a lot of security implementations that we hadn’t really dealt with before. Some of these are fairly significant projects that cost significant dollars,” Freese says. “These are the type of things we have to explain why they are needed. I have a head start because it’s a required set of initiatives; nevertheless, we have to come up with a cost-effective way to do this.”

Freese says security organizations will eventually have to concede and formulate some sort of steering committee, otherwise they’ll be operating in a vacuum and eventually impede business. For example, having legal and HR already at the table goes a long way toward solving any potential difficulties having to do with discovery or NERC compliance around HR management systems.

“[A steering committee] does a great deal to enhance the credibility of security if it’s done correctly. I think it shows there are optimum solutions to protect the business as well as the company’s data and networks,” Freese says.

“It doesn’t have to be adversarial. I think we’re a good example. We’ve evolved into an organization that trusts that business and security will mesh and will sustain each other. It does change relationships a great deal.”

Michael S. Mimoso is editor of Information Security. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).

## Committee by committee



### American Electric Power Executive Security Committee

CHAired BY Jerry Freese

NOT chartered

MONTHLY meetings with a fluid membership

COVERS security initiatives, compliance activities, and legislative and regulatory updates.

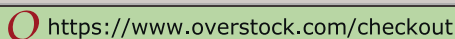
MEMBERSHIP includes HR, legal, finance, IT, government affairs

representatives, reliability officers and compliance officers. •



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



 <https://www.overstock.com/checkout>



Identified by VeriSign

**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](http://www.verisign.com/is) or call 1-866-893-6565 or 1-650-426-5115.



**CISOs ARE QUICK TO POINT OUT**

they are often at odds with internal auditors. Auditors are duty-bound to regulations and internal policy, and are accountable to ensure that industry and federal mandates are carried out by business leaders. Security officers bemoan that auditors pull the security staff in so many directions, and have them concentrating on controls that satisfy so many regs, that compliance supersedes security and the strategic plan is forsaken.

Reality may be a bit less contentious.

“I don’t think we have different goals personally. Internal audit and information security have same goal, which is to mitigate risk,” says Anthony Noble, vice president of IT audit at media giant Viacom. “Internal audit has a broader frame where we’re trying to mitigate financial risk, while information security mitigates data loss or disclosure. They shouldn’t have clashing agendas.”

Noble has refined this vision sitting on Viacom’s equivalent of a security steering committee, an ad hoc entity composed of information security, audit, finance, legal and human resources that formed on the heels of a publicly disclosed breach earlier this year.

**not so  
different**



# Internal Audit

- Sarbanes-Oxley
- PCI
- NERC
- FERC
- GLBA
- HIPAA
- Internal privacy policy
- Internal acceptable use policy

Check with CISO on PCI encryption upgrade status

NERC CIP deadlines upcoming

Review privacy policy updates with legal!!

# ent

**Internal audit and information security may often find themselves at odds, but in the end, their respective goals are the same.**

BY MICHAEL S. MIMOSO

As a result, the committee pushed through controls to secure personally identifiable information that include awareness training programs, the elimination of PII from business processes (e.g., the use of Social Security numbers as identifiers), and a DLP implementation that scans files for sensitive information. Noble's job is one of checks and balances that ends up being much more than a rubber stamp on the process. Up front he helps evaluate the committee's plans and points out potential gaps that could increase risk. And on the back end is the validation of whether work was done as promised and that controls are working and effective. His participation up front via the committee allows him to monitor controls as they're being developed and ward off shortcomings before they're put in production.

"It's much more efficient to have that evaluation up front," Noble says, adding that he—and legal—audits against regulations such as Sarbanes-Oxley and state data breach notification acts, as well as internal policy. "We work fairly closely in developing the plan, and then there is that aspect of 'audit blessing' [afterward]."

Mergers and acquisitions (Viacom acquired CBS in 1999, and then the two split again in 2005) as well as the requirements presented by Sarbanes-Oxley drove information security and audit closer.

"[Security and audit] shouldn't have clashing agendas. The main area we might clash is if we say, 'Might it be good to do this control?' [and] they might turn around and say it's too expensive, that there's not enough risk to make the control cost effective," Noble explains. "In the end, we're both trying to mitigate risk. They have to evaluate the risk of data loss and we have to look at the risk of financial information being incorrect."

Whether tossed together contentiously or coexisting amicably, audit and security better get used to the sight of each other, especially in the current economic downturn that could bring more regulation and more demands for IT risk to be documented and presented.

"The current problems have really been driven by people accepting too much risk, and not necessarily that controls weren't there. From a business aspect, they weren't evaluating risk adequately," Noble says. "Personally, that's the aspect [that's going to grow]; you have to document more the risk you're taking to prove you're aware of risk. Enterprise risk management will be key."

Noble isn't in the camp that more controls will be the answer. Companies are already bogged down in expensive compliance programs, especially around SOX and PCI. Former Speaker of the House Newt Gingrich in November went so far as to call for a repeal of SOX.

"Companies are going to look to cut the cost of compliance with SOX and things like that. I can see companies screaming and saying 'SOX is costing us too much, we can't afford it in this climate,'" Noble says. "I think there will be a corresponding push toward more documentation of the business risk being taken by companies and more transparency to that. I think it's going to be difficult to implement more regulations because of the cost element because the cost of the control is going to be more than the risk. It's a cost balance."

## **GAP ANALYSIS**

Ram Sastry, an internal IT auditor at American Electric Power in Columbus, Ohio, believes that more regulation is inevitable in his industry and that it will draw him closer to information security. New NERC (North American Electric Reliability Corp.) standards that govern cybersecurity in utilities such as AEP aim to narrow gaps that expose critical infrastructure to attack. Sastry's teams are in place to assess what director of IT engineering security Jerry Freese and his teams are doing to ready business units and process owners.

"That's a good place where we have a strong working relationship," Sastry says. Sastry was a member of Freese's Executive Security Committee (*see "The Company You Keep," p. 12*) for three-and-a-half years up until 2006, participating alongside other business leaders in assessing information security projects as they pertain to the business.

Sastry says his role is one of evaluating initiatives for policies, procedures or processes that may be absent and vital to the success of a project. While up-front input is vital, in the end he has to ensure compliance with internal or industry regulations.

"If you ask me from an audit, compliance and regulatory standpoint, committee or no committee, this is what you need to get done," Sastry says.

Sastry, who is responsible for internal audits on NERC policies and processes, as well as AEP's SOX compliance processes, says audit looks at a new policy or upgrade from a different angle than security.

"We look at it from the lens, Can we audit from this policy? Is this policy auditable? Is it actually implementable? Are we having wide-scale exemptions that water down the policy? Are you directing people to do things but there's no way of preventing or detecting violations? Or are there mechanisms for providing a directive control, then preventing them from doing it and detecting them if they had done something inappropriate?" Sastry explains. He adds that his teams review internal control testing and those results are provided to external auditors who use them to build on their testing efforts.

Clearly, there has to be an affinity with information security for internal auditors.

Sastry says information security policies and standards are referenced as controls by internal audit.

“Absence of their policy and standard doesn’t give me a get-out-of-jail-free card. If there’s a problem I will state there’s a problem whether there’s a missing policy or procedure. Their lagging is my point,” Sastry says. “Where they’re not lagging, they’re absolutely an ally of mine.”

Sastry says it’s a healthy tension between internal audit and security, one that arises, obviously, when security is lacking an important cog in a policy or process. It’s Sastry’s job to point out the gap, and the internal or external policy line item that mandates why that gap must be filled. Sastry says the presence of a security steering committee, meanwhile, helps soothe some angst in those cases.

“If you put audit and the independent objective review of systems and security at one end of the spectrum, and you put the processor who is trying to do job No. 1 which is make money and keep customers happy at the other end, [the committee] lies in the center and tries to balance things,” Sastry says. “The

committee brings all points of views together, and says let’s get a compromise, a tradeoff set of solutions that adequately address the risk side, and the cost, compliance and process sides of the equation.”

The committee’s biggest benefit, Sastry observes, is the instant buy-in it affords to projects.

“At the end of that meeting, everyone agrees we have considered the alternatives, the risk, why we need to do it and we move ahead,” Sastry says. “You can go to lower levels of management and say that this has been agreed to by the ESC and now you have to comply with it. In our organization, if senior and executive management say you will do it, generally we will get good adoption.”

Clearly the days of operating in silos are over for information security.

“The key is collaboration, especially up front on plans and policies,” says Viacom’s Noble. “You both need to agree on what needs to be done and the level of control in the organization. From there it’s the business of internal audit to go in and validate.”

---

*Michael S. Mimoso is editor of Information Security. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

# Where security pros live

➔ **FREE** Webcasts

➔ **FREE** White Papers

➔ **FREE** E-mail Newsletters

➔ **FREE** Downloads of the latest Security Software

➔ **FREE** Online Security Training for CPE credits

➔ **FREE** Breaking News and Security Alerts

**FREE** Membership to  
SearchSecurity.com available at:  
[www.SearchSecurity.com/join](http://www.SearchSecurity.com/join)

 **SearchSecurity.com**  
The Web's Best Security-Specific Information Resource

TechTarget  
Security Media

 SearchSecurity.com

 SearchSecurity.co.UK

INFORMATION  
SECURITY

INFORMATION SECURITY DECISIONS

 SearchFinancialSecurity.com

HR



**necessary**

**cooperation**





ANITA OROZCO, director of human resources, Sonneborn



### **FIFTEEN YEARS AGO,**

when human resources executive Anita Orozco needed to hire or fire an employee, involving IT probably wasn't on her to-do list. But the Internet boom and employees accessing corporate systems from virtually anywhere changed that.

"Now it's definitely more important, whether getting a new employee set up with access to systems and software, or getting someone turned off," says Orozco, director of HR at Sonneborn, a manufacturer of refined hydrocarbons. "The turning off has become especially important. Generally, we'll give as much notice as possible to the IT staff so they can do what they need to do to protect the company."

Like others in her field, Orozco finds it increasingly important to work regularly with technology managers to ensure corporate data is secure. In the information age, human resources professionals are teaming up with their counterparts in IT security to investigate potential Web or email policy violations by employees, develop security policies and procedures, and plan for disaster recovery.

Bringing human resources and security together isn't always easy, though. The two have sharply different perspectives and there can be some tension, says Khalid Kark, principal analyst at Forrester Research. HR has its own set of policies and might view security as imposing IT policies that HR can't really implement; HR also has access to sensitive data, which security might want to limit, he says. It works best if a cooperative tone is set from the top, Kark says.

"Typically what happens in those organizations is the head of HR and the head of security have decided that they will work together," he says.

Winn Schwartau, founder of SCIPP International, a nonprofit provider of end user security awareness training, says the relationship between HR and secu-

## **The teaming of human resources and security pros is mission critical for protecting corporate data. BY MARCIA SAVAGE**

ity is “mission critical” but often can be overlooked. He encourages organizations to have the two departments work together in three areas: hiring of employees with access to proprietary information or control over large parts of the network; developing policy for employees who violate security rules; and making sure terminated workers cannot access corporate resources.

“We need to get HR as part of the process because security is about people,” he says. “It’s about their behavior, their intentions, proclivities, and tendencies.”

### BRIDGING GAPS

At Sonneborn, Orozco works across the hall from the IT director in the company’s Petrolia, Pa. office, which makes communication easy when security issues come up (see “*Lost in Translation*,” below). The company, which outsources its IT functions, counts about 160 employees in Pennsylvania and about 300 worldwide.

In addition to making sure new employees get the system access they need and former employees’ access

rights are terminated as soon as they leave the company, Orozco works with IT on security policy development.

When she first joined the company, the IT director expressed concern about the company’s policies on system use. “His argument was we need stronger controls, and management’s reply was that we can trust our employees,” she says. “So bridging that gap between the two and coming up with policies that would satisfy both has been important.”

Today, Sonneborn has tight controls on Internet use, and employees can’t download programs onto its systems. It also uses thin clients, and Orozco says the company has been free of computer viruses for years.

In working with technology personnel, she’s learned that they’re very structured and process oriented. “As long as I have a process and good checklist, it generally goes pretty well.”

In the end, human resources and IT are similar in that both are service oriented departments, she says. “They’re providing a service and I’m providing a service.”

Lee Kushner, founder and CEO of information

# Lost in translation

**DON'T USE JARGON WHEN COMMUNICATING WITH HUMAN RESOURCES.**



MELODY SILBERSTEIN

In working with human resources professionals, security professionals should make sure they’re “talking in a language the HR person can understand,” says Melody Silberstein, senior vice president of human resources at insurance brokerage Woodruff-Sawyer & Co.

“Sometimes my IT person and I are talking two different languages,” she says. “If I don’t understand what he’s saying, I don’t understand my risk.”

Using laymen’s language is critical in communicating the risks associated with newer tools that employees use, such as instant messaging, and also in supporting proposed equipment purchases, she says.

Since she’s been immersed in security, Silberstein has become aware of the security issues around outsourcing. IT security professionals can help HR teams understand the risks involved when they outsource and questions they need to ask third-party vendors, she says.

Lee Kushner, founder and CEO of information security recruiting firm LJ Kushner and Associates, says security professionals can help HR pros who are focused on recruiting to help them understand what type of person to hire.

“A big complaint of security professionals is, ‘HR doesn’t understand what I’m looking for,’” he says. “But if the security professional would actually sit down with the recruiter and give the recruiter a bit of an education on how to find or what to look for, you would definitely have more successful recruiting.”

Khalid Kark, principal analyst at Forrester Research, says security and HR professionals need open minds when they begin working together.

“Usually they have preconceived ideas around this is what HR or security is going to do,” he says. “Go in with the perspective that the other is there to help the organization. Don’t go in with the notion that HR doesn’t know or care about anything about security.”

—MARCIA SAVAGE



EDUCATION

University of Indianapolis  
Hacked: 11K Student,  
Faculty, Staff records stolen

Trojan horse captures data  
on 2,300 Oregon taxpayers

TECHNOLOGY

HOTEL CHAIN FALLS VICTIM  
TO 14,000 DATA-STEALING  
MALWARE INCIDENTS

40 Million  
Credit Card  
Numbers Stolen  
from TJX

Millions of U.S. customers were  
informed today that many of  
their credit card numbers

98,930 Affected In  
Forever 21 Data Breach

**THINK THE NEXT GENERATION OF MALWARE  
doesn't have a headline waiting for you?**

## THINK AGAIN.

Data-stealing malware is smarter, faster and more advanced than ever. It's infiltrating the most secure enterprises and yours could be next. But with Trend Micro™ Enterprise Security, powered by the Trend Micro Smart Protection Network, you'll be ready. This unique combination of solutions and services is the next-generation, cloud-client security infrastructure that blocks the most sophisticated threats—before they reach your network. Download our eBook and learn how easily Web threats like data-stealing malware can evade your current security solution and what you can do about it.

- ▶ Download our *Outthink the Threat* eBook and register for a free, onsite risk assessment now at [trendmicro.com/thinkagain](http://trendmicro.com/thinkagain). Or contact us for more information at 877-21-TREND EXT. 55



Securing Your Web World



security recruiting firm LJ Kushner and Associates, also sees the similarity. "HR is shared service, just like security. Security and HR have a lot in common because they affect everybody" in the enterprise, he says.

### COLLABORATIVE CULTURE

Melody Silberstein, senior vice president of human resources at Woodruff-Sawyer & Co., began working more closely on security issues with her IT director and IT manager about 14 months ago. The reason was twofold: the San Francisco-based insurance brokerage firm, which has 300 employees in six locations, was kicking off its first in-depth disaster recovery plan and also embarking on a review of its security procedures.

Silberstein leads the disaster recovery planning, which she says has involved understanding how quickly the firm could get its systems back up and running after an incident, revamping some systems for better backup, and building awareness.

"So much of disaster recovery is getting people to stop for a few minutes and think about what they'd

need if they had to walk out of the building and not come back," she says.

Reviewing the company's security procedures included looking at encryption policies for stored and transmitted data, and the physical security of its servers. As an insurance brokerage handling sensitive client data, security is critical, Silberstein says.

To tackle data protection projects, she and the IT executives get together as a team and bring in others from the company whom they feel could provide input.

"We'll define what our issues are, where we think we have gaps or risks, and what we need to close," Silberstein says. "If it's urgent or we're trying to close a gap quickly, we may meet weekly, but more frequently we set up meetings every other week and discuss what we figured out or how we closed a gap."

While the IT executives bring the systems expertise to these discussions, she and others can point to behavioral issues or what the risk will be from a people standpoint, she says.

The company fosters a collaborative culture in which everyone is working to achieve the best outcome, she says: "We try hard not to build silos."

### MATTER OF CIRCUMSTANCE

For Robert Miller, director of human resources at the Greater Los Angeles County Vector Control District, contact with information security pros is based on circumstance. The agency, which has about 100 full-time employees, contracts with an information security expert. It's the largest of five mosquito and vector control districts in Los Angeles County, serving six million residents.

For example, Miller worked with the contractor during a re-organization at the agency. The fiscal officer was slated for replacement, so Miller made a proactive move: "I had his computer backed up before we gave him the news because I didn't want any sabotage to our finance systems."

In litigation issues such as allegations of discrimination or harassment, Miller works with legal counsel and other agency officials to see where electronic evidence might support their position. They might decide, for instance, to pull an employee's emails for a particular time period. If the worker has a company-issued cell phone, they might also pull text messages. He taps the security pro for help in such cases.

In general, employees often don't understand that when they use company equipment to email or surf the Web, all that electronic information can be used as evidence, Miller says. He drafted and received approval from the district's board of

## Crisis coordination

### HUMAN RESOURCES AND SECURITY TEAMS WORK TOGETHER TO PREPARE THE ENTERPRISE FOR THE WORST.



Disaster recovery planning is a major area where human resources professionals team up with IT security pros.

The HR department is often the "conductor" of the crisis management plan while IT security teams help HR in ensuring systems remain operative, information is safeguarded, and employees can be located, says Paula Harvey, president of K&P Consulting, a human resources services firm based in Charlotte, N.C.

"Information technology and HR must work hand in glove," she says.

In crisis planning, HR works with information security teams, which tend to fall under IT in the enterprise, and physical security teams, Harvey says. HR and IT usually work well together, she adds.

"Both departments have spent time proving to companies how useful they can be and how they can save the company money instead of being a cost center," Harvey says. "They're kindred spirits."

—MARCIA SAVAGE



trustees for a policy that specifically outlines the organization's rules for proper email and Internet use.

"You have to have a policy in place that explains to people what their limitations on use are," he says. "They have to be fully aware it's discoverable and the boundaries they must stay within. That's for their protection and the employer's protection. The employer has to feel comfortable that people are doing what they're supposed to do when they're online, so security plays a large part there.

"Every human resources person who is involved in the strategic management of their environment needs whatever tools are available to assist the organization in moving forward," Miller says. "Information security is one of those tools."

At CIGNA, the information protection team works hard to make employees aware of company policies for Internet and email use, says Karen King, employee relations consultant at the Philadelphia-based health services and benefits company.

"When we first opened up the Internet and email to all employees, which we did over time, we saw a spike in the usage of it," she says. "HR, employee relations and information protection worked more closely together to figure out how to handle that and what types of disciplinary actions would be required."

The awareness campaign has paid off and employees are mindful of their Internet use and the need to ensure privacy of sensitive customer data, King says. In the event of a violation, the information protection team sends an email to the employee's manager, who engages employee relations or HR to confer on disciplinary action.

## **SECURITY BY COMMITTEE**

Money Management International, a Houston-based nonprofit credit counseling agency, has a committee that meets quarterly—sometimes more often—to discuss information security issues. Nearly every part of the business is involved in the committee, from the C-level to operations, which includes HR. Topics range from possible security breaches and awareness training to document retention and disposal.

Everyone in the organization, which has about 1,200 employees in more than 120 locations in 23 states, takes a proactive stance when it comes to security, says Thomas Anderson, national director of human resources at MMI.

"It's very important as far as our corporate mis-

sion, which is improving lives through financial education," he says. "Clients need to have comfort that their information is going to be properly safeguarded."

Anderson also is a member of the Society for Human Resource Management's Employee Health, Safety & Security Special Expertise Panel, which tackles topics such as risk management, workplace violence, theft and fraud protection, workplace monitoring of email and Internet use, and background investigations. Other members include Orozco and Miller.

Many companies have formed councils that include HR and security leaders along with other business managers, says Howard Schmidt, former White House cybersecurity adviser and president of the Information Security Forum, a nonprofit association of 300 international organizations. These groups go by various names, such as security

**"YOU'RE DEALING WITH TECHNICAL THINGS THAT  
TEND TO BE FAIRLY BLACK AND WHITE.  
AND YOU'RE DEALING WITH THE THE HUMAN  
ISSUES THAT ARE ANYTHING BUT BLACK AND  
WHITE; THEY'RE FULLY GRAY AND SUBJECT  
TO INTERPRETATION." —WINN SCHWARTAU, SCIPP International**

and privacy council or business risk council, but the general goal is to ensure technical policies are fair and consistent with HR requirements, he says.

Still, a lot of enterprises have a long way to go in bringing HR and information security teams together, says SCIPP's Schwartau. He works with many organizations in the finance and government sectors and has seen HR and security often disjointed.

"You're dealing with technical things that tend to be fairly black and white," he says. "And you're dealing with the human issues that are anything but black and white; they're fully gray and subject to interpretation."

But for Orozco, the divide isn't so difficult. "You just have to understand what their concerns are. As an HR person, my concerns have to be the same," she says. "Our jobs are to protect the company. That's what they're doing and that's what I'm doing."

---

*Marcia Savage is features editor of Information Security. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

*Financial*

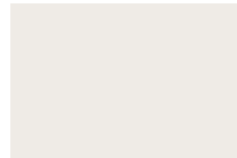


# risk spoken



MARK HOAGARD, CFO, First Capital

# here



## IS YOUR CHIEF FINANCIAL OFFICER YOUR ROLE MODEL?

That may be overstating the case, but increasingly, chief information security officers should have a lot in common with their colleagues in finance. As a 21st century CISO has to be more than a technologist, the outstanding CFO is much more than an elevated CPA.

“The CFO should be someone who has initiative, is well rounded, and who has broad business sense and broad business experience,” says Mark Hogard, CFO of Oklahoma City-based First Capital. “He has to think ahead, think outside the box, and make sure the company is prepared in this ever-changing world.”

Both positions have become even more demanding in today’s compliance-heavy business environment, with unprecedented requirements for data protection, privacy, consumer protection and corporate accountability. Even in the financial services sector where regulatory controls are old hat, the sheer volume of transactions and explosive growth of data has altered the paradigm.

Financial services executives call on a new breed of CISO, who looks to the example of the CFO to implement compliance and security in a risk assessment context, instead of simply firewalls, antivirus and intrusion prevention systems. There are sharp lessons to be learned for security officers from their financial counterparts.

**CFOs live in a world where risk management is the lingua franca. CISOs have to join the conversation.**

BY NEIL ROITER

## WHO ARE YOU?

CISOs have often been outstanding technologists, very adept at identifying and implementing new security products and systems. CFOs, on the other hand, don't regard their positions as being exclusively about numbers.

"The CFO position has always been about business evaluation, and the position has always been a business partner evaluating various business objectives," says Mike Stiglianese, who has the unique perspective of having served in both CFO and chief information technology risk officer roles at Citigroup.

That's where the CISO role needs to be, but typically is not. Much more often than not, the position is in IT, and therein lies much of the problem.

Stiglianese is surprised how few CISOs are like... him.

Now an independent consultant, Stiglianese spent his entire career at Citigroup—25 years on the finance side, including several CFO positions, and the last three as CISO. The things he's encountered outside the CFO chair have opened his eyes.

"The shocking thing was the lack of metrics and

a lack of discipline," he says. For example, he asked one organization how many applications it had, and was told 8,000 to 12,000. Count them, he said.

"They said, 'Everyone calls an application a different thing. I said, 'Let's have a meeting and define something. I'll call it an application and you guys call it whatever you want, but we're going to count how many of those things we have.'"

He says simple program and project management are missing, because information security is overly focused on technology and not on planning. "That type of stuff was the basics that you had on the CFO side."

The CFO sees everything in terms of risk assessment. What are the potential gains and what are the exposures? What is the potential return and how much can we lose if a loan or investment goes south? What will this new technology or this new service cost us and what can we expect in revenues—and when? What controls do we need for regulatory compliance and do they properly mitigate risk to the business?

Because he is grounded in risk assessment and business, the CFO has the ear of upper management—he's one of them—and will be much more receptive to supplicants who "get" business.

The IT-based CISO—especially if he is comfortable there—likely has less insight into the business and will have trouble selling new security programs and technologies to business people who think in terms of risk/reward and cost/benefit.

"If the CISO is a technology person, more often than not, he doesn't have enough gravitas with senior management to get their attention, to make them aware of a business issue," says Eric Holmquist, VP and director of risk management at Advanta Bank.

The CISO can be reduced to trying to sell insurance to executives who are not convinced of the risk.

The CFO understands that he must be able to take his special knowledge, translate it into business terms and communicate effectively to the investor community outside the organization and the board and management within.

"I have the financial information, and I have enough of financial background that I know what makes sense," says Stiglianese. "And, I'm going to make it easier for other people to understand."

At Citigroup, for example, the CFOs have business backgrounds, with "enough financial expertise to know what makes sense." They call on their financial experts to give them the information they need.

In parallel, Stiglianese says that in larger organizations, CISOs are moving into this role as business/risk managers, communicating with business groups and management on their own terms. They have sufficient tech savvy and rely on experts with the technical background.

## Warning signs

**BEFORE TAKING A JOB AS CISO, MAKE SURE THE COMPANY YOU ARE ABOUT TO JOIN IS FLUENT IN RISK MANAGEMENT.**

Eric Holmquist, VP and director of risk management at Advanta Bank, offers three signs that an organization doesn't take risk assessment seriously:

- Information security is positioned as an IT issue, and IT is being asked to manage something it has no control over and isn't a technology issue.
- The tone you hear is "just follow the guidance." You can never set regulatory expectations as your measure of success. That's always the minimum standard. You must exceed that.
- You see anecdotal evidence that people just give lip service to risk assessment, and that sloppy practices are acceptable culturally. If there aren't exceptionally good controls around data in motion, controls of third parties, etc., you have a big problem.

"If there isn't a tone from the top setting information security as a high priority, you're cooked," Holmquist says. ▶



—NEIL ROITER



## COMPLIANCE AND RISK

CFOs have always had to deal with regulatory controls, but not in as public and dramatic a way. The CFO was required to make sure the company was in compliance with GAAP standards, report to various agencies and make sure external auditors would approve financial statements.

But all this happened pretty much behind the scenes, says Stiglianese. Regulations such as SOX have changed the dynamic, drawing intense interest from investors on the outside and the board of directors within. When he started at Citigroup, the regulatory reporting group was under the CFO's office, but "as things have become more highlighted and spotlighted, you bring in a different level of talent to handle the regulatory reporting side."

GLBA created a similar environment for the CISO, but while regulatory change came gradually to the CFO, the CISO was thrust abruptly into the spotlight.

"The CISO," Stiglianese observes, "went from zero to 100 miles per hour instantly."

The upshot is that while CFOs understand the regulatory environment, how it affects the business and how it fits into the risk equation, CISOs are still learning.

"Coming from the financial background, with what we were doing with the compliance function," says Stiglianese, "I saw I was spending a lot of money in areas where I really didn't generate risk, and probably wasn't spending enough to mitigate areas that were riskier."

These are critical considerations. In contrast, there's the CISO, who comes to management with a shopping list of technologies he says they need to comply with PCI or meet the security requirements of SOX, GLBA or HIPAA. The checklist, rather than risk-based, approach will probably pry some dollars loose. However, it won't serve the best interests of the company, which may or may not be technically compliant, and is not significantly more secure than it was before the purchase.

Consider that the intent of these regulatory controls is to protect your company, its customers, its investors and its partners.

"Compliance is about protecting something, some resource, typically," says Dick Mackey, vice president at SystemExperts. "If you fall victim to compromise because your controls aren't good enough, you didn't achieve the goal or intent of the regulation."

The premise is that there is risk here. Address compliance within that context, so that compliance flows from your risk assessments, rather than being

bolted on.

"When you come up with compliance policy that's based on risk, you have to come up with something that works in all cases," says Stiglianese.

That's key to avoid overspending and devoting redundant resources to comply with each regulatory requirement, especially in large organizations, where compliance may become fragmented among various business units.



**"WHEN YOU COME UP WITH A COMPLIANCE POLICY THAT'S BASED ON RISK, YOU HAVE TO COME UP WITH SOMETHING THAT WORKS IN ALL CASES." —MIKE STIGLIANESE, independent consultant**

"One of the first things you realize is that we [financial institutions] are more heavily regulated than most," says Anish Bhimani, managing director for security and risk management at JPMorgan Chase. "So, how do you demonstrate compliance across a number of varying sets of requirements?"

When you build your security program on risk assessment, you are going to protect your company. When you build a program based on compliance, you have, well, compliance.

"We never set the bar for any program based on regulatory expectations," declares Advanta's Holmquist. "I set the bar higher than their expectations. We create as robust a program as we can based on awareness, accountability and the ability to take action. We always exceeded regulators' expectations."

## COMPLIANCE IN THE TRENCHES

Risk is also well understood by regulatory auditors and bank examiners, who are not—and should not be—simply working off a checklist.

"With regulators, I've always found I was able to do things with a risk-based approach," says Stiglianese, "as long as I was able to take them through what my methodology was for evaluating risk."

Depending on whom you talk to, compliance in the financial sector is something of a black and white affair, but that's not to say it's all or nothing. The overriding consideration is the safety of the business—that is to say, is there a real danger that the business could collapse and put customers and other institutions in jeopardy. That's at the heart of many regulatory requirements and a different consideration than the soundness of the business, which speaks more to its level of profitability.

So, while banks should use risk assessment to



**“COMPLIANCE IS BLACK AND WHITE. HOWEVER, THE WAY SOME OF THE REGULATIONS ARE WRITTEN REQUIRES INTERPRETATION BY THE REGULATORY AUTHORITY?”**

—ANISH BHIMANI, JPMorgan Chase

develop programs that meet or, preferably, exceed regulatory requirements, comply they will.

“We follow guidelines laid out for the company,” says First Capital’s Hogard. “Risk assessment determines to what degree of effort and cost does the company expend making sure we’re complying with the regulations.”

Hogard applies the 80-20 rule, achieving 80 percent of compliance quickly at 20 percent of the effort, then implementing more effort-intensive methods to enhance compliance.

The key is presenting a plan that makes sense to examiners/auditors. If your company can’t implement controls immediately, presenting a risk-based, specific plan—with a time frame—will work.

“Generally, it looks something like a 24-month rolling plan,” says Steve Katz, founder and president of IT security consultancy Security Risk Solutions,

who managed information security at JP Morgan, Citigroup and Merrill Lynch. “It gives business managers as well as auditors and examiners a sense that you’re not just trying to solve the immediate problems. If there are open compliances, you have a plan to remediate over time.”

“Compliance is black and white,” says JPMorgan Chase’s Bhimani. “However, the way some of the regulations are written requires interpretation by the regulatory authority.

“SOX 404 is a classic example—it’s maybe 150 words long. Our goal has always been to assume the strictest interpretation unless you hear otherwise.”

## **DOTTED LINES**

The relationship between the CFO and CISO varies from one organization to the next.

For compliance, in larger organizations such as Citigroup, the CFO may rely on the CISO to provide metrics to support internal audit and, in turn, rely on audit to evaluate the security/compliance controls.

In smaller—not to say small—less complex companies, the relationship may be more direct.

“I look to our IT director to help assess if we have the proper controls, and if controls we are thinking of implementing will actually provide the integrity we are looking for,” says First Capital’s Hogard. “We want to make sure that before we invest the dollars our plan will actually be effective.”

Often, the CFO is the one giving thumbs up or thumbs down to the CISO’s spending requests. The CISO will be far more successful if he’s one of the new breed of security officers who’s grounded in the business and risk assessment.

“I was somebody who basically denied investing in a lot of proposals and then spent three years getting the proposals passed,” says Stiglianese.

“The interdependency is more of the CISO on the CFO than the reverse. When I was CFO, as long as I was not having any information security breaches, I didn’t mind if I never saw the CISO come in asking for money.”

Nonetheless, as a CFO he would have been more receptive to funding requests from CISOs, now that he understands their importance.

“The proposals weren’t articulated in a way I could understand. They made no sense to me, so we didn’t make the investment. I learned there’s a need for a more efficient way to communicate between the two functions.”

*Neil Roiter is senior technology editor of Information Security. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*



# Focused on finance?

## Introducing SearchFinancialSecurity.com!

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

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

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

**[www.SearchFinancialSecurity.com](http://www.SearchFinancialSecurity.com)**



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

TechTarget  
Security Media



INFORMATION  
SECURITY

INFORMATION SECURITY DECISIONS







# appropri urgency





MARK WEISCHEDEL  
CIO, American Red Cross

iate

### SHAWN PARTRIDGE CONTINUALLY

nudges his staff and his superiors at Rockford Construction in Grand Rapids, Mich., to view information security—and IT in general—as a means to bring about positive changes for an industry beset by economic woes.

“Until I came here, IT was a support mechanism,” says Partridge, whose company has no CIO. “It was seen as a cost center only.”

Since Partridge, vice president of IT, implemented Web portals to make site management easier, employees “used to running projects with a walkie-talkie and a pad of paper” are not only embracing the new technology but are helping him evangelize the importance of good security habits. “We implement different levels of access” for foremen, customers, and others with a stake in a project, Partridge says.

As threats to corporate data grow, putting organizations’ reputation and revenue on the line, many CIOs and IT executives view information security with appropriate urgency. They’re working to elevate security’s role in the enterprise by teaming up with CISOs or by occupying dual roles—leading both IT and information security efforts.

For its part, the American Red Cross initially created and filled its CISO spot about six years ago, says Mark Weischedel, CIO at the Washington, D.C.-based emergency response organization. Since then, the CISO’s responsibilities have changed substantially.

“In the beginning it was all about policy and strategy,” says Weischedel, who reports to the organization’s CEO. “The CISO position was very highly leveraged, and the capabilities were very limited. Since then, we have added more technical depth, plus we are pushing out more [to the CISO] in terms of [security] policy, compliance, education and awareness.”

He adds that a steady stream of attacks has elevated information security’s importance across the organization. “They are an everyday occurrence, but unless you are immersed [in information security], you won’t understand the risk enough to develop an

**IT executives focus on elevating information security in the enterprise.** BY AMY ROGERS NAZAROV

effective level of controls” with which to respond to them, he says.

Suzanne Hall, named to the CISO post in October, says that the placement of the CISO and CIO within the Red Cross’ hierarchy weighed heavily in her decision to accept the job. She reports to Weischedel.

“Mark and I had conversations about this during the recruitment process,” says Hall, who most recently served as CIO at Lerner Enterprises, a real estate development company based in Rockville, Md., that also owns the Washington Nationals baseball team. “I felt very confident that there was a strong synergy between the CISO and the CIO here, and I know that the CIO has a seat at the table with the CEO.”

The Red Cross has what Weischedel describes as “well-established audit functions” among various groups within the organization, each a check and balance on the other. Among other positions, the Red Cross has a chief of audit, a chief of investigations and an ombudsman—any or all of whom may touch issues related to information security.

Security is so deeply woven into the fabric of the organization that “there is a natural partnership and

affinity between the things our CISO does and the other parts of the Red Cross,” he says.

## AN AFTERTHOUGHT

The Red Cross and other large, established organizations have the breadth and the resources to rearrange responsibilities as business demands and the threat landscape shift. Unfortunately, plenty of other organizations continue to view information security as a technical afterthought. That bias is reflected in how infosecurity managers’ duties are viewed by others within the organization.

In many cases, “we are still seeing IT focused on the primary objectives of the business—delivering services, maintaining network availability,” says Scott Crawford, research director of the security and risk-management practice at Enterprise Management Associates, an IT consulting firm in Boulder, Colo. Security’s role in addressing “risk management is often an afterthought, which is discouraging,” he says.

Crawford, former CISO at the Vienna-based Comprehensive Nuclear Test Ban Treaty Organization, says that rocky relationships between line-of-business personnel and security managers continue in many organizations.

“The business people—and even some in IT—tend to see security staff as being in the business of saying no—‘No, you cannot pursue this line of business because it is too great a security risk,’” says Crawford. Until management takes the view that information security touches the business at every level, clashes are likely to continue, he adds.

## PUSHING SECURITY

In order to persuade others in the C-suite to give appropriate weight to information security, savvy CIOs frequently take pains to work closely with employees outside of IT. Education is of paramount importance in that effort, says Tim Johns, the CIO and head of IT security at Georgia Urology.

“In the clinical environment, change is never a good thing,” says Johns. “A lot of folks have worked here for a long time, so when you come in and say, ‘You need to change your password,’ they say, ‘But I like my password—it’s my daughter’s wedding [date]!’” You have to sell them on the reasons why they need to change their password. You tell them, no, we’re not being attacked, but I am trying to prevent that from happening.

“I like to say that I have 28 bosses,” he adds. Johns reports to the CEO and the managing partner, to say nothing of the two dozen-plus physicians with whom he and his staff work every day. Although he says GU’s CEO thought Johns “went a little overboard” when he expanded GU’s security policy from three

## Missed opportunity

### ORGANIZATIONS CONTINUE TO PUT SECURITY ON THE BACK BURNER AS THEY DIVE INTO VIRTUALIZATION.

The sluggish adoption of security controls in virtualized environments illustrates how security remains an afterthought in many organizations, says Scott Crawford, research director at Enterprise Management Associates.

In an EMA survey of more than 600 enterprises worldwide, only 17 percent of respondents use detective controls to monitor hypervisor security. Just 26 percent use controls to prevent potential or detected hypervisor threats.

“IT has a once-in-a-generation opportunity to integrate security into a new technology in its earliest stages of deployment, yet what this data suggests is that IT—and the business—is missing the opportunity,” Crawford says.

In the absence of significant numbers of proven threats, businesses are still weighing the need to integrate security directly into virtualization initiatives, he says. “Unfortunately, this means that even with new and emerging technology, we may be back to business as usual for dealing with threats after the fact, despite the security lessons so painfully learned over the last decade.”

—MARCIA SAVAGE



# INVENT YOUR FUTURE. Get Certified!



Early Exam Registration Deadline: 11 February 2009

Exam Registration Deadline: 8 April 2009

Exam Date: 13 June 2009

**CISA**  
CERTIFIED INFORMATION SYSTEMS AUDITOR™

**CISM**  
CERTIFIED INFORMATION  
SECURITY MANAGER®

**CGEIT**  
CERTIFIED IN THE GOVERNANCE  
OF ENTERPRISE IT™

Visit [www.isaca.org/infosecmag](http://www.isaca.org/infosecmag).

**ISACA**  
Serving IT Governance Professionals



pages to 37, some explanations about the necessity for HIPAA compliance and other regulations helped the CEO understand precisely why Johns was implementing a host of new procedures and rules.

And just as business people need to elevate security considerations, security people need to prioritize learning about their companies and the type of security risks that could harm them, says the Red Cross' Hall.

"Traditionally, CISOs have not had that business focus," she says. "As a profession, CISOs must work as a group to help build that skills set. It's a model we must continue to develop."

**NEW HEIGHTS**

At retail giant Target, recent changes to top management's responsibilities around security reflect a push to elevate some infosecurity matters to a new level of business criticality.

Over the last couple of years, "we made the decision to treat corporate compliance, fraud prevention and other areas primarily as business risks, then as technical challenges," says Tony Heredia, vice president of corporate risk and responsibility at the Minneapolis-based company.

Target's size and scope drove the changes. Given the array of industries the company straddles—

# 10 top priorities

**EVERY YEAR, THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO) CONDUCTS A SURVEY OF STATE CIOs TO IDENTIFY THEIR TOP POLICY AND TECHNOLOGY ISSUES. HERE ARE THE RESULTS FOR 2009:**

**POLICY**

- 1. Consolidation
- 2. Shared services
- 3. Budget and cost control
- 4. Security
- 5. Electronic records management/digital preservation/e-discovery
- 6. ERP strategy
- 7. Green IT
- 8. Transparency
- 9. Health information technology
- 10. Governance

**TECHNOLOGY**

- 1. Virtualization
- 2. Document/content/email management
- 3. Legacy application modernization and upgrade (ERP)
- 4. Networking, voice and data communications, unified communications
- 5. Web 2.0
- 6. Green IT technologies
- 7. Identity and access management
- 8. Geospatial analysis and geographic information systems
- 9. Business intelligence and analytics apps
- 10. Mobile workforce enablement



**"Security has been a high priority and will continue to be. States are relatively open environments simply because of the nature of their business and it can be problematic!"**

—DOUG ROBINSON, NASCIO executive director



retail, financial services, health care—the company found itself “pulled in recent years in different directions around regulations, from PCI to HIPAA to GLBA,” Heredia says. “We needed to find a way to address all of these risks.”

Thus some issues related to security standards and governance now live in his group’s purview, while Beth Jacob, Target’s CIO and a peer of Target’s general counsel—to whom Heredia reports—continues to oversee the technical aspects of the company’s information security strategies.

As an example, Heredia points to ongoing efforts to shape employees’ security-related behavior, such as educating them about why keeping password-covered sticky notes on or near their computers is a bad idea. While this task had once been handled by those on the technical side of the house, it’s now considered part of standards, governance, training and enforcement, all of which Heredia and his staff ultimately oversee.

In shifting duties around, “we took our time,” he adds, noting that technical and organizational changes designed to address new ways of managing risk have been phased in over the last two years.

## REPORTING STRUCTURE

Given that each organization needs to consider myriad factors—from its size to the regulations it faces to its security or IT head count—Enterprise Management’s Crawford suggests that it’s often best when security personnel report directly to the CEO rather than to the CIO.

“You don’t want to have the person who is supposed to be keeping tabs on doing the right thing reporting to the group they are supposed to be keeping tabs on,” he says.

At Rockford Construction, Partridge reports to the vice president of operations, who reports to the executive VP, who reports to the CEO. He is optimistic that his influence will grow over time.

“Management is still trying to figure out where I really fit into the organization,” he says. “It would be good to have IT and information security in a more strategic, less reactive arrangement.” •

---

*Amy Rogers Nazarov is a freelance writer based in Washington, D.C. She has worked as a staff reporter at several technology magazines. Send comments on this article to [feedback@infosecurymag.com](mailto:feedback@infosecurymag.com).*

*SMB's*



# rising profile



TOM SCHILL, VP of operations, Medio Systems

### YOU'D HAVE A TOUGH TIME

finding the small or medium-sized business that doesn't rely on technology to help it both thrive in good times, and better weather the bad times. And with technologies such as Web 2.0, cloud computing and virtualization emerging, there's an evolution under way that could enable SMBs to compete—to get more done with less, raise productivity, and protect or increase profits.

“Maintaining an up-to-date IT platform is essential for the competitive success of almost every business, and it can serve as an equalizer for small and medium-sized businesses as IT increasingly fuels everything from back-office operations to customer sales and service,” says Chaim Lowenstein, CIO at solutions provider Web Commerce LLC.

Jim Peterson, technology coordinator at Goodnight Memorial Library in Franklin, Ky., agrees, and adds that forging relationships with other senior managers and executives can be key to raising security's profile within the company. “Most small businesses have budget constraints. While the case for security is easy to make, many small-business managers will balk at the price of appliances, servers, software and services,” Peterson says.

Fortunately, there are signs that this type of attitude is starting to change.

A CDW Small Business Driver's Seat Report published in April found data security to be the most pressing interest of SMB executives—coming in as a higher priority than wireless technologies, business intelligence, and even e-commerce and marketing. The survey also found that 47 percent plan to have a formal business continuity/disaster recovery (BC/DR) plan in place within three years. And of those without a dedicated IT worker, 33 percent will create that position in the next three years.

## Security has the attention of SMB execs; the time for facilitating integration is at hand.

BY GEORGE V. HULME

## THE RELATIONSHIP EDGE

That data is welcome news for anyone charged with securing SMB systems. Most SMB managers say getting the ear of management is the key to increasing the security budget, and that starts with forging solid relationships with business unit leaders.

“Relationships with other business units are very important. Those units, if not part of the entire security plan, can undermine any efforts that get put into place. Security is a company effort, and managing the different aspects of security requires that all business units participate and support the security plan,” says Tom Schill, VP of operations at mobile search firm Medio Systems.

Having all aspects of a business carry their weight (or at least not fighting security expenditures) is ideal. But it's not always easy getting there. Most security managers at smaller firms say they try to tackle major security projects one at a time. This may involve first securing the network perimeter, getting BC/DR plans in place, then maybe focusing on Web applications, rather than trying to do too much, too fast.

“I work with each department to build working relationships surrounding the core of security, and communicate how the security measures are woven into the work efforts of each department. I avoid plans that make security a new project, or that involve more time from departmental personnel,” says Schill.

Thus, if a new network segment is going to be built, try to weave the security of that network into the early phases of the budget. The same applies with new wireless networks, Web applications and other initiatives. Most SMB security managers agree that they have a better chance of success that way, rather than trying to get funding after the project already is fully planned and in deployment.

Yet properly managing and securing those applications and their underlying infrastructure isn't easy for the typical SMB. SMBs must operate with tighter budget constraints and fewer staff than their big enterprise competitors. This makes it all the more important for security officers in these businesses to work with managers across the organization.

When it comes to securing their systems, smaller businesses probably won't have a single manager dedicated to shoring up networks and applications, while it's common for big business to have dedicated CISOs, as well as teams of network and application security specialists. Unfortunately, SMBs often are focused on delivering their products and services, or believe they're too small to be targeted by criminals.

“Many SMBs focus on product delivery and have little interest in putting security controls in place. In some instances, they believe they're too small to be affected by a security problem,” says Schill.

In fact, less than one-third of the CDW survey respondents have completed formal BC/DR plans, and only 29 percent employ at least one full-time IT professional. Skimping on relatively small expenses for proper IT management, BC/DR and information security is a risky way to run any business. But smaller businesses in particular cannot afford a single breach or a disaster such as a fire or flood that wipes out the physical offices and data. For the unprepared, any of these events can strike a devastating blow.

## SECURITY MEANS BUSINESS

A new twist on the attitudes toward data security is starting to emerge. Consumers, business customers and partners increasingly care about how well their data is being protected by those with whom they're doing business. In March 2007, a survey by Javelin Strategy & Research revealed a correlation between a consumer's perceptions of a retailer's reputation for protecting credit card information and their willingness to shop with that retailer. A staggering 78 percent of respondents said they'd be unlikely to shop at a retailer following a breach of customers' data.

Despite the risks, many small businesses still are hesitant to invest much into their IT security efforts. “Security concerns are the same for them as they are in larger companies. But putting in the proper security controls, software and processes is difficult if you're working at a business that won't provide the budget,” says Schill.

While it's questionable whether regulatory compliance, for the sake of compliance, actually does much to improve security, there's no doubt that laws such as HIPAA are starting to have an impact on how SMBs must approach security. This is true whether the SMB is regulated directly or not.

And while all companies that process credit card data need to comply with the Payment Card Industry Data Security Standard, many SMBs either outsource the process or don't accept credit card payments at all. However, many SMBs are increasingly finding that their large business partners and customers are asking for verification that proper security controls and BC/DR plans are in place.

Meanwhile, Schill advises that SMB security managers be careful not to push tight security for security's sake: “You have to be personal with [management]. Ask them their needs and feel out their opinions. The more you seem interested in protecting their interests, the more likely they are to help you with yours.”

---

*George V. Hulme is a technology and business journalist based near Minneapolis. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*





## Kick back.

**You just hired an (ISC)<sup>2</sup><sup>®</sup> infosecurity pro who's ready to hit the ground running.**

Even the most knowledgeable hiring manager can't be expected to keep pace with the staffing demands of a field that changes by the second. Fortunately, certified (ISC)<sup>2</sup> professionals are on their toes from day one protecting you from today's vulnerable networked world.

Indeed, (ISC)<sup>2</sup> does the legwork long before a candidate can even get a foot in the door. Our CISSP<sup>®</sup> or SSCP<sup>®</sup> on a resume means that applicant has been reviewed, tested and qualified. And since Continuing Professional Education credits are a pre-requisite to maintaining certification, (ISC)<sup>2</sup> graduates are always a step ahead of the rest.

Your job is to match the professional with the position. Our job is to ensure that you identify the one who can get the job done. So insist only upon candidates with (ISC)<sup>2</sup> Gold Standard credentials. It's an instant leg up over anyone who doesn't.



Before your next hiring decision visit (ISC)<sup>2</sup> for a complimentary hiring guide, whitepaper, case study and other valuable resources at [www.isc2.org/HRCenter](http://www.isc2.org/HRCenter).



SECURITY TRANSCENDS TECHNOLOGY<sup>®</sup>

# 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](http://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

# PRODUCT Reviews

TESTING  
& ANALYSIS  
TO HELP  
YOU MAKE  
PURCHASING  
DECISIONS

## ENDPOINT SECURITY

# Trend Micro Worry-Free Business Security 5.0

REVIEWED BY SANDRA KAY MILLER

### Worry-Free Business Security 5.0

[www.trendmicro.com](http://www.trendmicro.com)

Price: **Starts at \$59.32 per user**  
**(one-year license for 51-250 seats)**



Trend Micro Worry-Free Business Security (WFBS) delivers comprehensive client/server protection for small businesses against a variety of Web threats for Microsoft Windows 2000/XP/Vista, Small

Business Server 2003/2008 and Exchange Server.

### Installation/Configuration **A-**

WFBS was a snap to install, configure and administer, stepping us through the configuration for the Security Server and agents to be deployed on client machines.

Compared to enterprise-class security applications, WFBS didn't require extensive network setting inputs.

The client/server security and remote messaging agents were created equally fast and simply. Client agents can be installed remotely via login scripts or downloaded from an internal or secured website.

The Vulnerability Scanner can scan the network and automatically deploy agents to unprotected systems.

We logged in to the Web Console through a browser connection. An SSL connection to the Security Server is optional, which we thought introduced unnecessary risk.

The Web Console was just about the most uncluttered security product interface we have ever encountered—eight menus are instantly accessible with a single mouse-click.

**Testing methodology:** We tested Worry-Free Business Security on Windows Small Business and Exchange servers connected to a variety of Microsoft Windows endpoints, including desktops and wireless laptops.

### Policy **B**

Policy creation is straightforward. Policies include the usual choices found in antivirus/antispyware, firewall and behavior monitoring applications. There are also settings to secure wireless connections and client privileges. The default scanning policies provide real-time scanning for incoming and outgoing traffic, automatic cleaning for infected files and deletion for malicious code that cannot be otherwise disabled.

### Logging and Reporting **B+**

WFBS can automatically generate a variety of useful reports aimed at IT and management. For instance, we were able to provide statistical analysis of security events for a security administrator as well as content filtering reports, informing managers which employees attempted to visit prohibited websites or send/receive inappropriate email.

The Outbreak Defense menu logged detailed information regarding infections and cleanups. Potential vulnerabilities based upon known threats were also identified. To quickly find a specific event or type of events, WFBS includes a Log Query screen that allows results to be exported to a CSV or text file.

### Effectiveness **A-**

WFBS can be effectively handled by an administrator or small IT department.

The Live Status menu let us view the health of our environment through color-coded buttons for specific threats as well as clients requiring updated agents.

WFBS effectively scanned and protected all of our servers and client machines from a multitude of common threats, including viruses, spyware/adware, spam, infected URLs, phishing and malicious Java and ActiveX applets.

Using only the default settings, WFBS provided adequate security for messaging. The only problems we encountered were with large and compressed files that appeared to hang up the system.

We found the Web Repudiation feature that scans Web pages for malicious code prior to being displayed particularly useful in preventative network and system health.

WFBS also includes a basic firewall, which is adequate for use with mobile laptops.

### Verdict

WFBS is an easy and affordable way for smaller organizations to cover all security bases. •



# PRODUCT Reviews

## WEB APPLICATION SECURITY

# Cenzic Hailstorm Enterprise ARC 5.7

REVIEWED BY PHORAM MEHTA

**Cenzic**

[www.cenzic.com](http://www.cenzic.com)

Price: **\$26,000**



Web application security has moved from a nice-to-have to a must-have requirement, for data protection and compliance. Cenzic's Hailstorm, which we last reviewed in 2005, reflects the growth in the depth and maturity of Web application vulnerability assessment software.

### Installation

**B**

Enterprise ARC includes a management server/console; database for checks, assessments and results; ARC Execution Engine (AEE); distributed scanners that run scans with the Web application to run in different parts of the network and the standalone enterprise desktop scanner.

These components can be installed on one or more machines. The only combination that might be a little tricky is the AEE and desktop software on the same box. In this scenario, you have to stop the AEE service before you can run the desktop client.

Use the desktop application for applications needing some manual interaction and constant monitoring during the assessment, and use AEE for assessments that can be completely automated.

The installation wizard is straightforward and walks you through the various options, including setting the network port and passwords for communicating with the database.

**Testing methodology:** We installed the server, database and desktop client on a Windows 2003 Server and used a Windows XP machine as an execution engine and tested against several Web applications.

### Configuration

**B+**

Hailstorm offers three methods to add applications: Users can run an auto-discovery scan on Web application ports, add applications manually, or import a CSV file. You can assign a risk factor, and group applications for better management. Running and scheduling assessments is as simple as it gets.

The desktop application allows custom assessments that are a combination of checks from best practices (OWASP), regulatory standards, and custom attacks created in-house. We selected the OWASP and best practices assessments against a classic ASP/MS SQL and a Joomla (LAMP) Web application, respectively.

Hailstorm offers by far the best attack customization and new attack creation capability in the industry. To offer flexibility, Cenzic has added features such as interactive assessments, where the user navigates through the website manually.

### Effectiveness

**A**

The two areas enterprises spend the most time on when using a vulnerability scanner are the home page/central display and the results/reports. Cenzic has remarkable interactive dashboard that shows trends and activities.

During the review assessments, we were able to watch the findings and graphs updated as vulnerabilities were discovered. The details on each finding were available instantly, along with the HTTP request/response, complete explanation of how the attack was executed and remediation recommendations.

One feature that sets Hailstorm apart is the Hailstorm Application Risk Metric score, which incorporates the risk factor assigned to each application and the severity of the vulnerabilities discovered. This helps you focus remediation efforts and determine which vulnerabilities present the most risk. It also measures if risk is decreasing and if remediation is effective over time.

### Reporting

**B+**

Reporting is by far the most improved module. The reporting engine is a powerful tool to monitor progress, manage compliance and distribute relevant information in a timely manner. The Crystal Reports viewer can export reports in many formats.

### Verdict

Enterprise ARC 5.7 is a true enterprise-class solution for managing Web application vulnerabilities. •



## DATABASE SECURITY

# Hedgehog Enterprise 2.2

REVIEWED BY JAMES C. FOSTER

Sentriago

[www.sentriago.com](http://www.sentriago.com)

Price: **\$2,400 per database server CPU**



Eight years after the release of Microsoft SQL 2000, we're still looking for help from bolt-on security product vendors to harden and protect critical production database servers. Sentriago's Hedgehog Enterprise 2.2 is designed to monitor and protect against known and unknown database threats.

### Installation/Configuration **A**

The Hedgehog installation was quick and painless. It took approximately 30 minutes to get the basics of a single instance up and running. This included the server, used for centralized management and reporting, and one sensor running on SQL Server 2005.

Agents provide functionality that network-only-based solutions lack. For example, they can monitor and protect against local attacks and malicious use. They also can access server memory for payload inspection; network appliances typically go inline and protect outside the box. You have to deploy agents manually or with a third-party product.

### Management/Monitoring **B**

Hedgehog has a robust yet intuitive Web-based user interface that enables security administrators and engineers to protect databases in a matter of hours. It leverages role-based access permissions at the user and group level.

**Testing methodology:** We tested Sentriago Hedgehog Enterprise 2.2 on a Windows 2003 Server in a lab environment with the product monitoring databases for both active threats and user activity for Microsoft SQL Server 2005.

Within the interface, you can assign permissions by roles. The users assigned to a role then inherit those permissions. There are more than 30 types of granular permissions.

LDAP integration is included by default, to enable you to tie into Microsoft authentication.

Rule creation is about as good as it gets. Provided you understand databases and SQL statements, a four-minute Flash demonstration gives you all the information you need. You can create simple rules to trigger alerts against attacks or suspicious users. In addition, you can create a custom query that is executed on a target database when an associated rule is matched. For instance, if a user is found violating a policy, then you could automatically revoke that user's permissions to a protected database. Other valuable options include terminating that user's session or quarantining him.

Hedgehog comes packed with virtual patching capability, allowing you to prevent known database attacks through a series of identification rules and prevention triggers.

Hedgehog can use a number of output interfaces, such as email, syslog, Windows log file, CSV, Hedgehog internal log file format, and/or its two-way SNMP or XML API engines. These facilities give you a mechanism for collecting or integrating alerts and logs into a SOC, SIEM or log management product.

Three compliance wizards come bundled with 2.2: PCI, SAS 70 and SOX, which walk you through a series of configuration options to meet requirements.

Hedgehog supports Microsoft SQL Server 2000, 2005 and Oracle 8.1.7 or later.

### Reporting **B**

Basic monitoring can be done through built-in dashboards, which have alert filter shortcuts to swiftly check the last 10 minutes, hour, day, week and month.

While the alerts should be monitored in near real time via the dashboards or a third-party product such as ArcSight or HP OpenView, executive and incident reports also add value. Canned reports come in PDF and HTML. Hedgehog's custom report engine allows you to slice and dice any of the data.

### Verdict

You cannot buy a better database security solution for the money. Sentriago's Hedgehog security suite installs quickly and can be leveraged for monitoring real-time external threats and malicious internal user activity. ▶

# PRODUCT Reviews

## IT COMPLIANCE

# GoldKey Secure USB Token

REVIEWED BY JOEL SNYDER

**GoldKey**

[www.goldkey.name](http://www.goldkey.name)

Price: **Starts at \$132 per user token**



The GoldKey Secure USB Token works with Windows and Macintosh operating systems to provide a secure place to stash encryption keys for virtual disks. By keeping encryption keys on a small, removable USB token, GoldKey simplifies the task of locking away important information on laptops and encourages good security behaviors.

GoldKey takes on one of the most difficult tasks in hardware-supplemented encryption by providing a manageable hierarchy of master keys, group encryption keys, and the ability to duplicate tokens.

### Performance

**A**

We had no problems in our tests of GoldKey USB on Windows and Mac laptops. Everything worked as advertised without any problems or bugs.

One of the main concerns about encrypted virtual hard drives is the impact on system performance. We tested a GoldKey encrypted virtual disk against one using the operating system's native encryption system (both Windows XP and Mac OS X), as well as a local laptop drive. On our ThinkPad laptop running

**Testing methodology:** We used MacBook Pro and IBM ThinkPad X61 laptops to test the GoldKey USB key. We encrypted volumes and used them for day-to-day operations for a week. In addition, we used simple benchmark tools to compare performance of GoldKey USB, native O/S hard drive and native encrypted file systems.

Windows, the GoldKey disk was about 50 percent faster than a drive encrypted using Windows tools, and about the same speed as the local 7200 rpm laptop drive. On a MacBook Pro, GoldKey was 75 percent faster than the native OS X encryption, although about 60 percent slower than the local 7200 rpm laptop drive. Windows users should see little performance impact in modern laptops.

### Management

**B+**

One of GoldKey's unique features is the ability to use group encryption keys as well as personal encryption keys. A virtual disk may be encrypted by one member of a team, with full access by other members in the same group. GoldKey provides a basic management tool that makes management of groups and group memberships easy.

GoldKey also supports master and grand master keys, as well as the ability to duplicate tokens. Together, these tools help eliminate one of the greatest fears of encrypted data: permanently losing the key. While GoldKey's mechanisms won't scale up to a Global 100 enterprise and don't integrate with the corporate directory, they are easy to use and simple enough for fairly large deployments.

However, be aware that GoldKey doesn't have any online magic to access controls. You can't remotely revoke privileges to read or write a volume from someone, and if someone loses an encrypted volume and token, and writes down the password to the token, whoever finds all three will have full access to the volume. GoldKey doesn't protect you against rogue employees, just forgetful ones.

### Other Security Functions

**C**

While testing GoldKey, we kept hoping it would do more than it does—but it doesn't. Features such as auto-lock of laptop and encrypted drives when the token is removed are present, but they can't be centrally controlled or locked. Other common features, such as automatic timeout to require reauthentication, aren't available. While you can email around GoldKey-encrypted volumes, there is no real integration with any application other than the file system.

### Verdict

While GoldKey is far from a do-everything desktop security solution, it handles the problem of key management for encrypted volumes very well. ▶

## Sour Note on Endpoint Suites

Tests suggest AV products need more than a little tuning.

Antimalware vendors are loading up—with traditional signature-based detection, heuristic detection, detection based on common attack characteristics and exploits of known vulnerabilities, application controls, host firewall...whew!

But how well is all this working? Recent tests from a couple of sources—Virus Bulletin (VB) and Secunia—didn't have all the answers, but the findings were interesting enough to make us wonder, yet again, how effective are these products and how do you test that effectiveness.

The annual VB100 certification test—which has been around since 1998—didn't tell us much except that AV vendors can shoot fish in a barrel—in this case, a WildList virus sampling they surely all have signatures for. But other test results, detailed in the October Bulletin, detecting bots and worms, polymorphic viruses and especially Trojans, were more revealing. While all the major vendors scored perfectly on the VB100 test, they missed 5 to 15 percent on the Trojans test.

The reason? First, this was a fresh batch of specimens, so the products had to depend on their other detection techniques, with disappointing results. John Hawes, VB technical consultant, says the Bulletin is moving rapidly to ensure fresh samples for each evaluation—bots and worms as well—to test the mettle of these endpoint security suites. And, Trojans are a particular challenge.

“Trojans are difficult because there are so many of them; 90 to 95 percent of new malware reported are Trojans,” he says. “Huge, huge numbers of malware are coming out all the time, and keeping on top of it is quite a tricky task.”

Secunia's Internet Security Suite test was designed to test a dozen products' ability to detect exploits. Secunia turned 144 malicious files and 156 malicious Web pages against XP SP2 with missing patches and a number of vulnerable programs. The results were dismal. Symantec was tops with 64 hits. The rest? Look at your hand. Count the fingers.

“For a long time, I've viewed signature-based detection as a commodity,” says Ed Skoudis, co-founder and senior security consultant of Intelguardians. “The other stuff is where all the interesting detection happens, especially as signature-based detection grows less effective over time because the bad guys are moving so fast.”

A case in point was this year's Defcon Race to Zero, in which a team of three researchers from Mandiant used obfuscation techniques to get 10 well-known viruses and exploits—including Slammer and the 20-year-old Stoned virus—past major AV scanners. It took them six hours.

Secunia CTO Thomas Kristensen thinks things might be even worse if the bad guys tried harder.

“What makes people lucky is that the bad guys still have quite a bit to learn,” he says. “They are not that good at exploiting the latest vulnerabilities on a massive scale. If their attempts to exploit are caught, it's simply because they're using some old payload that is already known by the different security solutions.”

The bottom line? Security suites are essential, but don't get lulled by vendor claims, especially when it comes to zero-day exploits. A combination of good software, up-to-date patches and user education mitigates the problem, but there is no solution. ▶

Neil Roiter is senior technology editor of Information Security. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).

## Unified Email Management

Mimecast

[www.mimecast.com](http://www.mimecast.com)

Price: **Varies by company size; \$5/seat per month for 5,000 seats**

Email security has become a complex affair. Spam continues to grow as an operational issue, and email-borne malware and phishing attacks persist. Archiving requirements, legal discovery rules, data loss prevention and the sheer volume of messages have created a management monster.

Mimecast offers a multifaceted SaaS package as demand for email services grows and the vendor landscape consolidates. Most of the major players have been acquired: FrontBridge (Microsoft), Postini (Google) and, most recently, MessageLabs (Symantec), leaving independent MX Logic. Mimecast is banking on offering what it says is the most comprehensive service package, including antispam, antivirus, archiving and storage management, e-discovery and data loss prevention. The pitch is one service instead of point solutions.

“There are no tradeoffs in terms of control,” says Peter Bauer, Mimecast chief executive. “Customers use the service as if they are the only users. We incorporate important enterprise features, such as Active Directory integration and sophisticated audit logging.”

Email services have growing appeal. Regulatory requirements are driving archiving in the face of increasing volume. Revised FRCP rules put pressure on organizations to perform complete, fast e-discovery—at astronomical costs.

Mimecast also promises business continuity; if a customer's Exchange Server goes down, end users can still receive email from Mimecast.

Mimecast entered the North American market in February. It faces stiff competition in services, given Microsoft's and Symantec's muscle and Google's aggressive pricing packages. ▶

—NEIL ROITER

**SR. VICE PRESIDENT AND GROUP PUBLISHER**  
Andrew Briney

**PUBLISHER**  
Jillian Coffin

**DIRECTOR OF PRODUCT MANAGEMENT**  
Susan Shaver

**DIRECTOR OF MARKETING**  
Kristin Hadley

**SALES DIRECTOR, EAST**  
Zemira DelVecchio

**SALES DIRECTOR, WEST**  
Dara Such

**CIRCULATION MANAGER**  
Kate Sullivan

**PRODUCTION MANAGER**  
Patricia Volpe

**PRODUCT MANAGEMENT & MARKETING**  
Corey Strader, Jennifer Labelle

**Sales Representatives**

- Eric Belcher ebelcher@techtargtarget.com
- Neil Dhanowa ndhanowa@techtargtarget.com
- Patrick Eichmann peichmann@techtargtarget.com
- Suzanne Jackson sjackson@techtargtarget.com
- Meghan Kampa mkampa@techtargtarget.com
- Jeff Tonello jtonello@techtargtarget.com
- Nikki Wise nwise@techtargtarget.com

**TechTarget Inc.**

- CHIEF EXECUTIVE OFFICER** Greg Strakosch
- PRESIDENT** Don Hawk
- EXECUTIVE VICE PRESIDENT** Kevin Beam
- CHIEF FINANCIAL OFFICER** Eric Sockol
- PUBLISHER, CHANNEL** Doug Olender

**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

**Subscription Customer Service**

*Information Security*  
610 Academy Drive, Northbrook, IL 60062  
Phone: 888-804-5501  
<http://subhelp.infosecmag.com>

*Information Security* (ISSN 1096-8903) is published monthly with a combined July/August, December/January issue by TechTarget, 117 Kendrick St., Ste. 800, Needham, MA 02494 U.S.A.; phone 781-657-1000; fax 781-657-1100. All rights reserved. Entire contents, Copyright © 2009 TechTarget. No part of this publication may be transmitted or reproduced in any form, or by any means without permission in writing from the publisher.

# ADVERTISING INDEX

ADVERTISER	PAGE
ISACA ..... www.isaca.org	39
(ISC) <sup>2</sup> ..... www.isc2.org	45
Nokia ..... www.nokia.com	17
RSA Conference ..... www.rsaconference.com	53
SearchFinancialSecurity.com ..... www.SearchFinancialSecurity.com	35
SearchSecurity.com ..... www.SearchSecurity.com/join	23
SystemExperts ..... www.systemexperts.com	46
Trend Micro ..... www.trendmicro.com	27
VeriSign ..... www.verisign.com	19



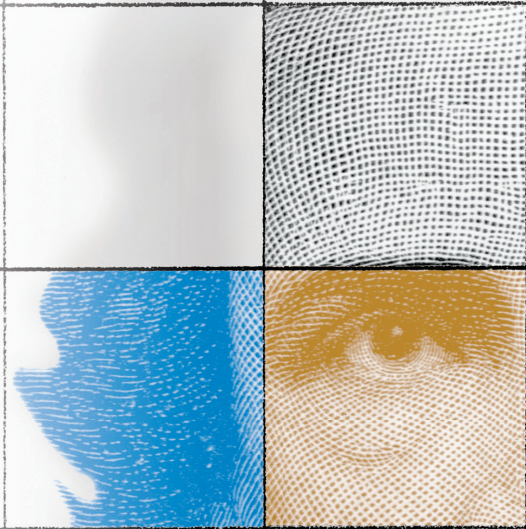
# RSACONFERENCE

WHERE THE WORLD **TALKS SECURITY**

Do more than  
keep pace.  
Set it.

In a security environment where every day brings new challenges, staying ahead isn't just an option, it's mandatory. As the information security event of the year, RSA® Conference 2009 is your opportunity to engage with the greatest minds in technology. You'll focus on critical issues and formulate strategies to create solutions that will influence the industry now and in the future. And you can do it all at RSA Conference 2009.

- Learn the latest trends at over 240 targeted sessions
- Discover practical solutions from 500+ speakers
- Get the tools for success from over 350 exhibitors



## REGISTER

APRIL 20–24, 2009 | MOSCONE CENTER | SAN FRANCISCO  
[WWW.RSACONFERENCE.COM/2009/US](http://WWW.RSACONFERENCE.COM/2009/US)  
ENTER PRIORITY CODE: IS128

**How do you think the economic downturn will affect security budgets?** It's always been a real chore to justify an information security budget because you can't put a monetary figure on the return on the investment. Information security is there to make sure nothing [bad] happens, so if you're doing your job, nothing [bad] is happening. Given that you're already starting behind the eight ball, the economic upheaval in the banking industry is just going to put more of a burden on security professionals to get more funding. They'll have to learn how to live with less. Take good stock of your resources, the skill sets of your team, your networking infrastructure and see what you can do within the limited budget that you'll be getting.

**Can outsourcing help?** It's certainly part of the picture. Going from JPMorgan to Republic First Bank—from a very large international corporation that had a large budget for security to a smaller regional bank that doesn't have the [same] resources—gave me good insight on how to manage and do more with less. If you're a small or midsized bank, you might not have the resources to have an ethical hacking team like I had at JPMorgan, or you can't afford some of the more expensive tools. So you have to rely on vendors to perform some of these services. Typically, we have vendors performing our vulnerability assessments and penetration testing.

**What else might help in lean times?** There are things you can do with a small team or a small budget. It's going back to basics. One of my main focuses when I come into a security position is to get a really detailed understanding of the flow of confidential and restricted data. You have to know where your data is going and who it's going to; once you know and understand that, you can start targeting areas of risk. You need to have a mature risk assessment process in place so you can prioritize these risk areas. Once you prioritize the risks associated with the various areas, you can start focusing your limited resources—whether it's budget, assets or staffing—on those areas. You probably won't cover every single one, but at least you've hit all the high-risk areas. ▶

Today's economic climate may mean belt tightening for many security officers, but Anthony Meholic already learned how to do more with less when he joined Republic First Bank after working at global powerhouse JPMorgan Chase. The senior vice president and information security officer at the bank, which serves the greater Philadelphia area, knows what it takes to protect corporate assets in a tough economy.

# ANTHONY MEHOLIC