PLUS: PRIORITIES 2009 | SCHNEIER VERSUS RANUM

INFORMATION SECURITY®

FEBRUARY 2009

BUDGET SQUEEZE

HOW TO MAINTAIN SECURITY DURING A RECESSION

10 LOW-COST WAYS TO IMPROVE YOUR THREAT MANAGEMENT POSTURE

5 TIPS ON HOW TO STRETCH YOUR BUDGET

TechTarget
The IT Media ROI Experts

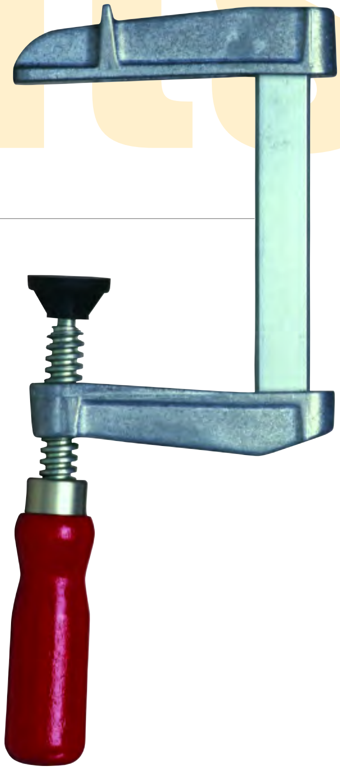
INFOSECURITYMAG.COM

contents

FEBRUARY 2009

VOLUME 11 NUMBER 2

FEATURES



ALSO

Security on a Shoestring Budget

BY KELLEY DAMORE

WHILE WE'RE ALL happy to see 2008 behind us, 2009 could be as challenging as 2008. The new Obama Administration has brought optimism, but businesses have yet to be rewarded with a stable stock market. Intel, for its part, announced layoffs as did Microsoft—the first time in its 30-plus year history. As a result, we are still on shaky, shaky ground.

I think it would be safe to say that everyone is going through the exercise of belt tightening: Where can I cut costs? Do I need to make that purchase or do I simply want that item? The same holds true for security professionals. Budgets are being scrutinized and return on investment is being demanded. So, this month's issue is all about getting by on a shoestring budget and comparing yourself to your peers in terms of priorities for the year.

In our "Under Pressure" article *(see p. 21)*, Features Editor Marcia Savage dissects our annual *Information Security* 2009 Priorities survey. Data protection and threat management top the list of priorities. Specifically encryption of all sorts is of keen interest to readers. Regulations and industry mandates are fueling the interest. PCI DSS requires encryption and new state laws from Nevada and Massachusetts are forcing organizations to take a more proactive data protection approach. *(See "Raising the Bar," p. 4)*.

In our "Troubled Times" story *(see p. 13)*, Editor Michael Mimoso talks to security pros on the challenges of securing an organization in a recession and offer five ways to stretch your budget. Meanwhile, technical editor David Strom offer 10 tips that can help an organization get the most out of its current threat management infrastructure in order to save dollars and manpower. *(See p. 29)*.

Certainly the stakes are raised during tough times. The bad guys see an opening as employees get more frustrated and disgruntled. Add to the mix new technologies and a new generation entering the workforce that demand 24/7 access. How should you think about Web 2.0/social networking technologies? Bruce Schneier and Marcus Ranum argue the point in their Face-Off column. *(See p. 9)* .

While going through a recession is painful, it does give us all a good dose of perspective and appreciation. And hopefully with new regulations on the horizon, security pros will get more dollars and justification for security expenditures for the years to come.

We don't know when this recession will end, but some prognosticate that we are already half-way through it. And if there is a silver lining in all of this mess, it is that this recession will in fact end and we will be stronger and smarter because of it.

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

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

VIEWPOINT

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

Recession and Respect, Right On

INFORMATION SECURITY
THINK TANK
CARNEGIE MELLON'S CYLAB
BLAZES NEW TRAILS IN BIOMETRICS, INSIDER THREATS, KEY EXCHANGE & VIRTUALIZATION

In "Maintaining Security in a Recession" (November 2008) Kelley Damore is so right. Security is even more important in a recession because of increased danger of crimes by trusted persons when faced with increasing personal problems during recessionary times.

Unfortunately, security has been paid for with discretionary money, and that dries up during recessions.

In my experience many security people lost their jobs in the 1980, 1990, and 2000 recessions. However, this time around it may not be so bad because of the institutionalizing of security in the law making security mandatory, not discretionary.

We must concentrate on compliance and enablement as drivers of security rather than risk reduction that is not measurable nor manageable anyway.

And also, Jay G. Heiser is correct in his Layer 8 article, "No Respect" (November 2008). The special knowledge possessed by our information security tech nologists must find its way into the development of critical systems if we are ever to have a reasonably secure infrastructure. Our security technologists must be assigned as specialty participants in software development teams.

The way to do this is to make an engineering discipline on the technical side of security out of what is now just a folk art. We must concentrate more on technological excellence and diligence rather than voodoo risk reduction.

–DONN PARKER, CISSP (retired)

'No Respect,' No Way

I took a long time to respond to "No Respect," by Jay G. Heiser (November 2008), and now I am sure I disagree with it strongly, for a long list of reasons.

I don't know how many other people took the time to read this article, but it doesn't belong in *Information Security*. At first I thought the writer was simply campaigning for security professionals—that security is serious business and security professionals don't get enough respect.

But then it seemed to read like another "Everyone is stupid…except for me" article.

Now I realize it is something far worse than that. This thinking is totally corrupt and so seriously flawed it worries me the damage it can actually do. I hope no one else read it.

–STEVE SARAKAS, Callplex, Inc.

COMING IN MARCH

MUST READ!

CHOOSING A WEB APPLICATION FIREWALL

Enterprises rushing to meet PCI compliance requirements may find themselves in a quandary when it comes to choosing a WAF. We'll cover the factors you need to consider when investing in a WAF–from choosing the appropriate form factor to integration and management requirements.

SECURING MIDMARKET COMPANIES

Companies with 100-1000 employees don't have dedicated security staffs, yet have many of the same concerns and federal regulations of their larger brethren. We'll offer strategies for threat management and network security and how to leverage additional features in their existing infrastructure.

DEVELOPING POLICIES FOR WEB 2.0

Recent attacks on Twitter have thrust into the spotlight the risks of social networking for enterprise and midmarket companies.

We'll explore the risks associated with social networking sites and how you can develop policies that suit your organization's needs.

CLOUD COMPUTING RISKS

Internet-based IT services pose attractive economies of scale and efficiencies, but there are risks including loss of control of essential data, privacy implications and reliance on the security of a provider's infrastructure. We'll look at the security implications and what you need to consider when moving to the cloud.

Raising the Bar

Tough new data protection laws in Massachusetts and Nevada up the ante for security. BY JULIE TOWER-PIERCE

THERE'S ALWAYS BEEN a premium on data protection, but a paradigm shift away from reactive laws toward more proactive and uniform breach-prevention frameworks may up the ante for information security practitioners who can expect a lot of heavy compliance lifting this year.

Hardcore data protection laws in Nevada, as of last October, and coming May 1 in Massachusetts, have changed the information security game for everyone. They've mandated prevention; shifting the focus from data-breach notification, though not eliminating that concern, to breach prevention by way of mandatory encryption. When it comes to data handling and data control, encryption is now front and center. The undertone is that data containment is how the game will be won, and encryption is the approach chosen by these states to achieve containment.

When it comes to data handling and data control, encryption is now front and center.

But even more significant than what these laws read, is what they will do. Requiring businesses to encrypt transmitted personal data (and under the Massachusetts regulations, the encryption of personal information stored on portable devices or laptops) raises the bar for security and technology practitioners, as does Massachusetts' new requirement for "comprehensive, written information security programs" to protect records containing personal information.

Effectively, these laws create a new baseline for practitioners who are intimately involved with regulatory compliance and transmission of personal data, regardless of where they do business. Lawyers spend months hashing out the meaning of any new law, and the extent of a law's applicability to a business. Information security practitioners don't have the luxury of time, especially where effective data control, risk management, and compliance are sought after. Practitioners must act now, starting by making a case to management about what needs to be done, including what resources and tools are needed, for containment.

Beyond the courtroom and corporate counsel offices, the real-world practical effect of these two laws is that companies should begin encrypting data in situations where they have already decided (deliberately or by default) that there is no business case for encryption. Information security professionals interested in being seen as strategists will approach this problem by finding a way to roll the regulatory requirement for encryption into existing corporate policies and procedures, such that the practice of encryption is a tightly integrated practice rather than a regulatory add-on.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

Meeting the new bar may involve uncomfortable expense, particularly for smaller businesses with small security budgets. However, a focus on data breach prevention and data containment is the right approach (even if government mandated) and will only gain more regulatory traction as we move into 2009. The emphasis on prevention will serve long-term corporate interests by reducing costs due to breach remediation, public relations clean up, and business distraction caused by sensitive data disclosure.

In the end though, it's a near certainty that data breaches are going to happen. Comprehensive corporate policy, that carefully contemplates major currents in the law and reflects a strategic mindset, will go a long way toward minimizing those risks and put companies in the best posture to address the fallout. ▸

Julie Tower-Pierce, Esq., in an attorney, past professor of cybercrime and cyberlaw, and author. She is admitted to practice in Vermont and the District of Columbia. Send comments on this column to feedback@infosecuritymag.com.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

Analysis | HEARTLAND PAYMENT SYSTEMS

The Breach of All Breaches?

Heartland is calling for changes on the scale of Johnson & Johnson's Tylenol recall but experts say constant vigilance is the only defense.

BY ROBERT WESTERVELT

WHEN HEARTLAND PAYMENT SYSTEMS announced a data security breach on Inauguration Day, the collective groan from security professionals could be heard around the world.

Heartland, one of the country's largest payment processors, had achieved PCI compliance. Yet the breach could be the largest ever, trumping that of TJX Cos. when 45 million credit and debit cards were pilfered by hackers who accessed the retailer's Wi-Fi systems.

How can a payment processor—whose primary business is to securely and efficiently process billions of transactions annually—fail in such a colossal way? The Heartland breach details are scarce, but the early lesson seems to be that you can't rest on your laurels, even once you've achieved compliance. No matter how hardened your systems are, a determined person with the right skills can, and will, find a way in.

A recent Ponemon Institute survey of 43 businesses that had experienced a data breach found that 84% involved organizations that had more than one major breach. More than 88% of all cases involved insider negligence.

"It's impossible to create an environment where you cannot have a data breach," said Larry Ponemon, founder and chairman of the Ponemon Institute. "Data breaches will probably continue even for the best of companies, but it's how you detect it, how you respond to it and how you manage the risk that matters most."

Heartland founder and CEO Robert O. Carr responded to his company's breach by calling for sweeping changes in the industry with encryption technologies. He likened the breach to that of Johnson & Johnson's massive Tylenol recall in 1982 after seven people died taking cyanide-laced Tylenol Extra-Strength capsules. As a result, Johnson & Johnson produced new safety seal packaging that would set the standard for the rest of the industry.

Carr is calling for end-to-end encryption, from the time a consumer swipes their credit card to the payment processor's systems.

"There is no single silver bullet that will secure payment systems, and constant vigilance and monitoring of the infrastructure will always be required," Carr said in a statement. "Nevertheless, I believe the development and deployment of end-to-end encryption will provide us the ability to implement increasing levels of security protection as they become needed."

The fact is, even encryption can lull businesses into a false sense of security, said Phillip Dunkelberger, president and CEO of encryption vendor PGP Corp. Encrypted data has to be unencrypted in order to be accessed. Technologies are available to secure sensitive data in motion, but once it arrives at its destination, he said, the data arrives in a clear form.

"Businesses have to understand how data moves through the company systems to understand how to protect it from internal and external threats," Dunkelberger said. "Many haven't reached that level of understanding yet."

"Malware detection is really critical so you don't have Trojans there when you deencrypt it," he said.

The payment processing industry is under constant bombardment from attacks, said Henry Helgeson CEO of Boston-based payment processor, Merchant Warehouse. The processor handles about 3 million transactions a month and $3.5 billion in transactions annually. Like many processors, Merchant Warehouse has a compliance officer whose job is to maintain the company's PCI compliance.

"I think the 12 bullet points in PCI are good to follow, but I don't think you should necessarily stop when you get through those 12 points," Helgeson said. "It's really scary that this happened to Heartland. Hopefully we'll get some details on this that says Heartland made a mistake and this isn't something that we're all vulnerable to."

> "I think the 12 bullet points in PCI are good to follow, but I don't think you should necessarily stop when you get through those 12 points."
>
> —HENRY HELGESON, CEO, Merchant Warehouse

Does the industry need to do something on the level of Johnson & Johnson's safety seal packaging to protect sensitive data? Ponemon doesn't think so. PCI lays out the fundamentals every organization must use to have the best defenses. Vigilance is the most important factor.

"The only way to do this right is a combination of good technology solutions and generally smart people who are educated and trained appropriately," Ponemon said. "You solve this problem by training people and giving them the tools to secure their data."

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

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

2009: Off on the Wrong Foot

DURING THE PAST MONTH we're seen both Monster.com and Heartland Payment Systems *(see story, p. 6)* announce they have been compromised with more than 100 million records possibly breached. Oracle released its quarterly patches while the Microsoft RPC worm, known by many as Conficker/Downadup, has multiplied across corporate networks infecting an estimated 10 million machines. While damage has been minimal, the worst is could be to come.

—*Information Security* staff

41

Number of security fixes Oracle released as part of its quarterly Critical Patch update

The decrease in spam in 2008; Attacks on social networks and flaws in web sites are rising however

3.4%

SOURCE: Symantec's MessageLabs Institutions

250,000

Number of businesses that use Heartland Payment Systems to process payroll and credit card payments

$1,600,000

Expenses incurred by banks affected by Hannaford breach

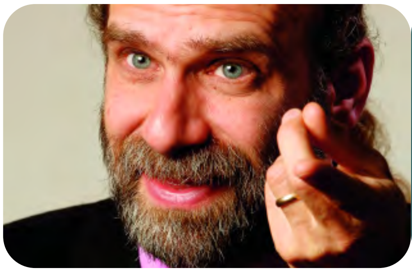
SOURCE: Maine Bureau of Financial Institutions

OVER-HEARD

> **We'll continue to witness the rise of managed service providers…amid pressure to minimize headcount. If you're not using one of these services, put it on your short-term radar.**
>
> –MIKE CHAPPLE, University of Notre Dame

FACE-OFF

SECURITY EXPERTS **BRUCE SCHNEIER & MARCUS RANUM** OFFER THEIR OPPOSING POINTS OF VIEW



Should companies be concerned about employees' social networking?

POINT *by* BRUCE SCHNEIER

ARE EMPLOYEES BLOGGING corporate secrets? It's not an unreasonable fear, actually. People have always talked about work to their friends. It's human nature for people to talk about what's going on in their lives, and work is a lot of most people's lives. Historically, organizations generally didn't care very much. The conversations were intimate and ephemeral, so the risk was small. Unless you worked for the military with actual national secrets, no one worried about it very much.

What has changed is the nature of how we interact with our friends. We talk about our lives on our blogs, on social networking sites such as Facebook and Twitter, and on message boards pertaining to the work we're doing. What was once intimate and ephemeral is now available to the whole world, indexed by Google, and archived for posterity. A good open-source intelligence gatherer can learn a lot about what a company is doing by monitoring its employees' online activities. It's no wonder some organizations are nervous.

So yes, organizations should be concerned about employees leaking corporate secrets on social networking sites. And, as much as I hate to admit it, disciplinary action against employees who reveal too much in public is probably in order. But actually policing employees is almost certainly more expensive and more trouble than it's worth. And when an organization catches an employee being a bit too chatty about work details, it should be as forgiving as possible.

> "As much as I hate to admit it, disciplinary action against employees who reveal too much in public is probably in order."
>
> —BRUCE SCHNEIER

That's because this sort of openness is the future of work, and the organizations that get used to it or—even better—embrace it, are going to do better in the long run than organizations that futilely try to fight it.

The Internet is the greatest generation gap since rock and roll, and what we're seeing here is one particular skirmish across that gap. (For a better understanding of the nature of the generation gap, I strongly recommend this article: http://nymag.com/news/features/27341/). The younger generation, used to spending a lot of its life in public, clashes with an older generation in charge of a corporate culture that presumes a greater degree of discretion and greater level of control.

There are two things that are always true about generation gaps. The first is that the elder generation is always right about the problems that will result from whatever new/different/bad thing the younger generation is doing. And the second is that the younger

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

generation is always right that whatever they're doing will become the new normal. These things have to be true; the older generation understands the problems better, but they're the ones who fade away and die.

Living an increasingly public life on social networking sites is the new normal. More corporate—and government—transparency is becoming the new normal. CEOs who blog aren't yet the new normal, but will be eventually. And then what will corporate secrecy look like? Organizations will still have secrets, of course, but they will be more public and more open about what they're doing and what they're thinking of doing. It'll be different than it is now, but it most likely won't be any worse.

Today isn't that day yet, which is why it's still proper for organizations to worry about loose fingers uploading corporate secrets. But the sooner an organization can adapt to this new normal and figure out how to be successful within it, the better it will survive these transitions. In the near term, it will be more likely to attract the next-generation talent it needs to figure out how to thrive. In the long term...well, we don't know what it will mean yet.

Same with blocking those sites; yes, they're enormous time-wasters. But if an organization has a problem with employee productivity, they're not going to solve it by censoring Internet access. Focus on the actual problem, and don't waste time on the particulars of how the problem manifests itself.›

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.*

COUNTERPOINT *by* MARCUS RANUM

IT SEEMS TO me that everyone rushes to blame the new-whatever for problems that they should have already known about and understood for a long time. Keeping information confidential or secret has always been difficult, and I really doubt new technology changes the situation a great deal. It seems less a matter of worrying about employees blogging secrets than simply having stupid employees. My experience is that a stupid employee is a curse that keeps hurting an organization vastly out of proportion to any other contribution he or she might make. There's probably nothing new or different about that, either.

Whenever I hear someone complaining about how difficult it is to keep information from leaking, I immediately think about the secrecy Apple has managed to maintain surrounding some of the devices it has produced. Clearly, it's possible to build a complex piece of electronics, with contractual relationships and sourcing arrangements all over the world, and not have the design be leaked months ahead of time. So my suspicion, when people are complaining about information leakage, is simply that they haven't taken it seriously and are complaining about the horse having left an unlocked barn. That's an extremely common practice in corporations; sure, it's reasonable to blame the employee who blurted out a secret on his blog—but ultimately I see these problems as symptomatic of poor management and bad hiring choices more than anything else.

In other columns, I've criticized security training as largely ineffective, but this is one place where establishing an organizational culture of security really is critical. How is it that the people who are

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

designing and building iPods can keep a secret, while researchers at labs such as Los Alamos can e-mail design information about nuclear weapons in the clear. It's a matter of having a shared sense of purpose and, perhaps, technological support where necessary.

Mostly, though, it's not a technical problem— management has to, as it were, manage people. Too much of the time, managers are behind the technology power curve and abrogate their responsibility to understand what employees are doing. I worked at one company where, out of curiosity, I checked firewall logs and discovered that about 20 percent of the engineering staff was spending 90 percent of its time arguing on Slashdot. Never mind information leakage— that's just plain dysfunction.

I don't know how much industrial espionage actually goes on, but it seems as if the traditional methods are effective: if you want to know what your competitors are doing, talk to their customers, hire people who used to work for them, or get advance copies of product literature from their resellers and business partners. I've been involved in a couple of situations where I worked for one security company, and would get résumés from people who worked at our closest competitor.

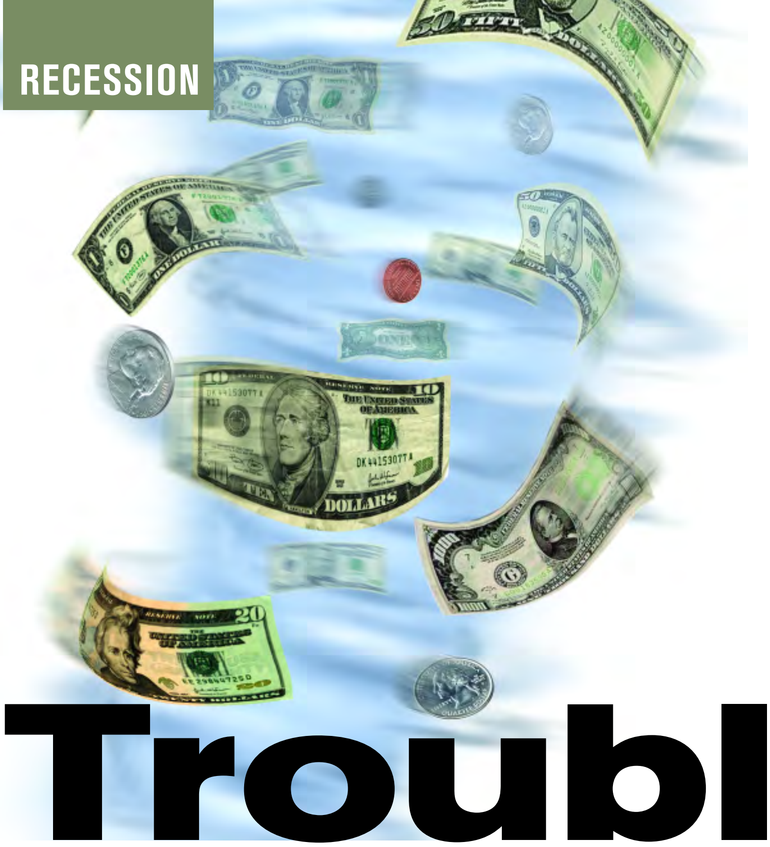
Employees are going to think about a competitor as a possible place to work simply because they have experience in that market or technology, and the experience might translate into a decent position. If someone were trying to deliberately spy on a target, would it really be worth all the bother of wading through MySpace pages and collating résumés? I'd bet that hiring an ex-employee would be a whole lot simpler. Admittedly, I am biased: the sheer amount of banner ads and goofy marketing on social networking sites makes them unbearably slow and noisy. Trying to learn anything useful from them would painful—extremely so.

> "It seems less a matter of worrying about employees blogging secrets than simply having stupid employees."
>
> —MARCUS RANUM

I really have to disagree with you about CEOs blogging useful stuff and that "open" is becoming the new way of doing business. That's all just marketing crud; I have yet to see a CEO give away anything interesting in a blog that wasn't carefully choreographed (and I suspect most CEO blogs are actually written by someone in the marketing department). While "open" is the big deal right now, I think it's largely just appearance. Our theoretical modern industrial spy would have to wade through press releases masquerading as blog entries, as well as "here are 400 pictures of me and my puppy" on blogging sites.

Sure, information leakage is a problem, but it makes more sense to be worried about information being targeted and pulled than it does information being posted by employees.

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.



Troubled Times

In a difficult economy, security pros must measure risk and prioritize projects.

BY MICHAEL S. MIMOSO

GRIMLY AND ANTICLIMACTICALLY, the National Bureau of Economic Research made it official on Dec. 1 that the United States economy had been in a recession for more than a year. The projections for when the wounded dollar would be able to right itself weren't much better, with experts forecasting a continued downturn throughout this year with slight recovery starting in 2010.

Few markets are immune to a recession, yet information security seems somewhat armored against economic troubles. Why? Compliance requirements don't deflate in a recession. Hackers don't lower their swords in a recession. Laid off insiders aren't less disgruntled in a recession. And integration woes brought on by endless mergers aren't lessened in a recession.

But information security isn't completely recession proof. CISOs are facing flat budgets (or ever-so-slight increases) and non-essential projects and upgrades are being delayed almost across the board. Smart CISOs will be forced to vigilantly measure risk in order to strategically prioritize projects, decide which new projects should be funded or delayed and which functions to outsource.

CISOs have to walk a narrow tightrope this year, unsure whether economic recovery or deeper cuts await on the other side.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

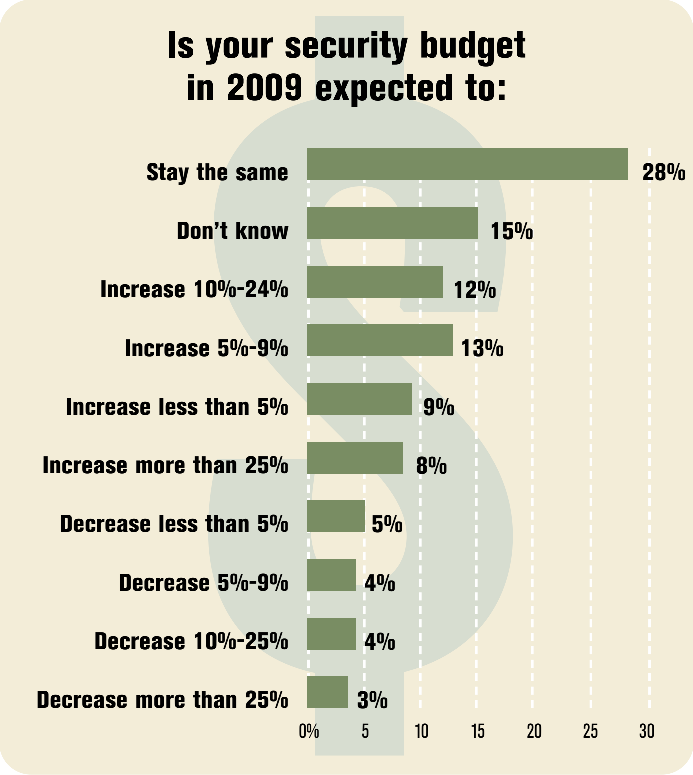
MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES



SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey. Respondents: 790

Do More With Less

So what can you do to balance fiscal responsibility and an upright security posture in 2009? It won't be easy.

Hackers smell blood in the water during down economies. You can bet their budgets aren't down and they aren't being told to delay attacks until the market turns; just the opposite, in fact. Web-based attacks grow more serious and target, in some cases, core elements of the Internet; most recently, attacks on PKI encryption and digital certificate fraud have grabbed the attention of security researchers and organizations.

Ironically enough, if new privacy regulations ultimately brought on by the recession—in addition to those enacted already in Nevada and coming in May in Massachusetts—are put in place, that may bring on a new spend cycle for security in the next 18-24 months.

In the meantime, you aren't waving the white flag. Seventy percent of the 800 security professionals who responded to a question about budgets in *Information Security*'s Priorities 2009 survey said security budgets would stay flat (28 percent) or increase anywhere up to 34 percent *(see chart, above)*. Rather than upgrade infrastructure and software at regular intervals, companies are taking a second look at the security tools they have implemented and taxing those to their limits. More emphasis on awareness training is another strategy companies say they'll use in '09 to contain costs.

"I'm heartened by the fact that security is not taking a hit. People are saying just because things are difficult in the market, we're not going to let our guard down, because it's going to cost us more in the long run," says Howard Schmidt, president and CEO of the Information Security Forum, and former White House cybersecurity czar. "[Hackers] anticipate security pros are distracted doing other things and anticipating that this is the time to strike when people are not focusing on security. But everybody who has been in this business a while says this is the time to strengthen resources."

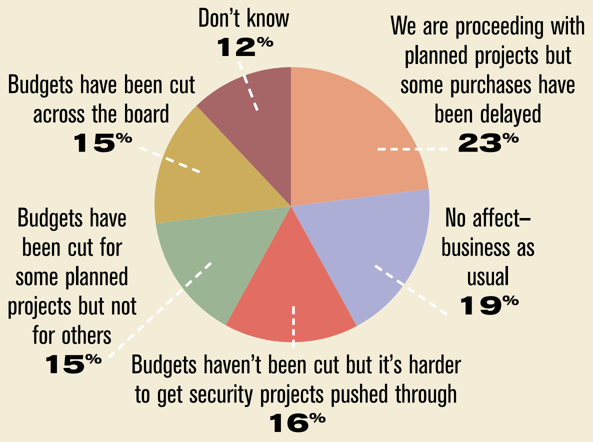
James Routh, chief information security officer for The Depository Trust and Clearing Corporation (DTCC), says there are innovative ways to use the technology and people you have in-house to keep costs in check. The DTCC has done so by implementing security controls early in the software development lifecycle, employing security assessments for service providers, purchasing automation tools for knowledge management, using network monitoring tools to keep an eye on inbound and outbound traffic, and finally, outsourcing some day-to-day security functions.

"There's a perception if budgets are cut, innovation goes with it. I would say it's just the opposite," Routh says. "I would say we have to be more inno-

"There's a perception if budgets are cut, innovation goes with it. I would say it's just the opposite. I would say we have to be more innovative and adopt best practices with an eye toward saving operating costs as we do it."

—JAMES ROUTH, chief information security officer, The Depository Trust and Clearing Corporation (DTCC) vative and adopt best practices with an eye toward saving operating costs as we do it. It requires some level of innovation to do that. Regulators fear an economic downturn means lower spend on information security, and that means higher risk. That's not true as long as innovation is applied."

Which of the following best describes the impact of the economy on security budgets/spending in your organization?



SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey. Respondents: 790

The DTCC clears and settles equity, bond and mortgage-backed securities, money market transactions and over the counter derivatives for corporate and government customers. In 2007, it processed $1.8 quadrillion in securities on the back of a core processing infrastructure with industrial strength resiliency and security. Routh's security program is mature, a key factor in the decision to trim spending on hardware, software and people for the first time in four years. Routh says his organization's risk management capabilities aren't suffering in 2009, but some projects such as an evaluation of Web application firewalls are being postponed *(see chart, above)*.

"There's a few nice-to-have projects we've made a conscious decision not to spend money to evaluate the technology or to implement—at least not this year," Routh says. "In our case, we've been doing a bunch of core process implementations, like security monitoring and identity management, and those we're continuing to fund. There's one or two other projects that were emerging technology-type projects that we've decided to put on the back burner."

One of Routh's big wins is inserting security controls early into software development lifecycle at the DTCC. Vulnerabilities are weeded out well before they appear in functional code that ends up in production and that has resulted in close to $2 million in productivity gains on a base of $150 million spend for development, Routh says.

"Those gains are exclusively the result of having mature and effective controls within our system and software development lifecycle," Routh says. This is a three-year-old initiative that educates and certifies developers in all DTCC environments in security. Developers are also provided with the necessary code-scanning tools and consulting and services help to keep production code close to pristine.

"We've been able to take resource time and reinvest it in other highly productive activities as a result of our ability to weed out vulnerabilities so we don't have to fix code once it goes into production," Routh says.

> "[Inserting security controls early in software development] has resulted in close to $2 million in productivity gains on a base of $150M spend for development."
>
> —JAMES ROUTH, chief information security officer, The Depository Trust and Clearing Corporation (DTCC)

The DTCC has also managed to dramatically trim its spending on service provider assessments through the adoption of the BITS shared assessment program, a set of tools for financial services organizations that includes questionnaires and best practices to help them evaluate a provider's security. The Standardized Information Gathering questionnaire is completed by the provider, and that is followed up by a third-party assessment of a provider environment using BITS' Agreed Upon Procedures (AUP) and its 44 standardized controls. Routh says the DTCC spent $300,000 on vendor site

EDITOR'S DESK
PERSPECTIVES
FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM
MANAGING SECURITY IN A RECESSION
UNDER PRESSURE: 2009 PRIORITIES
GOOD SECURITY ON THE CHEAP
PRODUCT REVIEWS
SPONSOR RESOURCES

assessments in 2007, and chopped that down to $1,100 in 2008, and those costs were training related.

"We used to have to go onsite for all the vendors to do site assessments using our proprietary method, and it was expensive for providers and us (travel, time, cost)," Routh says. "We don't have to do that any more. We can rely on the AUP. That's done by a third party. It's consistent. It's done against a better set of controls, and far more effective from a security standpoint than a SAS 70 review. The more firms that adopt it, the less we have to spend on assessments. That's

BUDGET TIPS

Line Items

HERE ARE FIVE TIPS FOR STRETCHING YOUR ORGANIZATION'S SECURITY BUDGET.

1 **ACCESS YOUR RISK.** Affordable security begins with a thorough assessment of all possible vulnerabilities. A common first step is a risk assessment that determines the organization's risk profile based on threats, threat probabilities and vulnerabilities, potential business impact, and key performance indicators. By gaining awareness of truly compulsory concerns, companies can target specific needs and avoid a costly "shotgun" approach to IT security. For instance, if laptop theft is not a high risk, it is considerably less expensive to offer an education program to employees on laptop theft than to install an anti-theft solution on all laptops.

2 **CONNECT PEOPLE AND PROCESSES.** Technology enables the protection of data and systems, but it also involves people and processes. This fact should never be overlooked; if companies have invested in security, they need to maximize their investment by looking at the people and processes involved, too.

3 **LOOK FOR A HETEROGENEOUS SOLUTION.** Many organizations have built a data center with products from multiple vendors. Therefore, security solutions need to integrate with a variety of third-party products and support multiple platforms so that organizations do not have to pick and choose features or purchase multiple solutions in order to provide end-to-end security.

4 **INVEST IN SECURITY THAT WILL GROW WITH YOUR BUSINESS.** Future growth of the business should always be considered when planning for security. According to a recent study by IDC, unstructured data in traditional data centers is scheduled for a compound year over year growth of over 60 percent, which will increase the need for corresponding security. Choosing a solution that will grow with the business will save the cost and effort of reconfiguration a year down the road.

5 **GO FOR EXPERTISE, NOT COST.** After an in-depth risk assessment, it is essential to choose a security partner who can meet all business needs of an organization. A vendor with an extensive portfolio and proven expertise in the field can address current and emerging security concerns across the entire IT environment. This may not always be the least expensive option, but the cost of choosing the right partner in the beginning vastly outweighs the cost of a data breach brought on by an incomplete security strategy. ▸

SOURCE: Gary Lefkowitz, director, HP Secure Advantage

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

an area where we've got substantial savings by adopting a best practice."

Automation is another area where enterprises can optimize processes and be efficient with resources. While the DTCC may be spending less on hiring new bodies for example, it can and will re-apply those resources toward automation. A knowledge management portal was purchased from Archer Technologies for all of the DTCC's core processes, including information security. The workflow for more than 100 applications was customized for the Archer tool. Now, rather than gathering and sharing documents, and responding to requests for additional information from regulators and auditors—something that used to occupy 35 percent of Routh's team's time—they are given access to the portal. Routh estimates his team now spends less than 15 percent of its time demonstrating due diligence because of the automation.

Compliance Laws Stave Off Budget Cuts

While the DTCC has a massive security infrastructure and a mature organization, midmarket companies find themselves having to be more innovative when it comes to reining in costs. Security budgets are often integrated into overall IT budgets and are annually usually less than $100,000. Still, more than 30 percent of Priorities 2009 respondents said it will be business as usual to an extent around security, primarily because of regulations such as HIPAA and PCI DSS that mandate formal security programs and the implementation of certain technologies such as encryption for PCI.

David M. Stephenson Jr., information systems manager for the Clark & Daughtrey Medical Group in Lakeland Fla., runs a four-person IT team, each of whom has responsibilities over security, including identity management, firewall administration and remote access. Stephenson says the security budget for the medical group's seven-location, 50-provider multispecialty practice is not subject to cuts this year primarily because of HIPAA, but also because the group is in the midst of a conversion to electronic medical records.

> "We've been told to hold off on upgrades unless there is something in the upgrade to the current release that fixes something that is broken."
>
> —DAVID M. STEPHENSON JR., information systems manager Clark & Daughtrey Medical Group

While some IT projects such as a server consolidation initiative via a VMware implementation, and the evaluation of a storage area network, are on hold, security projects are moving forward. Stephenson says he's looking into two-factor authentication for remote connections over an SSL VPN used by contracted transcription services or managers and physicians working outside the office.

What primary strategies will you use to reduce or contain security costs?

38%

Delay or cancel nonessential upgrades or implementations

SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey. Respondents: 790

"We've been told to hold off on upgrades unless there is something in the upgrade to the current release that fixes something that is broken," Stephenson says. "That would be OK, but if we want new features, that kind of stuff we're being told to hold off."

Since new features are out, midmarket companies such as Clark & Daughtrey and enterprises such as the DTCC are looking at

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

infrastructure they own and are figuring how to stretch those investments beyond what they were initially purchased for.

Stephenson stresses that IT managers, in the midmarket in particular, must pay attention to the release notes for new features in updates to products they've purchased. Clark & Daughtrey, for example, outsources its email security (spam and spyware) to AppRiver, and has deployed eight Astaro Security Gateway boxes to handle network and endpoint security at its seven locations and 400 full-time and contracted employees. The Astaro boxes are all-in-one appliances that handle everything from firewall duties, antivirus, content and URL filtering, intrusion prevention and remote access via an SSL VPN.

Remote users for the longest time were connecting via VPN using a free Microsoft PPTP (point-to-point tunneling protocol) connection that Daughtrey says was a nightmare to configure and wasn't very secure. Reading through Astaro release notes after his arrival at the clinic, it had slipped through that Astaro had included an SSL VPN with a recent update to its gateways. Stephenson stresses that IT and security managers should be conducting similar exercises with the technology they have in-house today.

"If money gets cut, then that definitely is a good time to look and ask if we have something in place already? I don't want to find out that we have had a feature the whole time, paying maintenance for it, and not turning it on," he says. "Re-evaluate what you have. You may have been approved for what you need and not realize you've got it, and it may take just some training. You may get the primary purpose of a project done, but all the little secondary benefits get ignored because you don't have time to do it."

The DTCC's Routh suggests going further for enterprises with the resources to do so; tweak your intrusion detection systems, intrusion systems, network behavioral analysis tools to do what you may not have originally envisioned them to do.

"Basically use whatever perimeter toolset that exists for managing the perimeter and turn it to detect outbound malicious traffic," Routh says. He points out that the bulk of today's Web-based attacks are about surreptitiously installing malware on a target machine that essentially, via keyloggers or the like, and phoning home sensitive information that an attacker can turn into a quick profit. "That's an example where the money we've already spent on perimeter-based networking tools today needs to be pointed inward within our enterprises to improve malware detection," Routh says.

"We used to worry about inbound traffic from external sources; that's what the tools are set up to do—that's what a firewall is for," Routh says. "This day and age, it's more important to monitor outbound traffic, that's what will tell where you have infections."

"This is a bad time to cut back on your vigilance, or to postpone some very critical implementations.

—DR. GENE SPAFFORD, founder of the Center for Education and Research in Information Assurance and security (CERIAS), Purdue University

Despite Economic Woes, Don't Let Your Guard Down

While it may be tempting to curb spending on a perceived cost center such as security during a recesssion, it's imperative that security managers convey to upper management the risks of lowering your shields.

"If you look at the world situation today, the economy is bad everywhere, and that tends to bring out more people seeking shortcuts to finding funds," says Dr. Gene Spafford, founder of the Center for Education and Research in Information Assurance and security (CERIAS) at Purdue University. “This is a bad time to cut back on your vigilance, or to postpone some very critical implementations. This is something you need to convey to management. This is a time when people committing fraud are getting more creative, and are larger in numbers. Your business is less able to absorb losses.”

Former cybersecurity czar Schmidt, for one, is encouraged by talk he’s heard that companies are dedicated to maintaining an upright security posture.

“When you’re under siege,” Schmidt says, “is not the time to let your defenses down.” ▸

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

Q P O
R S T
O P Q
S T U

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

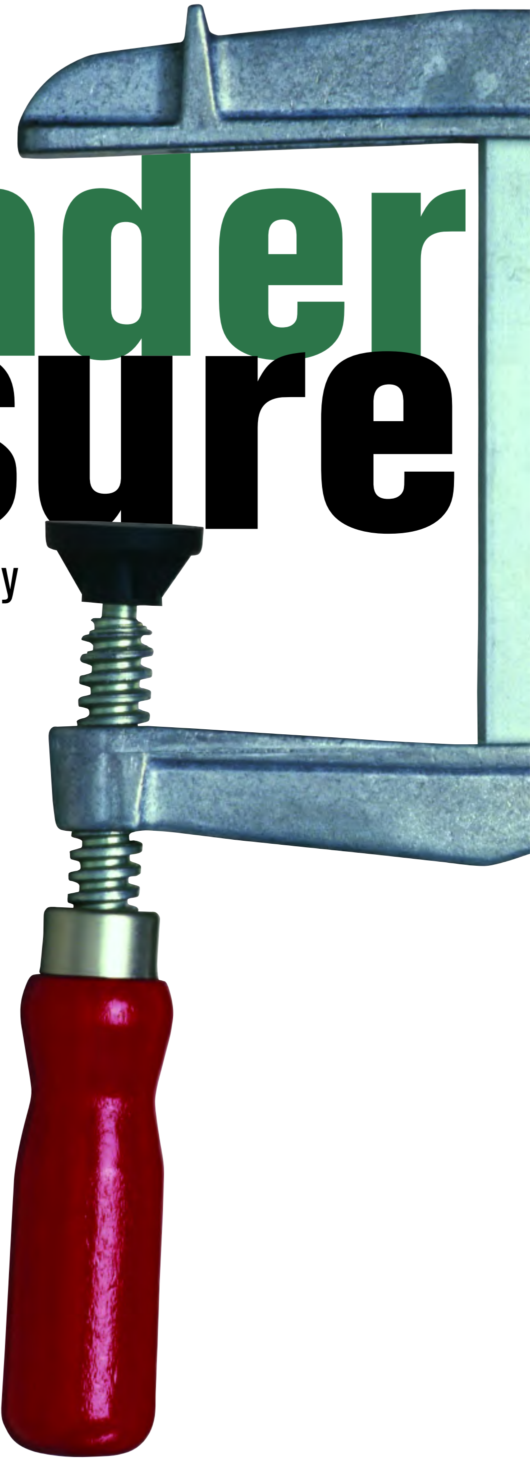
GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

PRIORITIES SURVEY

Under Pressure



Encryption, DLP, and disaster recovery were among top priorities for 2009 while threat management remains a constant concern. BY MARCIA SAVAGE

WITHOUT A DOUBT, compliance demands and fears of bad publicity from stolen or lost data continue to push security to the top of corporate agendas. But a deepening recession could put a real squeeze on security efforts this year.

Readers who participated in *Information Security*'s 2009 Priorities survey ranked data protection, threat management and disaster recovery as top concerns. At the same time, 28 percent of the more than 900 respondents expect their security budgets to remain flat and 23 percent are delaying some purchases. More than half expect security budget cuts if the economy doesn't rebound.

"With tightening budgets, anything that's not essential will probably be put on hold," says Justin Drain, data security manager at Fremont Bank in the San Francisco Bay Area. "If what you have planned isn't designed to deal with compliance or an active threat, it would make sense to put it on hold."

Kevin Dickey, CISO and deputy CIO for Contra Costa County in the San Francisco Bay Area, doesn't have much choice. Data protection is a priority for him, but he's limited in what he can do because the county has been undergoing a series of deep budget cuts.

"The budget cuts force us to be leaner and meaner," he says.

UNDER PRESSURE

Tight budgets notwithstanding, organizations are under pressure to protect sensitive customer data. As of November, 44 states had enacted laws requiring notification of security breaches involving personal data, according to the National Conference of State Legislatures. Other government and industry requirements such as HIPAA and the Payment Card Industry Data Security Standard (PCI DSS) also mandate companies secure their customers' sensitive information.

New personal data protection laws passed in 2008 will add to the pressure. In October, Nevada enacted a law requiring encryption for transmission of personally identifiable information over public networks. A Massachusetts law takes effect May 1 that requires businesses not only encrypt transmission of personal data but also personal data stored on laptops and removable storage devices.

"The trend is increased emphasis on data protection," says Mark Steinhoff, national financial services lead and principal at Deloitte & Touche LLP's security and privacy services. "What we are seeing with our clients is increased concern not only around the regulatory drivers, but brand and reputation risk associated with having the information disclosed in an unauthorized manner."

In addition to protecting their customers' personal data, organizations are paying more attention to securing sensitive corporate data such as trade secrets and strategic plans, he adds.

Data protection, including encryption, data loss prevention (DLP) and database access controls, was one of the top areas where survey participants said they plan to

DISASTER RECOVERY

Planning for the worst

RESTAURANT OPERATOR OUTSOURCES DATA CENTER TO ENSURE UPTIME.

SOME TIMELY PLANNING helped OSI Restaurant Partners LLC avoid disaster when Hurricane Charley hit Florida in 2004, shutting down power in Tampa. The company operates more than 1,200 restaurants, including Outback Steakhouses.

The year before, CIO Dusty Williams and his team outsourced its data center–which was housed in the company's Tampa headquarters without backup power–to Qwest. When Charley hit, "none of the restaurants even knew anything happened," he says.

Disaster recovery planning is critical for every company, Williams says: "No matter what business you're in these days, if systems are down for any length of time, it will have a major impact on either revenue generation or cost containment."

Eighty-two percent of participants in *Information Security*'s 2009 Priorities survey say disaster recovery and backup is among their data protection concerns.

Since moving the data center to Qwest's secure CyberCenter in Tampa, OSI expanded its disaster recovery efforts by adding a backup facility located in Qwest's Chicago CyberCenter. "We look at it as an insurance policy," Williams says. ▸

–MARCIA SAVAGE

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

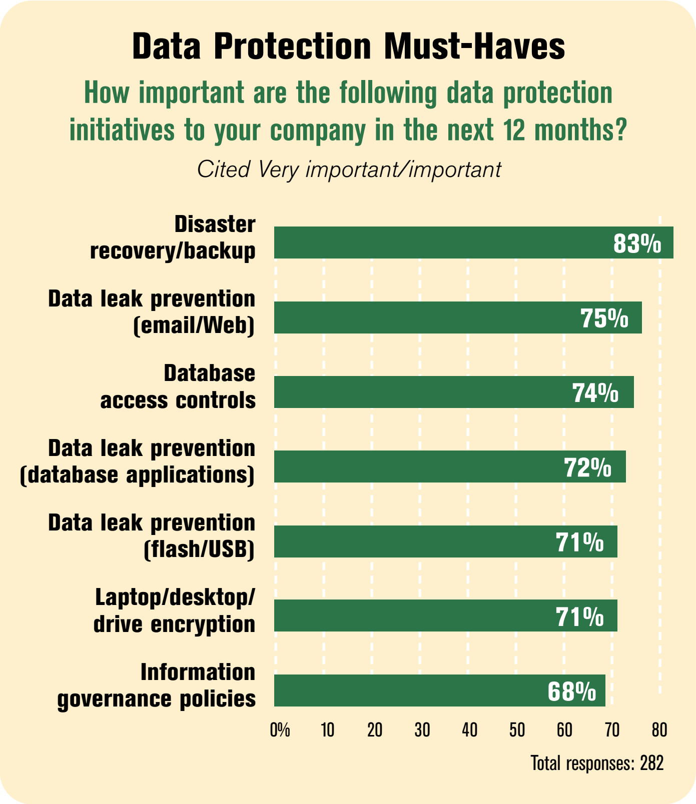
MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES


Data Protection Must-Haves

How important are the following data protection initiatives to your company in the next 12 months?

Cited Very important/important

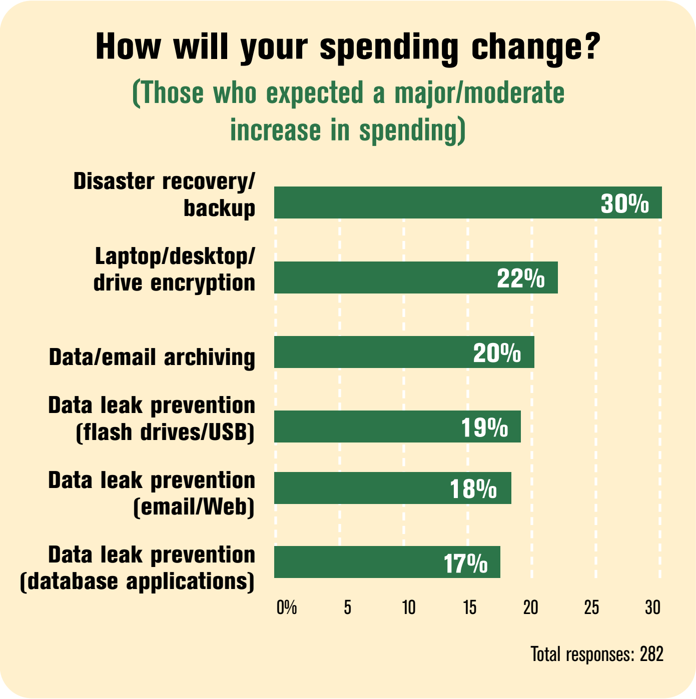
Total responses: 282

SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey

spend more in 2009; 71 percent rank laptop/desktop/drive encryption as an important data security initiative this year. Compliance was by far the top driver for data protection efforts with 72 percent of respondents citing it as the main motivator.

The breach notification laws have made data protection "the hottest topic," says Brad Sanford, CISO at Emory University in the Atlanta area. Organizations "don't want the bad press, especially after seeing what happened to companies like TJ Maxx," he adds.

In the fall, Emory began rolling out a full-disk encryption project with the initial focus on about 1,500 employee laptops and possibly a few high-risk desktop workstations. The university chose a solution that would allow it to encrypt removable media like flash drives in addition to laptops and desktops; a few power users will receive a full installation that lets them manage removable media and encrypt files individually. "When we finish that, we'll probably look at encryption of data backup tapes," Sanford says.


How will your spending change?

(Those who expected a major/moderate increase in spending)

Total responses: 282

SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey

Contra Costa County started last year to encrypt its backup tapes to mitigate the risk of data loss, Dickey says. The county also hammered out laptop encryption guidelines for county agencies. Spending money on full-disk encryption is small compared to the cost of losing personally identifiable data, but the challenge is convincing executive management, he adds.

Pasadena Federal Credit Union uses PGP encryption to secure sensitive internal and external email exchanges in several departments and plans to expand its data protection efforts.

"Some technologies I will

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

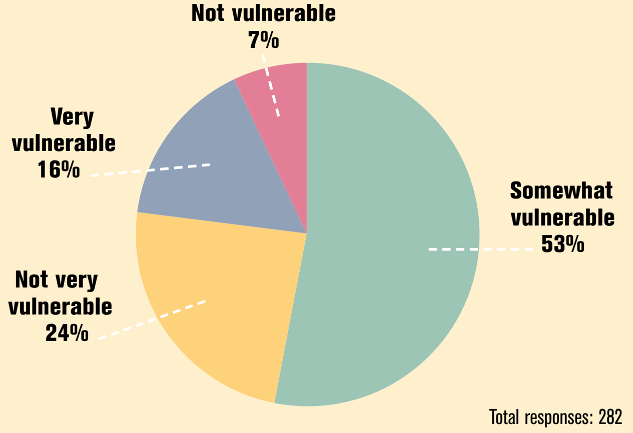
UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

How vulnerable are data protection deployments to potential budget cuts due to the economic downturn?



Total responses: 282

SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey

be implementing in the near future are network traffic encryption for our internal network and PGP key validation and encryption for all employee email accounts," says Mike McDanell, information security officer at California-based PFCU.

In addition to encryption, organizations are eyeing DLP technologies. Seventy-one percent of survey respondents say preventing data leaks via flash drives and USB tokens is important and 75 percent say preventing data loss via email and the Web is key.

Fremont Bank's Drain says a major focus for him in 2008 was deploying a DLP tool, which handles multiple protocols. "The problem hasn't been completely solved, but I feel a lot safer now," he says. The DLP deployment was driven by more than compliance demands, he says, calling it an overall best practice.

ACCESS CONTROL

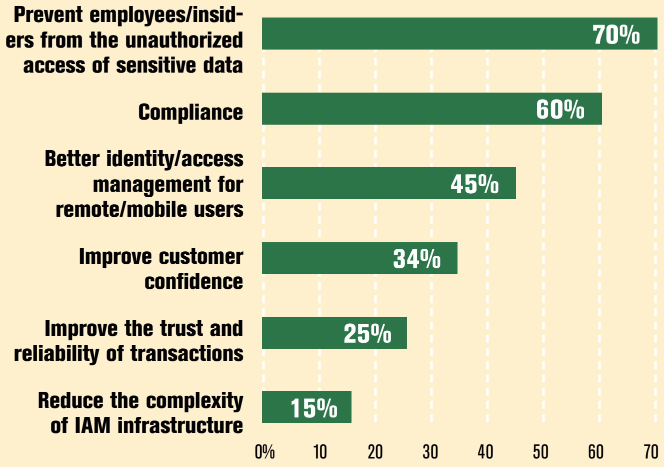
Alongside their encryption and DLP efforts, organizations are focused on controlling users' access to sensitive data and other corporate resources. Survey respondents cited several identity and access management challenges ahead for 2009, including strengthening endpoint security (67 percent), getting better at strong authentication (55 percent), and improving user access rights (56 percent).

"We're certainly looking at improving our password controls and expanding our use of two-factor authentication," Emory's Sanford says. "The whole identity management struggle—provisioning and de-provisioning of accounts, making sure the right people have the right level of access into critical systems—is paramount."

Being a university, Emory's environment is fairly decentralized. Figuring out how to effectively manage access in an environment that involves

What are the biggest drivers for improving identity and access management at your organization?

(Could choose up to three)



Total responses: 241

SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey multiple service providers and other third parties is a challenge for many organizations, Sanford says.

USA Federal Credit Union plans this year to replace the multi-factor system it implemented at the end of 2006 to meet FFIEC requirements. The system turned out to be cumbersome, which turned off some online members, says Carolyn James, senior vice president and CIO at USA Federal.

"In the past couple of years, there have been some great developments with multi-factor [technology]. Now, it's more integrated with your platform and almost invisible to members," she says.

The credit union is making the investment in order to promote its online services, which are a cost-effective means of serving members, she adds.

Scott Crawford, research director at IT consulting firm Enterprise Management Associates, says the biggest issue with strong authentication is making it more transparent and less expensive for a business to manage. Physical tokens are expensive to distribute and maintain; companies such as AdmitOne Security, which provides tech-

WEB 2.0

Businesses ban social networking sites

SITES FOR SHARING PERSONAL INFORMATION RAISE SECURITY CONCERNS.

SOCIAL NETWORKING SITES such as MySpace and Facebook may be digital darlings in today's hyperconnected culture, but they're not too popular in the enterprise. In fact, most are apt to ban their users from accessing such sites.

Forty-two percent of participants in *Information Security*'s 2009 Priorities survey say their policy is to ban user access to social networking sites entirely. Another 27 percent restrict access somewhat.

"In a business environment, social networking is a very bad thing and we look at it as something that needs to be restricted at every point," says Justin Drain, data security manager at Fremont Bank. "It's extremely risky."

Security experts have warned that attackers can use social networking sites to collect personal data about people and carry out social engineering attacks. At the 2008 Black Hat Briefings in Las Vegas, a pair of security consultants demonstrated a series of MySpace attacks, which combined social engineering and technical hacks.

Scott Crawford, research director at IT consulting firm Enterprise Management Associates, says enterprises tend to steer clear of social networking sites even if the marketing department sees it as a new media outlet. "Unless there is some compelling reason, they're inclined to shut it off," he says. "It's a best practice as far as security."

In academic environments with student populations, however, banning or restricting use of Facebook and other sites isn't so feasible.

"We do have some monitoring but we don't restrict it," says Edmond Kwok, desktop engineering manager at the University of San Francisco. "Some of our courses use social networking sites; one uses Second Life as a teaching tool." ▸

—MARCIA SAVAGE

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

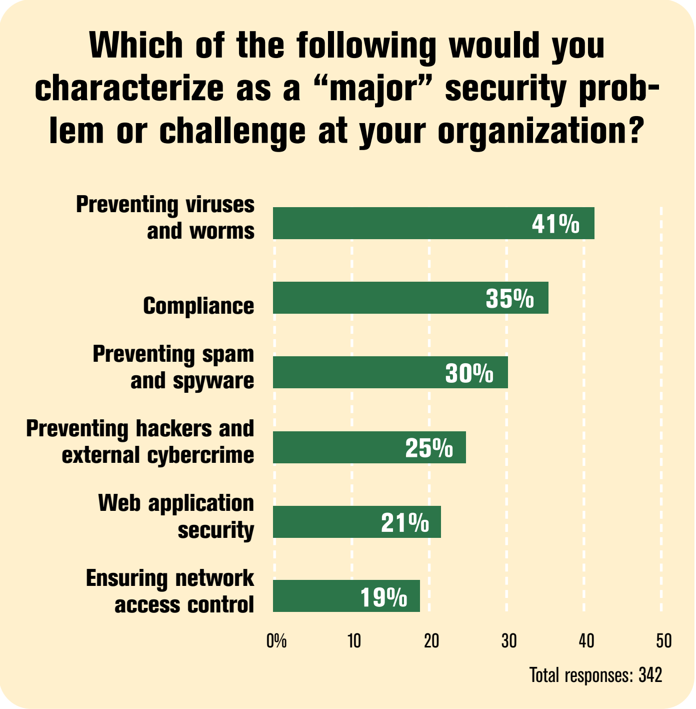
MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES


Which of the following would you characterize as a "major" security problem or challenge at your organization?

SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey

nology that uses keystroke biometrics to authenticate users, offer new approaches, he says.

But Crawford calls endpoint security "the most troublesome aspect of security" for most organizations. "I see businesses still trying to get a handle on making it work and getting some control over what's happening on the endpoint."

Fremont Bank is among those working to gain control over the endpoint. The bank has implemented various tools and procedures to ensure better access control over endpoint devices, including portable storage devices. "We want to be able to say with a level of clarity and confidence that we know everything that touches our network," Drain says.

The University of San Francisco started focusing on endpoint security when it saw a spike in infected computers. It beefed up its security policies and deployed Sophos software for about 3,000 faculty members and employees. Centralized management and Macintosh support were key concerns for USF in the deployment, says Edmond Kwok, desktop engineering manager.

"We're seeing this as a solution to protect the end user and lower our support costs," he says.

Organizations are preparing for a continued onslaught of threats to endpoints and the overall network. Threat management—defending against viruses, malware and intrusions —is an area where 21 percent of respondents said they plan to spend more in 2009, ahead of data protection, identity management and application security.

"Just the sheer growth in malware code that's floating out in the wild has people very concerned because how do you deal with the staggering growth in threats that often directly target sensitive information?" Crawford says.

"You should assume attackers will get past some defenses, so this raises the bar on defense in depth," he says. "You want to contain them an make it as frustrating as possible to get to their desired targets…So that means increasing the number of barriers to sensitive information—without interfering with the performance of critical applications."

Organizations are always looking for better threat management solutions, says Emory's Sanford.

"The good guys and bad guys are at war on that front. They get better attack tools, you improve your defenses and it seesaws back and forth," he says. "Everyone is spending time consciously looking at where they are, what their defenses are capable of, their shortcomings, and how to improve."

Enterprises are focused on correlating threats to vulnerabilities—formulating all the data produced from various threat management tools so they can make meaningful decisions about mitigating threats, says Deloitte's Steinhoff.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

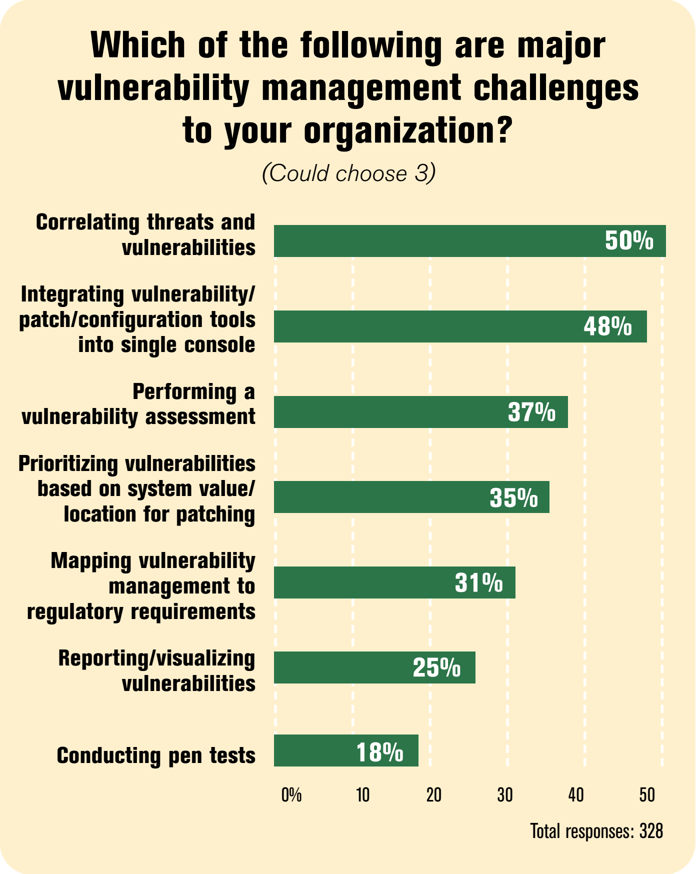
GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

Indeed, a half of survey participants cite correlating threats and vulnerabilities as their top vulnerability management challenge.

Contra Costa County's Dickey is looking at automated vulnerability scanning and patch management tools to reduce risk exposure—and to deal with fallout from the county's budget cuts. "We also need automated tools to replace the fact we don't have as many human resources to do manual reviews on desktops and servers," he says.



SOURCE: *Information Security*/SearchSecurity.com Priorities 2009 survey

COST CONTAINMENT

While organizations have threat management and data protection at the top of their to-do lists, many are "deferring some of the technology solutions based on budget constraints," Deloitte's Steinhoff says.

"Rather than spending dollars today on technology implementations, more [businesses] are taking their time and taking advantage of the current environment to think through, plan, evaluate and test the market for the right solution," Steinhoff says.

Twenty-two percent of survey respondents say delaying or canceling nonessential upgrades or implementations is their top strategy to contain security costs. Well over half say that threat management, data protection or identity and access management deployments are vulnerable to potential budget cuts.

At Emory University, Sanford expects to put a priority on initiatives that can be done for free or less money while putting off more costly projects for a couple years. Cost-saving initiatives include improving policies, ramping up security awareness, and utilizing open-source tools. Twenty-seven percent of survey participants say they will focus on security awareness as a cost-containment measure.

"There are a lot of ways to improve the security posture of your organization that aren't necessarily about buying tools and implementing them," he says. "Even something as simple as evaluating technologies you've deployed and making sure your default install configurations have the right security controls will go a long way to improving security."

USA Federal Credit Union is looking to consolidate a few of its security vendors in order to save money, James says. However, the gloomy economy won't impact the organization's security efforts. "It's a bleak year, but we'll keep our systems running and not give up on security," she says. ▸

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

GOOD SECURITY ON THE CHEAP

10 tips to protect your company in a down economy.

BY DAVID STROM

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

TIMES ARE TOUGH for the good guys, but a recession is always an opportunity for criminals. Threats to your sensitive data, your customers and your infrastructure are increasing dramatically, from compromised and malicious Web sites to unhappy employees to poorly controlled partners.

The good news is that you can tighten your security and tighten your belt at the same time. Quick-payoff strategies can help you stay on top of evolving security threats without neglecting your network infrastructure.

There are many clever ways to do this. We'll look at 10 steps you can take to improve your threat management posture that require minimum investment, manpower and give you a fast return on your investment.

#1 Secure powered-down switches.

For a small effort, you can lock down unused network ports and at the same time save money by reducing your overall power consumption with switches (from Adtran and D-Link, for example) that turn off or power down when they're not needed. Your investment in this new equipment will pay for itself in a year or less.

Auto shut-off is a good way to secure your unused ports, by keeping prying PCs from entering your network at unexpected places and also helps physical security, especially in publicly accessible buildings such as hospitals and government offices.

#2 Check out lower-cost endpoint security.

There are dozens of endpoint security appliances and agents that come with hefty price tags and long implementation lead times.

If you want some of the benefits without the hassles and cost, then one solution is to purchase TPM-enabled laptops and start using some form of protection, such as fingerprint scanners or encryption keys that are stored on the TPM to keep unauthorized users away. The combination is a potent one since the TPM ensures that no one else can tamper with the scanned fingerprint to access the laptop.

Also, consider an appliances from Napera or eEye Digitial Security's Blink software. These are representative of a trend to lower-cost endpoint security products that are drop-and-replace solutions for Windows-only environments.

Napera looks like a network switch and works with a combination of agent-based software and firmware on the switch. You can enable protection on various ports and make sure that each PC that connects to these ports has updated anti-virus signatures and OS patches, and is malware-free before it connects to your network. It starts at $3,500 for a 24-port device, so this could be appealing for many small businesses. Or it could be deployed to protect public areas of your campus such as conference rooms and visitors' offices, where a lot of unknown laptops connecting to your network.

Blink offers a lot of protection for less than $30 a seat per year, including personal firewall, anti-virus and host intrusion prevention modules that are all part of its single agent.

#3 Get VPNs for free.

If you haven't implemented a VPN yet, now is the time to start. As your workforce becomes more mobile, there is more potential exposure to eavesdroppers at Wi-Fi hotspots and hotels. VPNs also come in handy when you want to extend a network share across the Internet securely, and have access to your files when you are on the road.

Certainly, you can spend tens of thousands of dollars on VPN technology.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

But if you just want some basic and simple protection there are plenty of low or no-cost software alternatives that can do the trick, as long as you have a broadband connection at your disposal. One open-source offering is available at OpenVPN.org [http://openvpn.org/]; LogMeIn's Hamachi [https://secure.logmein.com/products/hamachi/vpn.asp] is another service that is free for personal use (otherwise it has a low monthly fee) and easy to set up. There is also a listing at FileShareFreak [http://filesharefreak.com/2008/01/27/vpn-tunneling-for-private-p2p-connections/] with some other offerings too.

The trick is making them universal for your staff to use, and providing support resources to guide the first-time VPN-ers through the process. The free VPNs could also serve as a stepping-stone to more capable products with heftier price tags and a way to justify their purchase later in the year.

#4 Avoid the Cisco "tax".

With the New Year, it is time to look at your annual support bills from Cisco, which you pay to keep current with IOS versions and for maintenance response time. I call this the "Cisco tax," and you should see if it makes sense to buy either a replacement device that you can keep as a spare or else find another vendor that doesn't charge for upgrades to their firmware/router operating system software (Adtran is one that comes to mind). Again, this could be a very quick payoff, although it does involve spending some money to produce savings down the road.

#5 Deploy (Almost) Effortless Encryption.

Certainly, encryption is one of those "nice to have, but hard to do" technologies that always seems to get on these lists. But, in recent years, a number of free or low-cost email and disk encryption tools have gotten better, so this could be the year to actually encrypt your removable disks and emails.

Two good places to start are the free open-source TrueCrypt [www.truecrypt.org] and Voltage Security's low-cost but easy-to-implement Voltage Security Network service.

TrueCrypt has a disk encryption client for Mac, Linux and Windows machines. Though it lacks enterprise management tools, it's excellent for small companies, executives and workgroups (for more on TrueCrypt [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1340488,00.html] check out Russ McRee's *Information Security* article). Voltage offers hosted email encryption that doesn't require any client installation and can work with Outlook and Webmail installations, all for about $65 per seat per year. Voltage handles all the administrative details, and the hosted service is quick and easy to implement.

And, of course, there is the long-time favorite from PGP, which is priced at less than $100 a seat, depending on what features you want to include. All of these products make managing the encryption keys extremely easy: one of the drawbacks of implementing enterprise encryption is handling expiring keys when employees leave, or recovering them when they forget their key.

You could also turn on BitLocker and FileVault in the native Windows and Mac OS, respectively. They provide extra protection without spending an extra dime. However, they are hard to deploy across the enterprise—you definitely get what you pay for here.

#6 Get to Know Your IDS.

You might think simply having an intrusion detection system is enough of an achievement, but it is time to get up close and personal with your IDS and do a better job of tuning it to your particular circumstances. This means adjusting its configuration, understanding its reports and logged activities, and doing some rudimentary analysis.

Granted, there is never enough time in the day, but if you are going to stay on top of the latest threats, you need to spend some more time with your IDS analysis to understand what it is telling you. If you are using Snort as your main IDS, check out Richard Bejtlich's podcast [http://media.techtarget.com/audioCast/SECURITY/richard_bejtlich_snort_FAQ.mp3] and check out forums on snort.org [http://www.snort.org] to gain more expertise.

Another option is to send one or two of your staff to get additional training in understanding your system's features and ways that you can tighten it up. While training budgets are the first to go in a recession, this is one investment that can provide quick paybacks, and provide additional threat protection with very little incremental effort.

You might think simply having an intrusion detection system is enough of an achievement, but it is time to get up close and personal with your IDS and do a better job of tuning it to your particular circumstances.

#7 REALLY Terminate ex-Employees.

We're talking about the waves of layoffs of all types of employees, not just in the IT department. As your company contracts, the biggest threats are from staff who have been on the inside and are now jobless. Studies have shown that an ex-employee can be a security nightmare. Never changed any of your passwords on key servers? Do you have the same master password for multiple machines? Now is the time to change that behavior.

You should also do an assessment of other risks from newly terminated staff. Are your access control policies up to date? Did you disable all the security keys, passwords and access codes? Do you know if your remote gateways are still be used by these people? Time to check access logs and make sure that the access directory entries of the departed are removed as well.

#8 Get Rid of SQL Injection Once and for All.

It is amazing that an exploit so long in the tooth can continue to affect, even destroy, so many servers. SQL injection is basically a back door entry into your databases through unprotected Web pages. A hacker can create and execute it without any programming knowledge and little skill. Why is this still a source of pain?

One reason is that really eliminating SQL injection requires the cooperation of several different departments, working together to make sure that the vulnerabilities aren't ignored. Another reason is that vulnerable sites are easy to find, especially since a couple of quick Google searches with a few keywords can often uncover problems without a hacker having to even enter your network with any probes. (Check out this good quick tutorial on protecting yourself from Google hacking [http://www.informit.com/articles/article.aspx?p=170880&seqNum=4].)

So, let's try to stamp this out forever this year; take the time to really go through your applications to make sure that it doesn't find you on someone's list next fall. Do an audit, hire a specialist consulting firm, or get educated on how to fix your database/Web server programming to prevent what is still an unfortunately common exploit from happening. Go to OWASP.org [http://www.OWASP.org] and get lots of tips on how to set up your database access properly and understand exactly why and how you are vulnerable.

It is amazing that an exploit so long in the tooth can continue to affect, even destroy, so many servers

If you want something more potent, you can download a free version of Acunetix's Web Vulnerability Scanner and various free trials of HP's assessment tools [https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5E14344_4000_100__], such as WebInspect.

Another thing to try is modsecurity.org's [http://www.modsecurity.org] open-source Web App Firewall; check out this *Information Security* article on modsecurity [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257087,00.html] to learn how to get the most from this tool.

Of course, just because you downloaded the free scanner and didn't find anything at first doesn't mean that you are protected for all eternity, but at least you can get a start on how to use these tools and understand how you are vulnerable. The trick is doing a regular series of scans to make sure that no one created any new backdoors.

#9 Stop Data Leaks.

One data breach lawsuit can ruin your whole day. As more data traverses the Internet, it makes sense to look at lower-cost tools that can stop data leaks or at least be more proactive about them. Code Green Networks and eTelemetry Metron SE are examples of monitoring products that can be easily deployed and don't cost as much as some of the alternatives. They can also scale up to some fairly large installations.

Granted, this is spending probably more dough than you want to—we are talking five- or six-figure purchases here—but, still, if you have tried some of the other lower-cost steps we recommend this might be a smart place to make a moderate investment.

#10 Pay your own people to find innovative solutions.

This is so simple and easy to implement that you will wonder why you didn't think of it. Set up a reward system to foster out-of-the-box thinking and ways to tune your security posture by having your own staff make and then benefit from their suggestions. You can avoid hiring consultants and increase morale at the same time. Your own people are the real experts when it comes to understanding the major weaknesses of your systems. The more you can encourage them to come forth, the better for everyone around.

David Strom is an expert on Internet and networking technologies who was the former editor-in-chief at Network Computing, *Tom's Hardware.com, and DigitalLanding.com. He currently writes regularly for PC World, Baseline Magazine, and the New York Times and is also a professional speaker, podcaster and blogs at strominator.com and WebInformant.tv. Send comments on this article to feedback@infosecuritymag.com.*

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

Touch-Free ID

Vein-reading biometric authentication introduced in health care. BY NEIL ROITER

AN ACCIDENT VICTIM is rushed to the ER. He has no ID—perhaps his wallet is still in the wreckage if his car, perhaps he simply left it at home. A staff person takes the victim's hand and waves his palm over a vein reader. In seconds, the hospital knows not only who he is, but has access to all his records, including blood type, allergies, pre-existing medical conditions and, yes, insurance.

Not every use case for vein reading technology is this dramatic, but health care facilities, along with financial institutions, are prime market targets for Fujitsu's PalmSecure, which has been in use in Japan and is now being marketed through partners in the U.S.

"It makes the registration process, once someone is enrolled, much more streamlined for subsequent visits," says Rogel Reyes, director of patient access for Pleasanton, Calif.-based ValleyCare Health System. "Each time they come to a point of service they are not asked for their card or license; they simply place their palm over the scanner."

Fujitsu partner HT Systems markets PalmSecure as a specialized health care authentication package, PatientSecure. ValleyCare, which has some 35 scanning stations throughout its two centers in the Bay area, is an early adopter.

Though it's new in the U.S., vein-based biometric authentication has had some success in Japan, where Fujitsu's palm-based readers and Hitachi's finger-based Vein Reader are deployed at tens of thousands of ATMs.

PalmSecure is basically a one-inch cube. For general use, it's built into a mouse. Fujitsu initially offered a small market version, but recently released an enterprise version with support for single sign-on, starting with Citrix but to be extended to other top-tier vendors soon.

Though its still a small fraction of a biometric authentication market that hasn't exactly taken the U.S. by storm, vein-reading has some advantages. Unlike fingerprint identification, which checks for a physical match, vein-reading uses infrared technology to detect an individual's unique blood flow pattern. The head, the heart and the hand are the parts of body where veins are most dense. Obviously, the hand is the most practical place to take a reading.

Proponents say it is far more accurate and yields fewer false positives than fingerprint biometrics. And, fingerprints can be spoofed or damaged by injury or rough physical labor. For medical facilities, it's also a matter of hygiene. Waiting rooms, with scores of sick people are bad enough. Imagine all of them touching the same fingerprint reader.

That's why fingerprint readers have been unsuccessful in supermarkets, said Dan Miller, Fujitsu's business development manager for PalmSecure.

"People have germs. They didn't want to touch them. They failed miserably," he said. He added that the readers had to be frequently cleaned of a rich coating of grime, hand lotion, melted chocolate…you get the idea. Vein-readers can also read through opaque surgical gloves.

Hygiene and maintenance aside, the impetus for vein-reading in the health care industry is financial.

"The biggest ROI or biggest pain point we're solving, behind the scenes, is fraud," said Miller. "With health insurance at a premium, a lot of people are just giving their cards to family members."

> "The interaction with the sensor is not awkward. It doesn't require something as intrusive as iris recognition; you don't have to open your eye lid."
>
> —ANT ALLAN, analyst, Gartner

That's not only costly but dangerous. The fraudulent patient could wind up getting medication he can't tolerate, or the wrong blood type.

"Another advantage is simplicity and universality of use," says Gartner analyst Ant Allan. "The interaction with the sensor is not awkward. It doesn't require something as intrusive as iris recognition; you don't have to open your eye lid."

There are downsides, however.

"It's relatively expensive—several times more expensive than fingerprint, two to three times more than iris recognition," says Allan. "You'll likely see it at a few control points—passports, for example—when unit prices isn't barrier. You won't see it in every laptop because of the cost and size of the sensors." ▸

Neil Roiter is senior technology editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

PRODUCT Reviews

TESTING & ANALYSIS TO HELP YOU MAKE PURCHASING DECISIONS

HotPick INFORMATION SECURITY®

DATA PROTECTION

IronKey Enterprise Secure Flash Drive

REVIEWED BY ED TITTEL

IronKey

www.ironkey.com

Price: **From $79 to $299 for 1, 2, 4, and 8 GB devices**

IronKey Enterprise Secure Flash Drives enable organizations to control access to sensitive information on portable flash drives. Administrators can deny access to a flash drive until it verifies status with a management server, disable access to the device entirely, or destroy the contents to counter loss and theft.

Capabilities A

All IronKey Flash devices are waterproof, and feature tamper-proofing to foil chip extraction techniques, and limited access attempts before flash contents are destroyed.

Each device includes a high-speed, military grade crypto chip that operates in AES Cipher-block mode for data encryption, and that supports 2048-bit RSA keys for PKI and 256-bit SHA for hashing (complies with FIPS Validations 140-2 Level, 186-2, and 197). Each device is also assigned a unique digital certificate.

IronKey also provides a secure password store and does not permit encryption keys to be copied to other devices. The unit includes support for various portable applications, including a secure Web browser (based on Firefox), an identity manager with secure password storage online, and an encrypted backup utility. These drives work transparently with Windows XP, Vista, and Server 2003 and 2008.

Installation/Configuration B

What makes the enterprise edition so attractive is the setup process used to configure, issue and manage devices. The first step requires accessing secure IronKey servers to set up an administrator account and policies.

Testing methodology: We attempted third-party access numerous times, without success, and wiped flash drive content as needed.

By default, the devices destroy their contents after 10 unsuccessful login attempts, but this is configurable. Password policies set minimum length and various strength criteria. Software policy lets administrators enable components that include a secure Firefox version, secure sessions, secure backup, identity manager, and integration with RSA SecurID. Users may also be allowed or denied use of the my.ironkey.com website for self-service password recovery.

A first use of the administrative key leads the trusted user to a secure Web page, where initial configuration is set up and stored. Subsequent logins at end-user and administrative levels lead to an enterprise-specific Web server operated by IronKey.

Generally, users are limited to password backup and recovery, while master administrators control the entire IronKey Enterprise environment to delegate authority to user administrators for routine tasks such as creating users, or disabling and re-enabling IronKey devices.

The console tools are well-built and reasonably easy to follow and use, although admins must work their way through a large number of screens and some activities can take a bit of time and learning.

Enterprise Effectiveness A

The real power of the IronKey Enterprise comes from its ability to set up and manage thousands of secure flash devices. Administrators can set and manage policy for all of the flash drives whose digital certificates originate from the management console, and enable or disable devices across the entire enterprise from that console.

IronKey's Silver Bullet Services provide multiple options that can limit access to data on drives that have been lost or stolen, or that may still be in possession of an employee that has been judged to represent some kind of threat. Administrators can deny access to specific devices, disable access to its contents, destroy the contents or reprovision devices to new users.

Verdict

IronKey Enterprise is a powerful and effective way to establish and maintain control over mobile information assets.▸

Review how we grade at searchsecurity.com/grading_criteria.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

MOBILE SECURITY

PGP Endpoint

REVIEWED BY SANDRA KAY MILLER

PGP CORPORATION

www.pgp.com

Price: **Starts at $49 per user**

PGP Endpoint meets the urgent need to protect data on mobile and removable storage devices, delivering centrally managed, granular device and port control, coupled with automated whole disk encryption.

Installation/Configuration B

The PGP Endpoint architecture comprises an administration server, database, management console and client. PGP leverages Active Directory and Novell e-Directory for quick integration into directory services.

Preparing the host server for installation required more manual intervention than similar products, but the setup went smoothly once we got to the server components wizards.

The client can be automatically deployed through the distribution utility, using directory services or third-party tools, but we stuck with manual installation via USB drive. PGP tests for connectivity to the administration server before completing the installation. As with similar products, the client offers centralized hardening to prevent tampering.

The management console presents an easy-to-use Device Explorer panel with a hierarchical tree listing the default settings for 17 assorted devices and ports, as well as user-defined devices.

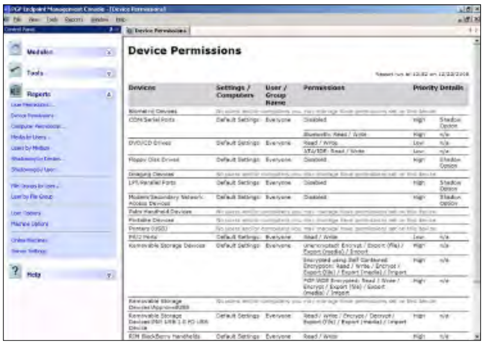
Policy B+

Devices and ports are either allowed, blocked, or the data passing through must be encrypted.

We were able to quickly enable policies that ranged from global enforcement of granular policy, such as only the use of company-issued USB thumb drives upon which everything is automatically encrypted, to specific settings for individual users.

PGP Endpoint let us easily specify what devices and ports were authorized, set rules for their use, and determine what data should be set to read-only, read-write and encrypted, or blocked.

Testing methodology: We deployed PGP Endpoint on Microsoft Windows Server 2003 with Active Directory and tested using a variety of devices running Windows 2000, XP and Vista operating systems.



Device Permissions

Report run at 12:02 am 12/22/2008

Devices	Settings / Computers	User / Group Name	Permissions	Priority	Details
Biometric Devices	No users and/or computers you may manage have permissions set on this device				
COM/Serial Ports	Default Settings	Everyone	Disabled	High	Shadow Option
			Bluetooth: Read / Write	High	n/a
DVD/CD Drives	Default Settings	Everyone	Read / Write	Low	n/a
			ATA/IDE: Read / Write	Low	n/a
Floppy Disk Drives	Default Settings	Everyone	Disabled	High	Shadow Option
Imaging Devices	No users and/or computers you may manage have permissions set on this device				
LPT/Parallel Ports	Default Settings	Everyone	Disabled	High	Shadow Option
Modem/Secondary Network Access Devices	Default Settings	Everyone	Disabled	High	Shadow Option
Palm Handheld Devices	No users and/or computers you may manage have permissions set on this device				
Portable Devices	No users and/or computers you may manage have permissions set on this device				
Printers (USB)	No users and/or computers you may manage have permissions set on this device				
PS/2 Ports	Default Settings	Everyone	Read / Write	Low	n/a
Removable Storage Devices	Default Settings	Everyone	Unencrypted: Encrypt / Export (file) / Export (media) / Import	High	n/a
			Encrypted using Self Contained Encryption: Read / Write / Encrypt / Export (file) / Export (media) / Import	High	n/a
			PGP WDE Encrypted: Read / Write / Encrypt / Export (file) / Export (media) / Import	High	n/a
Removable Storage Devices\Approved USB	No users and/or computers you may manage have permissions set on this device				
Removable Storage Devices\[illegible] USB 2.0 FD USB Device	Default Settings	Everyone	Read / Write / Encrypt / Decrypt / Export (file) / Export (media) / Import	High	n/a
RIM BlackBerry Handhelds	Default Settings	Everyone	Read / Write	High	n/a

Logging and Reporting B+

PGP Endpoint covers all the bases for logging every type of device or connection capable of transmitting and storing auditable information.

Within a few minutes, we set up an audit log that would allow us to prove that all endpoints within our network had encryption and policies necessary to meet regulatory requirements for data, whether it was passing over wireless, stored on a CD or sent to a hand-held device.

Logs record all events related to policy enforcement, as well as administrative actions, such as changing user access permissions. The dynamic tables in the management console let us sort and organize data based upon a multitude of criteria. Both logs and queries can be exported to CSV format. Using basic templates, we were able to quickly set up automated reports, such as "Applications denied today," or custom reports.

Effectiveness A

We found PGP Endpoint to command one of our highest ratings in this space in terms of securing and monitoring all aspects of endpoint security, as well as usability.

One of our favorite features is the ability to share encrypted data on removable media with another device without the client. With only a passphrase, we were able to access documents on an encrypted USB drive, change and save them, while enforcing security policy. PGP also allowed us to set temporary permissions and enforce extensive security measures on devices that weren't connected to the network, or portable media, regardless of the device on to which it was attached.

Policies were strictly enforced with complete transparency, without any impact on computing performance.

Verdict

PGP Endpoint is a cost-effective and comprehensive security solution that delivers automatic, seamless and transparent policy enforcement and auditing to endpoints.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

ACCESS CONTROL

Rohati TNS 100

REVIEWED BY BRAD CAUSEY

Rohati
www.rohati.com
Price: **Starts at $20,000 per appliance**

Rohati's new agent-less Transaction Network System takes traditional network access control to the application level to allow complete granular access control for Web-based applications, and file shares (We tested the beta version of this, pending release). Rohati calls this Network-Based Entitlement Control or NBEC. The concept behind this isn't new, but having the ability to do this without agent deployment could make deployment and integration that much easier.

Configuration/Management B

Setup involves a few different steps and resources. The complete system involves configuration of the TNS device, a management server, and possibly VLAN configuration on your switches.

The TNS 100 device we were issued was a 1U appliance that supports up to 4Gbps throughput with up to 256,000 connections. The initial setup utilized a serial console port with simple commands that resemble Cisco IOS syntax. This is useful if you are familiar with this type of command syntax. There are a couple of deployment options here when deploying out-of-band. If you choose not to use VLANs for segmentation, you can simply plug the TNS 100 into a switch and move on to the CMS setup. A little more effort is required for adding VLAN configurations. One of the drawbacks of not using VLANs is that you'll need to configure protected resources to only accept connections from the TNS 100 appliance. This is because the device would accept connection requests from systems other than the TNS 100, in order for the TNS 100 to properly protect the desired resource, you much send all requests through it.

Once the initial appliance setup is complete, you'll need to deploy the Central Management System or CMS to further configure the device. You'll need some server class hardware. Rohati recommends a dual processor 2.0GHz or better, as well as around 120 GB of space and 2 GB of RAM. You can use either Windows Server 2003 SP2 or various flavors of Linux for your host operating system.

The CMS software installation is very straightforward and consists of a single executable delivered via CD. Once installed, you must configure the CMS to talk to the TNS 100 as well as any LDAP system in use.

Policy Control B

Policies are configured via the Web interface over SSL on the CMS server. At the highest levels, Rohati groups everything into policy domains, which are containers for access control points that consist of rules and users. These rules are basically decisions that result in a permit or deny of a request targeted at a protected resource, such as a URL on a Web server.

When building these policies, you can set them in four different ways. An enforcement policy is used to restrict access to resources. A re-authentication policy is used to force additional security even after a successful authentication to a given resource. This would be particularly useful to protect sensitive areas of public sites, such as the administrative panel of the HR online system. A logging policy is a policy that doesn't restrict anything, but allows you to monitor the activity to that resource. This is great if you just need to determine if that resource is being misused and might require further security from the TNS 100 Finally, a simulation policy is used to test policies before they are enforced, allowing you to see what would have been blocked or allowed based on the test rule set. All policies are based on what Rohati calls User Directories, these are basically LDAP repositories such as Active Directory.

Effectiveness C

Rohati has built a great tool for protecting select resources, however, there are a few factors that may limit the overall effectiveness of this solution. Although the TNS 100 has the ability to utilize default attributes stored in LDAP, it is recommended that you create custom attributes for the purposes of policies. This method is effective, but also time consuming both initially and in long-term maintenance. The sensitivity of the resource will most like determine the level of granularity you

Testing methodology: Our lab included two Active Directory domains, the Rohati CMS server, and several SMB resources and Web Servers. Multiple clients were used with each policy definition and resources.

choose to use when configuring policies and custom LDAP attributes. Currently there are only two classes of resources supported, websites, and file shares. So if you plan on protecting resources other than HTTP, HTTPS, and SMB, you may run into a hurdle. Rohati, however, has shown they are willing to work through and provide solutions for unique scenarios.

Verdict

Rohati has done a good job in creating an effective solution for wrapping security into systems that may be lacking. This seems a good choice for applications and resources that don't already have great authorization and authentication. Although Rohati is planning a TNS 500 device to be released for in-line deployment later this year, integration may prove difficult in an organization of large size. The TNS 100, however, is a great solution for medium to small businesses that are looking to get an early start on centralized authorization.

EMAIL SECURITY

Astaro Mail Gateway 4000

REVIEWED BY JOEL SNYDER

Astaro

www.astaro.com

Price: **$7,995 plus $3,945 for security subscription**

Network firewall vendor Astaro has widened its portfolio with the introduction of the Astaro Mail Gateway, an antispam/antivirus security appliance.

We tested the AMG 4000, the largest of four Mail Gateway appliances, and found it well-suited for the small business market with an easy-to-use management system, appropriate feature set and reasonable antispam performance.

Antispam B

We looked at how well the AMG fared in a real-world test of 10,000 live email messages. Astaro has positioned itself against Barracuda, with a similar feature set and market focus.

We tested sending the same messages through both gateways as they entered our network, with similar results. The AMG caught between 76 percent and 94 percent of spam compared to Barracuda catching between 83 percent and 90 percent. The range of numbers is because both gateways use the concept of "suspected spam," so the figures depend on whether you consider suspected spam to be spam or not. Based on an easy-to-configure policy, the system manager can set spam and suspected spam to be dropped, passed through and tagged, or quarantined. Both gateways had a similar positive false positive count, with Astaro in the range of 7 to 37 messages and Barracuda in the range of 31 to 33 false positives.

Compared to other gateways, though, Astaro could use some work. For example, we also looked at Trend Micro's InterScan Messaging Security Suite, and had a higher spam catch rate of 97 percent and a lower (18) false positive count.

Testing methodology: We integrated the AMG 4000 into our production email stream, sending 10,000 messages through the AMG 4000 over about a week.

User Features A

The AMG comes out of the block with a nice set of end-user management features. End users will receive daily quarantine reports (if the system manager enables them) by email, with single-click links to release messages. Or, end users can log into a simple Web portal at any time to see their mail logs, quarantined messages, and to manage a trusted sender list.

System Management & Integration A-

The easy-to-use Web interface helped us integrate the AMG into our email network in less than an hour. Linking the AMG to an existing email server, especially Microsoft Exchange, is very straightforward. One of the issues with external antispam gateways is transferring and keeping the email directory updated on the external gateway. Astaro has several mechanisms to do this, and has put in special support to ease synchronization between AMG and Active Directory.

If you want to let users see their quarantine and mail logs, you'll also have to authenticate them, which Astaro made easy with links via LDAP, RADIUS and even TACACS servers. Astaro's directory synchronization and authentication makes life easy for the network manager.

Astaro offers good reporting and mail monitoring, with several levels of instantaneous reports, easy log and quarantine searches, and automatic generation of executive summary reports. What is missing is the ability to dive deeper into each message. The information you might want in order to debug problems is present in separate text-based log files, but none of this is linked to the easy-to-use GUI-based logging. We also found that some of the reports don't add up. For example, although we sent more than 10,000 messages through the AMG, the summary reports only showed about 7,500.

Verdict

An outstanding first offering, the Astaro Mail Gateway should be on the short list of anyone for a simple, small business anti-spam gateway.

EDITOR'S DESK

PERSPECTIVES

FACE-OFF: BRUCE SCHNEIER VERSUS MARCUS RANUM

MANAGING SECURITY IN A RECESSION

UNDER PRESSURE: 2009 PRIORITIES

GOOD SECURITY ON THE CHEAP

PRODUCT REVIEWS

SPONSOR RESOURCES

ADVERTISING INDEX

the Academy **35**
www.theacademyhome.com

- Free infosec videos for security professionals from network admin to director of IT
- Free information security videos for home users/end users

ISACA **28**
www.isaca.org

Lumension **12**
www.lumension.com

Minimizing Security-Related Total Cost of Ownership

RSA Conference **20**
www.rsaconference.com

SearchFinancialSecurity.com **38**
www.SearchFinancialSecurity.com

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

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

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

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

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

SR. VICE PRESIDENT AND GROUP PUBLISHER
Andrew Briney

PUBLISHER Jillian Coffin

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

PRODUCTION MANAGER Patricia Volpe

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

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Neil Dhanowa ndhanowa@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Suzanne Jackson sjackson@techtarget.com

Meghan Kampa mkampa@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

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

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

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

TechTarget®
The IT Media ROI Experts

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