

INFORMATION **SECURITY**

APRIL 2010

ENDPOINTS ON THE LOOSE

Mobile and portable storage
devices are busting out
and putting data at risk



SOPHOS

- ☒ Malware Protection
- ☒ Data Protection
- ☒ Business Productivity
- ☒ IT Efficiency
- ☒ Compliance
- ☐ Hospital food



SECURITY SO SIMPLE YOU FEEL
INVINCIBLE

WORRY LESS. ACCOMPLISH MORE. WWW.SOPHOS.COM

SOPHOS
simply secure

FEATURES

19 Target: Portable Storage Devices

ENDPOINT SECURITY Security of endpoints such as thumb drives, SIM cards and mobile devices can no longer be ignored. Today's workforce is bringing these personal, portable storage devices into the workplace, and you need to manage and protect your organization's data.

BY LISA PHIFER

**28 Fending Off Fraud**

ANTI-FRAUD Today's anti-fraud technologies create gated communities for online banking.

BY JERRY SILVA

34 Strategizing for Better Times

PLANNING Security teams will continue to focus on efficiency and alignment with business when the economy improves. BY MARCIA SAVAGE

**15 FACE-OFF****Should the Government Stop Outsourcing Code Development?**

Is outsourcing code development a threat to national security? Marcus Ranum and Bruce Schneier go head-to-head on this topic.

BY MARCUS RANUM & BRUCE SCHNEIER



ALSO

4 EDITOR'S DESK**Two Steps Backward**

The firing of Pennsylvania's CISO because of his comments on a conference panel illustrates the continuing disconnect between management and information security.

BY MICHAEL S. MIMOSO

8 PERSPECTIVES**In the Cloud: What Lawyers Fear**

Be prepared to help legal teams overcome concerns about cloud computing. BY JULIE TOWER-PIERCE

11 SCAN**Troyak Shutdown Has Cybercriminals Playing Defense**

Shutdown of ISP has helped slow spread of notorious Zeus crimeware kit. BY ROBERT WESTERVELT

13 SNAPSHOT**Botnets Tap Out****42 Advertising Index**



Secure your business in
15 MINUTES.
Get around-the-clock protection.



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

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

McAfee Secure in 15 toolkit:

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

Visit www.mcafee.com/mid/secure15





Two Steps Backward

The firing of Pennsylvania's CISO because of his comments on a conference panel illustrates the continuing disconnect between management and information security. BY MICHAEL S. MIMOSO

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

I MET BOB MALEY a year ago at Black Hat when a mutual friend introduced us. I'd learned about him 18 months earlier when former colleague Dennis Fisher interviewed him in the pages of *Information Security* magazine. His was a noteworthy story; [Maley, CISO of the state of Pennsylvania at the time, built the state's information security program from nothing](#). In four years on the job, Maley oversaw an overhaul of ancient security policies for the state's 47 agencies. He brought in intrusion prevention technology to the state's networks and introduced identity and access management in order to get a handle on who was doing what with the state's digital assets. He did outreach with the security community in order to stay abreast of what was happening in a very fluid environment, and took what he learned to best introduce security concepts to the state government culture.

And that [outreach cost him his job](#) and smudged all that good work.

Maley took part in a panel at the recent [RSA Conference](#) alongside other state CISOs. He made a mistake during the discussion and talked about someone circumventing a state Web application to send driver's license applicants to a particular driving school that said it would facilitate quicker license exams.

Reports say Maley, who took vacation time to attend RSA, shared very little detail about the intrusion and only did so in order to illustrate a point he was making on the panel.

According to state spokespeople, this is a policy violation; state officers must get permission to publicly discuss state matters. This trip-up apparently cost Maley his job.

Looking beyond what this means to Maley and his family, this is a travesty for the information security industry. Talk about taking two steps backward. The irony of the situation is that the conference room where Maley made his misstep was a scant hundred yards away from the keynote room where none other than cybersecurity coordinator Howard Schmidt and FBI director Robert Mueller made very public pleas for information sharing for the greater good.

Yeah right. Nice try. Tell that to Bob Maley.

The short-sighted people responsible for Maley's dismissal have stuck a dagger in the sharing business and the greater good business. Why would any of you dare sit on a panel and talk about attacks, disclosure, research or anything else that teeters on the line of titillating? Why would you, if you're Google for example, blog about the Aurora

Reports say Maley shared very little detail about the intrusion and only did so in order to illustrate a point he was making on the panel.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

attacks or the Chinese hacking into Gmail accounts? If you're Adobe, why talk about a foreign government trying to poke around to get at your source code? If you're a defense contractor, could you imagine again sharing details about stolen jet fighter blueprints? Nope. Look at what happened to Bob Maley. "That's not happening to me," you'd collectively say. And no one would blame you.

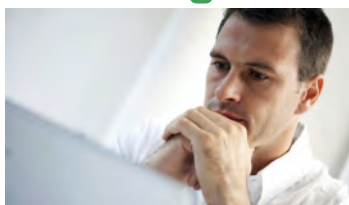
Now let's not relieve Maley of blame; he screwed up. He violated policy. But is it a firing offense? Take him out to the figurative wood shed and let him have it behind closed doors. Make it understood that this isn't the way to do things, sure. Suspend him if you must. But to let him go and send this message is unconscionable. It wasn't thought through. And it illustrates the disconnect that still exists between information security and decision makers. It illustrates that companies and governments, no matter their size, still don't put a premium on information security.

I'd imagine Bob Maley made a difference to the state of Pennsylvania. And he was trying to make a difference to his profession. But the management that's supposed to support him let him down and let him go. Misguided decision makers and bureaucracy got in the way of a security professional doing his job—again. Just when we think we're taking steps forward in information security...

Michael S. Mimoso is Editorial Director of the Security Media Group at TechTarget. Send comments on this column to feedback@infosecuritymag.com.

COMING IN MAY

Database Activity Monitoring



Database Activity Monitoring (DAM) is emerging as a powerful and effective tool for both security and compliance. With the ability to monitor all database activity, including administrators, and alert on policy violations, database activity monitoring tools offer an unparalleled ability to protect our most sensitive assets, without interfering with business process. But not all tools are created equal, with fundamental differences in architectures, database support, blocking capabilities, and performance. We'll explore the inner workings of these tools and make specific recommendations on evaluating, purchasing, and deploying database activity monitoring.

Windows 7 Security



No operating system will ever be totally secure and while Microsoft has been lambasted for its lack of security in the past, it continues to provide improvements and changes to its software that increase security. In this feature, we'll look at the security features of Windows 7, including an Encrypting File System that now supports Elliptic Curve Cryptography (ECC), less cumbersome User Access Control and an improved AppLocker to control what applications can be installed on users' computers. We'll also discuss DirectAccess, a new connection capability in Windows 7 that securely connects remote users to enterprise apps.

Supply Chain Security



With many organizations relying on an ever-growing network of business partners, and growing regulatory compliance requirements for contractors and suppliers, third-party security has become a priority. This feature will provide a checklist for managing your business partners for supply chain security.

In every issue:

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

MUST READ!

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

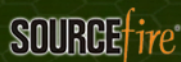
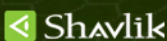
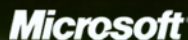
Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a firehose'.

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

Check out The Academy Pro at
www.theacademypro.com

the academy pro

Sponsored by:



www.theacademypro.com

The Academy Pro © Owned by Black Omega Media Group Incorporated



In the Cloud: What Lawyers Fear

Be prepared to help legal teams overcome concerns about cloud computing. BY JULIE TOWER-PIERCE

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

LAWYERS ARE ABUZZ over cloud computing. Though offsite data storage and services are hardly new concepts (think Skype or Yahoo Mail), the eyes of the law, which traditionally trail well beyond technology, are nervously fixating on cloud computing, or generically speaking, distributed online services such as SaaS (software-as-a-service), IaaS (infrastructure-as-a-service) and PaaS (platform-as-a-service).

As companies look to cut costs and gain flexible, convenient access to services and massive storage/data backup options, burgeoning interest in cloud computing solutions is understandable. But “computing in the cloud” is rife with legal mystery—*ahem*, fear of unknown and uncertain legal risk.

Understanding the mechanics and practicalities of how cloud computing works and how moving to the cloud legally impacts clients and corporations are just the tip of legal concerns over cloud computing—after all, *what you don't know might kill you* or at the very least, pose serious corporate risks. This lack of technical understanding, combined with a hotbed of fears over privacy, viability of the Fourth Amendment (constitutional safeguard against unreasonable searches and seizures) in the cloud, unbeknownst government meddling, third-party access, international sovereignty, security, forensic collection and e-discovery, disaster recover, and the absence of established legal precedent (i.e., case law), can derail even the best laid information security and technology plans for implementing cloud solutions, such as enterprise adoption of Google Apps.

Concern and caution hovering over cloud computing may be both misguided and reasonably justified. Demystifying Web-based applications and services, and the risk/security of cloud computing is key to removing barriers to the cloud. For starters, lawyers may need help understanding “the cloud,” namely how it works, where data resides and the complexities of data storage, access, retrieval, and security to better assess legal risk. As if understanding technology—such as local data storage and security issues, and application of existing law weren't challenging enough—cloud computing adds yet another layer of complexity and challenge for lawyers looking to insulate corporations and businesses from litigation risk. They may want assurances about the integrity and privacy of data, especially when it's

Demystifying Web-based applications and services, and the risk/security of cloud computing is key to removing barriers to the cloud.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

stored across the country or globe, while they await concoction of new regulatory cloud computing schemes or amendments to existing laws, such as to the Electronic Communications Privacy Act (ECPA) or the Computer Fraud and Abuse Act (CFAA). Of course, lawyers may also be on the lookout for clarity when it comes to understanding how security or privacy can actually be better in the cloud, especially in light of recent newsworthy hacks.

Information technology and security professionals who interface with lawyers and non-technical management are positioned to squelch many cloud concerns. By using straightforward, practical explanations and real-world analogies/examples, minus excessive technicalities when possible, you can impart a firm understanding of the mechanics of cloud computing and help lawyers gain perspective. With your technical prowess, you can help legal and non-technical management make sense of thorny issues like data privacy and unauthorized third-party access. For example, if your company is considering a migration to Google Apps, but is encountering push-back due to concerns about third-party access, unreasonable government intrusion or seizure, or disaster recovery, you can play a pivotal role in helping lawyers or management understand how data is stored or handled (e.g., encryption), the practicality of access by third parties, and technical processes in place to handle unforeseen risks. You'll need to make sure a cloud service provider gives you answers to these questions. The end result, of course, being that you can more easily accomplish your technical and security objectives.

You can also head-off or anticipate management "what-ifs" related to computing in the cloud. For example, if legal is concerned that a government warrant or subpoena served on a cloud computing data center could disrupt your company's access to services, make it known what precautions are set in place to prevent disruption. Again, you'll need to make sure the service provider provides these details. If cloud concerns center on disaster recovery, discuss the processes in place that mitigate risk; perhaps talk about how cloud vendors like Google and Amazon can offer assurances that their services are designed with disaster recovery in mind. You can also talk lawyers and management through risk anxiety of cloud technology and help shape policy by addressing issues such as the need to conduct a forensic analysis of data stored in the cloud, or what happens if the integrity of the data is compromised by the storage medium such that it loses value in court.

Sure, maybe you didn't go to law school, but you have the real-world technical savvy that can prove instrumental to helping lawyers litigate and shape the development of sound and workable cloud computing law, as well as corporate policy. In many ways, you are a powerful player in driving away fears, substantiated or not, that would otherwise impact acceptance and comfort of new technologies. So, go ahead, let your voice of technical reason resonate in the law. •

Julie Tower-Pierce is an attorney, past professor of cybercrime & cyberlaw, and co-author of Virtual Incorporation. Send comments on this column to feedback@infosecuritymag.com.

what drives *your* approach to IT security?

Balancing business priorities
and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our **ISO 17799/27002 Compliance Program** helps you to focus resources on your most important business risks and comply with regulations such as **Sarbanes-Oxley, FFIEC, HIPAA, PCI, and Gramm-Leach-Bliley**. Best of all, our approach works equally well for “Main Street” businesses and the Fortune 500 clients we’ve proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

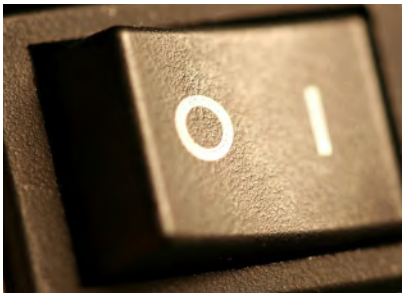
- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

Analysis | BOTNETS

Troyak Shutdown Has Cybercriminals Playing Defense

Shutdown of ISP has helped slow spread of the notorious Zeus crimeware kit.

BY ROBERT WESTERVELT



MANY EXPERTS in the security industry are speculating why Kazakhstan-based Troyak.org, the ISP serving a large chunk of the Zeus botnet, [suddenly went dark March 9](#), severing the ties between thousands of zombie machines and the command-and-control servers they use to receive their marching orders.

Whether the shutdown is a mixture of efforts by law enforcement and anonymous security researchers, or the action of the ISPs that service Troyak is anyone's guess. But experts says the activity appears to be throwing a wrench in spam and phishing campaigns and slowing the spread of different malware variants of the nasty Zeus crimeware toolkit, which has been a serious problem for the banking industry.

"There appears to be an ongoing effort to keep Troyak shut down, which is encouraging and definitely the right approach," says Sean Brady, a global expert on issues and mitigation strategies related to online fraud at RSA, the security division of EMC. "Right now the fraudsters are spending time, money and resources to get online and that is time, money and resources not being spent on fraud activities."

In studying the demise of Troyak, Brady found the ISP to be connected to a spider web of malware networks that work to ensure that the connection to their malware servers remains active. RSA's FraudAction Research Labs uncovered eight malware hosting networks and five upstream providers that use legitimate ISPs to connect to the Internet. In addition to Zeus Trojans, the servers host the RockPhish phishing toolkit, JabberZeus instant messaging drop servers and the Gozi SSL data stealing Trojan. He says cybercriminals, tied to crime gangs in various eastern European

"Right now the fraudsters are spending time, money and resources to get online, and that is time, money and resources not being spent on fraud activities."

—SEAN BRADY, a global expert on issues and mitigation strategies related to online fraud, RSA, the security division of EMC

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
SECURITY

FRAUD PREVENTION

RECOVERY
STRATEGIES

SPONSOR
RESOURCES

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

countries, may have taken years to build out their networks.

"What has happened is that the fraudsters are using their networks and rerouting their traffic in an ongoing, unstable effort to remain connected," Brady says. "Whoever is behind taking Troyak down is also cutting more threads to the spider web they've created. There is an ongoing effort to keep addressing the other connections."

Other experts are not so convinced that the cybercriminals are on the run. They point out that historically, once a botnet is crippled, the bot herders have been able to find new servers to rebuild their networks and reconnect to create a new armada of infected machines. In 2008, the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for maintaining the Internet's domain name system, de-accredited EstDomains, an Estonia-based ISP known for harboring malware and spam. The lesson learned for cybercriminals at that time was to not host malicious domains with a single service provider. In the same year, another rogue ISP, [McColo](#), had its connections severed by its upstream providers. McColo hosted command and control servers running the Srizbi spam botnet. Spam volume temporarily declined, but has since rebounded, exceeding the levels prior to McColo's demise.

The action against Troyak may be a step in the right direction, but cybercriminals have demonstrated that they can quickly turn to other illegal activities, putting security teams in a constant game of whack-a-mole, says Gunter Ollmann, vice president of research for Damballa, a security vendor that sells botnet detection and prevention services.

"It's ineffective in the long run unless you remove and shut down all the command-and-control servers simultaneously," Ollmann says. "There are thousands of botnet operators and each of those operators run multiple botnet campaigns, so it's very difficult to gain complete control of a botnet."

But it's not necessarily about gaining complete control, says Adam Rice, chief security officer of Mumbai-based Tata Communications Ltd., India's largest tier-1 ISP. It's about disrupting the cybercriminal community, making it more costly for them to route their malicious traffic, he says. Microsoft's legal action in February to shut down the command-and-control network of the [Waledac botnet](#), a notorious spambot that produces an estimated 1.5 billion spam messages daily, is an example of the kind of disruption that puts cybercriminals on the run, he says.

"The ability to do that kind of disruption exists right now," Rice says. "I think that right now, it's not a real big secret to anybody where a lot of this bad traffic originates, where it's going and who does what to whom."

"There are thousands of botnet operators and each of those operators run multiple botnet campaigns, so it's very difficult to gain complete control of a botnet."

—GUNTER OLLMANN, vice president of research, Damballa

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

Botnets Tap Out

ISPs AND TECHNOLOGY companies such as Microsoft are taking aim at spam- and malware-spewing botnets and the service providers hosting their command-and-control (C&C) servers. Recently, proactive action took down the Waledac botnet and temporarily disrupted the nasty banking Trojan, Zeus. Here's a recap:

—Information Security staff

Waledac • Dubbed [Operation b49](#), Microsoft was able to disconnect virtually all C&C communication to the Waledac botnet, one of the most prolific spreaders of spam and malware. A cooperative Virginia judge signed an order on Feb. 22 allowing Microsoft to disable nearly 300 Waledac domains. Waledac is believed to be part of the Storm botnet and acted as a dropper for the Conficker worm.

Troyak/ Zeus • The mysterious March takedown of Troyak.org, a Kazakhstan ISP, disrupted the dangerous Zeus botnet. Zeus is a family of malware that primarily targets users' banking credentials and other sensitive data. Troyak, the Russian word for Trojan, reportedly hosted 25 percent of Zeus' command and control servers.

Mariposa • The [Mariposa botnet](#), 13 million computers strong, was taken down in December. Three Spanish men, operators of the botnet's C&C servers, were arrested before Christmas after authorities contacted the hosting provider who cooperated in the takedown. Police and courts in Spain authorized officials to change DNS resolution records so that infected computers would no longer talk to the C&C servers—a take on DNS cache poisoning. Authorities were able to track the men responsible via an IP address when one forgot to VPN into the C&C server.

McColo • The [granddaddy of all takedowns was McColo](#). In November 2008, two ISPs cut off hosting provider McColo, based in San Jose. McColo was the genial host for several large botnet command-and-control servers, and the take down according to security companies such as Arbor Networks caused spam levels to dip by as much as 75 percent. However, [it didn't take spammers long to find new hosts](#) and spam levels quickly shot back toward pre-McColo levels.

OVER-
HEARD



“Don't tell me about the pains you have in determining what has to be fixed, I don't care. You're in the software business, you're writing code, that's what you're supposed to do. If you can't handle it, get out of the business.”

—TIM STANLEY, director of information security, Continental Airlines
to Microsoft, Adobe and other software vendors.

WE'LL GET
YOUR IT SYSTEMS
TO TALK...



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

OPTICS FOR SECURITY INFORMATION MANAGEMENT IS AN AFFORDABLE AUTOMATED LOG MANAGEMENT SERVICE THAT CENTRALIZES, ANALYZES AND RETAINS LOG DATA AND HELPS YOU USE IT TO SUPPORT BUSINESS FUNCTIONS. SCALABLE TO 100% OF YOUR LOG DATA, SO YOU CAN REST EASY, GLASSHOUSE HAS GOT YOU COVERED.

FOR MORE INFORMATION CONTACT: SECURITY@GLASSHOUSE.COM

WWW.GLASSHOUSE.COM

 **GLASSHOUSE**



Should the government stop outsourcing code development?

POINT *by* **MARCUS RANUM**

BEFORE WE get started, I need to confess my biases and background: I've been a coder, project leader, VP of engineering, CTO and CEO—I've held every job in the software task tree that exists in a software company. I'm going to make a few assertions in this column that I won't have room to back up in detail, but they're facts and you should accept them as such. Most of what we need to know for this discussion is summarized in this observation by the co-inventor of the buffer overflow, Brian Kernighan [<http://www.cs.princeton.edu/~bwk/>]: "Debugging is twice as hard as writing the code in the first place. Therefore, if you write the code as cleverly as possible, you are, by definition, not smart enough to debug it."

Finding security holes in software is harder than debugging. And finding a hidden security trapdoor in software would be even harder.

So it follows from this assertion that if you don't know how to write code at all, you're lunchmeat if anyone, anywhere, is able to inject malicious code into your software supply. In fact, the current primary mode of software production (please don't call it "engineering") is the "mashup"—a process by which applications are constructed out of other live applications, which are often large conglomerates of other applications, etc. The result is a software supply chain in which processing is dynamic and the behavior of a high-level program can be changed by

the owner of one of its components. Simply put, that means that whoever owns code you depend on, owns your data.

The operating environments of choice today operate similarly—the device driver for your USB keyfob or graphic card was written by a contractor to a subcontractor; it runs in kernel space and can access any process currently running in system memory. Whoever owns your device driver owns your keyboard, your hard drive, and your encryption keys—and, often, nobody knows who that is because it came with the hardware's OEM bundle.

In short, we talk like we're concerned about data leakage and information security, but our behavior says otherwise. And it's interesting to watch how the rest of the world has been dealing with the same problem. For the foreign powers, it was the fact that everything, eventually, is touched by code from Microsoft and microcode from Intel. It's every counter-intelligence officer's nightmare: all your secrets are eventually handed over to a trade secret—a protected mass of software and hardware produced by a country that has its own history of playing dirty

"We talk like we're concerned about data leakage and information security, but our behavior says otherwise"

—MARCUS RANUM

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

tricks with technology. In the early 1990s, the Europeans made a few muted whimpers about the topic, but since then it seems everyone has fallen silent.

But now—if we're smart—it's our turn to worry. Nobody in the government writes software, anymore—it's all outsourced. And because of the push toward using commercial off-the-shelf (COTS) software wherever possible, there's no dividing line between specialized code that does something important and the general-purpose code that automates an unclassified supply chain application—it's all the same stuff, from the same people, and it's being fielded to non-programmers. That's the part where it all breaks down—someone who doesn't know how software works (at least well enough to write it) doesn't know enough to tell if software might be misbehaving. "It works" is the only criterion non-programmers are *capable* of holding the software to. If you're not a programmer, you can't even imagine all the possible covert channels I could come up with to leak data through your firewall. We're beginning to see the size and shape of the elephant, thanks to malware writers and bot-herders, but I think the immortal words of Kurt Vonnegut are appropriate here: "Everything will get unimaginably worse and never get better again."

We're in the early stages of the government's IT death-spiral; it's impossible for the government to attract the kind of technical people it needs because they can make three times as much as contractors doing the same work, which means outsourcing is now the only option that remains. But here's the problem: you need experienced programmers to at least glance at a code deliverable to see if it's any good and to verify if the contractors actually accomplished what they were supposed to. So what do you have all over federal IT, today? Contractors reviewing other contractors' work to judge whether it's acceptable. The *only* way to tell if you've bought a load of crappy code is to have a good programmer look at it (because a bad programmer will look at it and think "I can learn from this...") You *cannot* be in the IT business without good programmers at the top of your technical food-chain.

What does it mean? It means that if I could say one sentence to Barack Obama, it would be, "Sir, our government's extreme reliance on outsourcing software development to third parties is a threat to national security."

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

COUNTERPOINT by **BRUCE SCHNEIER**

INFORMATION TECHNOLOGY is increasingly everywhere, and it's the same technologies everywhere. The same operating systems are used in corporate and government computers. The same software controls critical infrastructure [<http://www.schneier.com/essay-140.html>] and home shopping. The same networking technologies are used in every country. The same digital infrastructure underpins the small and the large, the important and the trivial, the local and the global; the same vendors, the same standards, the same protocols, the same applications.

With all of this sameness, you'd think these technologies would be designed to the highest security standard, but they're not. They're designed to the lowest or, at best, somewhere in the middle. They're designed sloppily, in an ad hoc manner, with efficiency in mind. Security is a

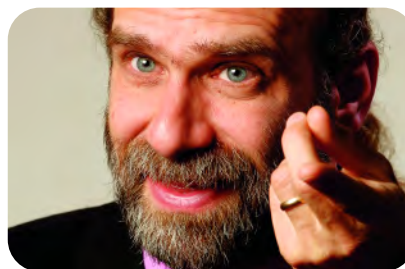


TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

"Code isn't magically more secure when it's written by someone who receives a government paycheck than when it's written by someone who receives a corporate paycheck."

—BRUCE SCHNEIER

requirement, more or less, but it's a secondary priority. It's far less important than functionality, and security is what gets compromised when schedules get tight.

Should the government—ours, someone else's?—stop outsourcing code development? That's the wrong question to ask. Code isn't magically more secure when it's written by someone who receives a government paycheck than when it's written by someone who receives a corporate

paycheck. It's not magically less secure when it's written by someone who speaks a foreign language, or is paid by the hour instead of by salary. Writing all your code in-house isn't even a viable option anymore; we're all stuck with software written by who-knows-whom in who-knows-which-country. And we need to figure out how to get security from that.

The traditional solution has been defense in depth: layering one mediocre security measure on top of another mediocre security measure. So we have the security embedded in our operating system and applications software, the security embedded in our networking protocols, and our additional security products such as antivirus and firewalls. We hope that whatever security flaws—either found and exploited, or deliberately inserted—there are in one layer are counteracted by the security in another layer, and that when they're not, we can patch our systems quickly enough to avoid serious long-term damage. That is a lousy solution when you think about it, but we've been more-or-less managing with it so far.

Bringing all software—and hardware, I suppose—development in-house under some misconception that proximity equals security is not a better solution. What we need is to improve the software development process, so we can have some assurance that our software is secure—regardless of what coder, employed by what company, and living in what country, writes it. The key word here is "assurance."

Assurance is less about developing new security techniques than about using the ones we already have. It's all the things described in books on secure coding practices. It's what Microsoft is trying to do with its Security Development Lifecycle. It's the Department of Homeland Security's Build Security In program. It's what every aircraft manufacturer goes through before it fields a piece of avionics software. It's what the NSA demands before it purchases a piece of security equipment. As an industry, we know how to provide security assurance in software and systems. But most of the time, we don't care; commercial software, as insecure as it is, is good enough for most purposes.

Assurance is expensive, in terms of money and time, for both the process and the documentation. But the NSA needs assurance for critical military systems and Boeing needs it for its avionics. And the government needs it more and more: for voting machines [<http://www.schneier.com/essay-286.html>], for databases entrusted with our personal information, for electronic passports, for communications systems, for the computers and systems controlling our critical infrastructure. Assurance requirements should be more common in government IT contracts.

The software used to run our critical infrastructure—government, corporate, everything— isn't very secure, and there's no hope of fixing it anytime soon. Assurance is really our only option to improve this, but it's expensive and the market doesn't care. Government has to step in and spend the money where its requirements demand it, and then we'll all benefit when we buy the same software. •

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



Focused on finance?

Introducing SearchFinancialSecurity.com!

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

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

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

www.SearchFinancialSecurity.com



SearchFinancialSecurity.com

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

TechTarget
Security Media

 SearchSecurity.com

INFORMATION
SECURITY

INFORMATION SECURITY DECISIONS

 SearchFinancialSecurity.com

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
SECURITY

FRAUD PREVENTION

RECOVERY
STRATEGIESSPONSOR
RESOURCES

TARGET:

PORTABLE
STORAGE
DEVICES

Security of endpoints such as thumb drives, SIM cards and mobile devices can no longer be ignored. Today's workforce is bringing these personal, portable storage devices into the workplace, and you need to manage and protect your organization's data.

BY LISA PHIFER

Thumb drives, removable memory cards and smartphones often carry business data without IT permission, oversight or protection against loss or theft. Unfortunately, these handy little portable storage devices can jeopardize gigabytes of sensitive information.

According to a study by Applied Research-West, three of four workers save corporate data on thumb drives, including customer records (25 percent), financials (17 percent), and business plans (15 percent). Yet fewer than half of businesses routinely encrypt thumb drives. Fewer still consistently secure data copied onto today's rising tide of consumer smartphones.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

Some companies underestimate business risk posed by unencrypted portable storage. Others acknowledge the risk but, in lean economic times, lack the budget to battle it. But these excuses could leave employers in hot water if a regulated data breach occurs.

"If [a portable device] carries customer or payment information, you have to protect it, no matter who owns it," says Mark Jordan, senior product manager at Sybase. "If you can't afford to manage and secure it, don't store sensitive data there. It's a cost versus liability decision; even one breach could bankrupt a small company."

With laptop full disk encryption (FDE) on the rise [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1303839,00.html], the next step is to plug these smaller data leak points. A holistic strategy for protecting data, no matter where it lives, is optimal. But portable storage is used differently, requiring tweaked policies and tools. The trick is to achieve consistent data protection while mastering the unique challenges posed by thumb drives, removable memory cards and smartphones.

"If [a portable device] carries customer or payment information, you have to protect it, no matter who owns it. If you can't afford to manage and secure it, don't store sensitive data there. It's a cost versus liability decision; even one breach could bankrupt a small company."

—MARK JORDAN, senior product manager, Sybase

COMPLIANCE DEMANDS MORE THAN ENCRYPTION

Regulatory compliance tends to drive portable storage protection projects [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257108,00.html]. From Sarbanes-Oxley Act (SOX) and the Federal Information Security Management Act (FISMA) to the California Senate Bill 1386 and Massachusetts Data Protection Act [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1380364,00.html], companies have plenty of motivation to stay out of breach headlines.

In April 2009, a single BlackBerry stolen from a hospital put 3,200 patient records at risk. In October 2009, one 4 GB thumb drive stolen from a worker's car exposed more than 15,000 community college student and employee records.

Unfortunately, breaches such as these are no longer rare nor limited to laptops.

"If I'm a compliance officer, responsible for keeping data private so that my company can thrive, I have to be thinking about not just my own machines, but data everywhere," says Sean Glynn, vice president of marketing at Credant. "My company is still responsible for that data and could face heavy fines if I can't report on its status."

But, from giveaway thumb drives to personal iPhones, many portable storage devices enter the workplace without IT approval.

"You could try to block those devices, but that horse has left the barn. Because it is executives who bring in the latest gadgets—executive bling—any policy that blocks

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

everything [unknown] quickly gets broken. Many of our customers are at the stage of auditing where data is going, trying to decide what to do," says Glynn.

Jordan counsels customers to consider all possible data loss vectors for each device. "Suppose a lost device is protected with FDE and restrictive passwords. That's great, but what happens when [a thief] removes that device's SD or SIM card? You have to make sure that everything is protected and that you can detect any attempted breach," he says.

Rigorous protection may also require more than native encryption. For example, "There's a perception that if you lock your BlackBerry, everything is encrypted" says John Jefferies, vice president of marketing at IronKey. "But the Mantech Crowbar [<http://cybersolutions.mantech.com/>] can snap the contents of a BlackBerry's SD card quickly, cracking a 4-digit PIN in 30 seconds."

While standalone media encryption is sufficient for some businesses, it may not satisfy auditors. In addition to centralized policy enforcement and reporting, "Some customers feel that they can't comply with SOX unless they can unlock a device to recover data if an employee leaves," says Jefferies. "Remote wipe and kill have also become increasingly important; the Massachusetts law mandates that functionality."

"There's a perception that if you lock your BlackBerry, everything is encrypted. But the Mantech Crowbar can snap the contents of a BlackBerry's SD card quickly, cracking a 4-digit PIN in 30 seconds."

—JOHN JEFFERIES, vice president of marketing, IronKey

DEFINE ACCEPTABLE USE POLICIES

Most people who find a thumb drive try to read it and then start using it to transport files. Smartphone purchasers usually synchronize contacts and email during setup. It is simply human nature to quickly copy a mixture of personal and business data onto these devices.

Risk reduction therefore begins with policies that govern acceptable use. Limit business data exposure by defining what can and cannot be copied onto each device and how that data may be stored, modified, deleted or shared with others. Identify how device status and data movement will be monitored and enforced, including scenarios in which IT may recover or delete business (and perhaps personal) data.

Tim Matthews, a senior director at PGP, recommends that policies assume multiple devices per worker—some IT-issued, some not. "Each person probably has one laptop, one phone, and several USB drives that they want to take home or share with partners and co-workers. These days, people often have at least two or three USB sticks, plus a terabyte removable drive [for backup], that are not provisioned by IT."

Even business phone procurement seems to be changing. "The trend now, based on consumerization and cost, is to let employees buy their own smartphones," says Khoi Nguyen, group product manager, mobile security group, Symantec. "Some companies are giving employees a stipend toward whatever device they want to use.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

But once users choose their phone, they have to sign [an acceptable use policy] where they agree to install certain required software and to let IT apply certain policies.”

Given device proliferation, Ram Krishnan, senior vice president of products and marketing at GuardianEdge, recommends defining policies to control data flow. “Define granular blacklists or whitelists to restrict data transfer onto *any* removable media,” he says. “In addition to [device] types, makes, and models, specify [permissible] port and file types—for example, letting presentations but not spreadsheets be copied [via] USB.”

To promote compliance, policies should reduce data risk while minimizing user impact. For example, Jesper Sveiby, product manager for Check Point Software Technologies mobile security solutions, suggests defining very selective encryption policies for smartphones and SD cards. “Customers often encrypt

calendar/contact files but leave the rest unencrypted, because users are very sensitive about anything that slows down their phone.”

On thumb drives, minimizing user impact might mean letting workers edit files on home PCs while automatically deterring offsite threat exposure. When thumb drives are used to share files with third parties, policies might mandate encryption in a way that does not require recipients to install decryption programs. For policies to be effective, common use cases such as these must be addressed, either by defining required practices or prohibiting unsafe activities.

“Customers often encrypt calendar/contact files but leave the rest unencrypted, because users are very sensitive about anything that slows down their phone.”

—RAM KRISHNAN, senior vice president of products and marketing, GuardianEdge

PORTABLE STORAGE MANAGEMENT OPTIONS

To implement policies that protect business data, portable storage devices must be inventoried, configured, and monitored—no matter who owns them.

IT-issued smartphones were traditionally managed using OS-specific platforms such as BlackBerry Enterprise Server. But the iPhone’s popularity fostered growth in unified consoles that manage heterogeneous smartphones. Platforms from Credant, Good, GuardianEdge, Sybase, and Trust Digital can now be used to provision and enforce data protection policies on Windows Mobile, Symbian, iPhone, and (sometimes) Palm. Although encryption capabilities differ for each mobile OS, unified consoles can still provide a single point of control and reporting—for example, to quickly issue a remote data wipe command on any lost smartphone.

Centralized management also plays a critical role in protecting thumb drives. Some solutions are drive-centric, for example, IronKey, Kanguru, and Sandisk offer consoles to remotely provision, monitor and enforce data protection on their own thumb drives. Alternatively, vendors such as BitArmor, CheckPoint, PGP, Sophos, and Symantec sell consoles that deliver unified management across their thumb drive, laptop/desktop, and (sometimes) CD/DVD encryption products. Here again,

Data Protection: Should it be Device Dependent?

Vendors have different approaches to data protection on portable storage devices.

Patrick McGregor, CEO of BitArmor, argues that data protection should be device-independent. "We take a fundamentally different approach because, in the world of removable media, a device by device approach doesn't scale," he says. "We protect data from the moment it's created by applying a 'smart tag' that goes with the data when it's copied onto a USB drive or home computer. The idea is to make data self-defending."

BitArmor uses software to watch over data as it moves, enforcing access and encryption rules embedded in the tag. IT-managed PCs can run an installed Control Agent; third-party PCs can run a lightweight Control Sentry embedded with the data. As a result, protection is persistent when data is copied onto any kind of thumb drive a user might acquire or even Windows Mobile smartphones.

However, vendors such as IronKey advocate (inherently device-dependent) hardware encryption. "We design our own chips, encased in a solid metal device that's tamper evident/resistant, using hardware-generated crypto keys that never leave the device and true random numbers," says John Jeffries, vice president of marketing, IronKey. Hardware encryption can better defend against brute force and cold boot attacks, while being less dependent on host/OS integrity, he says.

But data protection depends not just upon robust encryption, but also attack-resistant authentication and key storage. For example, Windows password prompt software used by Kingston, Verbatim, and Sandisk made headlines when researchers found they could capture and replay unlock sequences exchanged between a PC and those thumb drives.

Smartphones can face similar issues. For example, some versions of the iPhone are vulnerable to native PIN-code and encryption bypass attacks. To prevent corporate data access by compromised smartphones, products such as Trust Digital now check device integrity before allowing each email sync.

In short, device choice directly impacts IT's ability to protect any data stored there. Organizations with low risk tolerance may ban business data on consumer-grade thumb drives or smartphones. Others may adopt hybrid policies that permit limited data storage on riskier devices, but require corporate-standard devices for more sensitive data. •

"We design our own chips, encased in a solid metal device that's tamper evident/resistant, using hardware-generated crypto keys that never leave the device and true random numbers."

—JOHN JEFFRIES,
vice president of marketing, IronKey

—LISA PHIFER

a unified console can streamline tasks that span multiple devices, such as revoking all of a given user's data access.

Consoles that manage smartphone and thumb drive security are not yet common, although Credant and GuardianEdge have already done so. This could become a growing trend as enterprises cut device-level management costs by refocusing on their most valuable asset: data.

CONTROLLING DATA MOVEMENT

Of course, another way to reduce loss or theft risk is to restrict the data copied onto portable storage devices in the first place. For this reason, many companies pair portable data encryption with port blocking.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

For example, Sophos SafeGuard PortProtector and SafeGuard RemovableMedia can be combined to secure data copied over interfaces such as USB, FireWire, Bluetooth, and Wi-Fi onto CDs, DVDs, and thumb drives. “First, PortProtector allows, blocks, or restricts portable media plugged into computers inside your network—for example, denying iPods or allowing only devices of a particular type or under a specified size limit,” says Nagraj Seshadri, Sophos product manager. “Then we encrypt data on the media itself, using key rings to easily share data with coworkers, partners, and customers while preventing [unauthorized] persons from reading it.”

Port blocking can also be used to restrict the files copied from a desktop onto a phone or its removable SD card via USB or Bluetooth. However, data synchronized over-the-air to smartphones is usually controlled by a separate system, such as a mobile device manager. This could result in data leaks if policies are not coordinated—for example, a user who can’t copy a spreadsheet onto his phone via USB might try to get it there as an email attachment instead.

Eventually, analysts expect portable data encryption to be paired with full-blown data leak prevention to enable content-aware filtering and encryption. Vendors that have already taken steps in this direction include Symantec and Trustwave (BitArmor and Vericept).

Finally, portable storage devices may contain malware that could be copied into the enterprise. “When Conficker spread [as an auto-run Trojan carried on thumb drives], it was no surprise to those of us who remember floppy malware propagation,” says Jefferies. To mitigate malware threats, consider read-only usage modes, drive-resident anti-malware programs, and auto-run disablement.

PROTECTING DATA AT REST

Ultimately, data copied onto portable devices can be encrypted to deter unauthorized access, from pod slurping on unattended drives to hacking lost or stolen smartphones. Among portable data protection products, AES support is now common, and many enterprise-class implementations are FIPS 140-2 certified.

This might seem straightforward, but the devil is in the details. Questions to consider when encrypting smartphone, memory card and thumb drive data include:

- Which files should be encrypted?
- Which keys should be used to encrypt them? and
- How are those keys created, stored, accessed and revoked?

For example, an encryption product may assign a different key pair to each user and group in the corporate directory. Whenever data is written to any thumb drive, policy determines whether encryption is required, and if so, which user(s) and group(s) should have access. As data is copied, it gets encrypted with a key that only allows decryption by the intended recipients. This makes it possible to share encrypted data with co-workers based on group affiliation. Users logged in with directory credentials won’t need to enter extra passwords. If a user moves from one group to another or leaves the company, directory updates will cause data access rights to change automatically.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

But what if a user wants to share encrypted files with someone not enrolled in the directory or edit encrypted files on a home PC? For sharing data outside the organization, users can often be given permission to apply an additional encryption password that they can give to recipients out of band. The password can be used to open the document off site, where it can be edited in place, using only the encryption environment carried by the drive. If and when that drive returns to the office, those files can still be accessed in the usual onsite transparent fashion. Some products can also create self-decrypting archives for files need only be protected in transit—for example, when mailing a CD or DVD to a trusted third party.

Smartphone data sharing may be less likely, but can still present performance and portability challenges. “We can encrypt data on the device itself and on memory cards. On the device, administrators can define secure folders or choose to encrypt PIM [application] files,” says Nguyen. “On cards, in addition to secure folders, users can define a special key to share a folder with another user or device.” But, unlike a thumb drive, that memory card can only be decrypted on another device running the same encryption solution—for example, when moving files to a replacement smartphone.

Another approach, applicable to thumb drives but gaining popularity on employee-liable smartphones, is the encrypted sandbox. As Jordan explains, “In terms of encrypting the entire device, Apple hasn’t given vendors the ability to really protect everything. Afaria can do things such as enforce stronger passwords or configure VPNs, but it cannot replace Apple’s hardware encryption.” For customers who find a phone’s native protection insufficient, “We can also create a secure sandbox with our Office Mobile product, taking your email, password-protecting it, and encrypting it to keep that data safe in our little corner of the device.” In fact, many customers use both approaches.

“We can encrypt data on the device itself and on memory cards. On the device, administrators can define secure folders or choose to encrypt PIM [application] files. On cards, in addition to secure folders, users can define a special key to share a folder with another user or device.”

—KHOI NGUYEN, group product manager, Symantec

REPORTING PROTECTION STATUS

Finally, a critical component of any enterprise’s data protection strategy is the ability to track status. “It’s more than being worried about security. To be compliant, you need to be able to report on protection status, data status, policy status, and device status.”

Centralized consoles serve as the conduit for making real-time status inquiries and generating historical reports, but the challenge can be gathering status and issuing commands to offsite devices—especially oft-disconnected thumb drives.

Some thumb drives carry agents that run upon insertion. For example, Nate

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

Cote, VP of product management at Kanguru, says, "Our drives call back [to our server] over an encrypted tunnel, saying 'Here's my ID. Am I still approved for use?' If so, the boot sequence continues with setting or program updates and information needed for reporting purposes."

Like Kanguru, Sandisk's agent can remotely kill lost devices or audit them for compliance purposes. But Sandisk also gathers information for recovery purposes.

"We maintain an audit log of all files copied/from the drive, so that IT can reproduce that drive. We can also set a return-to-base time after which users must log into the domain to backup logs and data," says Dror Todress, head of marketing.

But of course, thumb drives (and to a lesser extent smartphones) may be used in venues without Internet access. "If you're on an airplane, our [Sophos] agent will use previously stored policies," says Seshadi. "The next time you log in, the agent updates itself. If an agent hasn't contacted a management center for awhile, it gets locked out—not by wiping the device but by disabling the user's keys." To defend against offline password-guessing, Sophos applies an exponential delay after each attempt, with lock out after X-number of tries.

BitArmor uses its SmartTag agent to track data access at the file system level. "We log when a file moves to a drive, all file opens/closes/deletes, when that drive last called in," says McGregor. Those events can be reported to BitArmor's console or sent to a SYSLOG server for use with third-party report generators.

But not all products track data movement. For example, "PGP Portable can report when and where certain devices were formatted to be encrypted, so that if a stick is lost, you have proof it was encrypted," says Matthews. "But we encrypt the whole container, no matter what's inside, so we don't track what files/folders are on the media."

Portable data protection auditing and reporting approaches vary, but centralized control and visibility are key differentiators between standalone device encryption and solutions that can meet enterprise needs.

Another important consideration is TCO; how well does a given vendor's approach dovetail with a customer's infrastructure and operations. Many vendors have started to focus on this part of the equation, giving large customers better/broader systems integration while offering small businesses a pay-as-you-go "cloud management" option. Attributes like these will only become more important as portable data storage devices continue to proliferate, and privacy laws make it harder to ignore them. •

"We log when a file moves to a drive, all file opens/closes/deletes, when that drive last called in."

—PATRICK MCGREGOR, CEO, BitArmor

Lisa Phifer is president of Core Competence [<http://www.corecom.com/>], a consulting firm focused on business use of emerging network and security technologies. Send comments on this article to feedback@infosecuritymag.com.

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. **Free.**

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.



www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.



www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.



www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.



www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.



www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.



www.SearchSecurityChannel.com

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES


SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
SECURITY

FRAUD PREVENTION

RECOVERY
STRATEGIESSPONSOR
RESOURCES

FENDING OFF FRAUD

Today's anti-fraud technologies create
gated communities for online banking. BY JERRY SILVA

IT IS NOW A WELL-KNOWN, new-millennium adage that “every time an institution builds a higher wall to fight fraud, the criminals just get taller ladders.”

This phenomenon not only continues to be true, but in addition to building taller ladders, criminals are also building more of them and expanding their targets. Looking for every chink in the walls, seeking out the edges and in areas that aren't as solid as they should be, fraudsters are making it much more difficult for financial institutions to build individual walls as point defenses against fraud.

Fortunately, there are technologies available in the online banking security market to create fortresses around vital assets. These new solutions are in part evolutionary versions of technology that has been around for a number of years, as well as new ways of looking at the

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

problem of fraud through dynamic analysis, and even non-technology processes that turn those individual walls into gated communities.

Read on for a closer look at these anti-fraud systems—the benefits they offer as well as some of their limitations.

THE NEIGHBORHOOD WATCH

In a neighborhood watch, a community comes together to create a vigilant system that keeps an eye on trouble before it has a chance to damage any property. There are systems available today that can look for certain behaviors and stop criminal activity by alerting subscribers to imminent threats so that they can arm themselves before an attack can be launched.

RSA, the Security Division of EMC, for example, markets its eFraudNetwork as such a watch system. This network monitors 150 countries for suspicious and known fraud threats including phishing, spoofed websites, and known sources of criminal activity, pulling that information into a shared database that is used by the company's clients as the basis for adding protection to their authentication and transaction monitoring systems. When a fraud pattern is identified in any of the eFraudNetwork members' systems, the network immediately stores the associated data (IP addresses, URLs, device information, account information, etc.) in a shared data store that is used by the company's real-time fraud detection solutions to watch for and catch the same pattern at other institutions. At the same time, RSA uses the information to shut down phishing sites through its partnership with ISPs and Web providers worldwide.

Fiserv also provides a similar neighborhood watch capability in its FraudNet product. Used in the area of bill payment, FraudNet looks for suspicious activity and known fraud events and uses that information in a shared manner to prevent fraud occurring in its CheckFree bill pay service. If a bill payment instruction is flagged as fraudulent in any of its members' systems, the FraudNet solution uses fraud information, such as user ID, IP address, and payee information to watch for similar patterns in the whole CheckFree

service. If a similar pattern is detected, the system can stop the instruction or provide the information to the institution for a secondary challenge to the user or even manually review before the transaction is committed. Subscribers to that service benefit from Fiserv's vigilance in deterring fraud before the fraudsters attack their institution. The company claims that 35 percent of all fraud detected in its bill pay service was found through the sharing of fraud information in the network.



The company claims that 35 percent of all fraud detected in its bill pay service was found through the sharing of fraud information in the network.

THE DEADBOLT

If an intruder does make it past the neighborhood watch, the next layer of protection is at the front door, where the criminal faces a lock. In the case of an online banking application,

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

this is the job of the institution's authentication system. While most consumers continue to use essentially the same authentication systems they have always used, mainly user ID and password, what goes on behind the curtain has become more sophisticated than ever. And in the business world, what was once sufficient to create stronger authentication—one time passwords or tokens, for example—is proving to be vulnerable to exploitation as well. To compound the problem, customers continue to ask for more authentication endpoints, both software and device based, and in-band and out of band systems.

Current authentication products add breadth of channels and a layer of intelligence to the authentication methodologies of the past. In addition to collecting second-level information like geography and IP information during the authentication process, today's technologies also bring in behavioral data to bear before authenticating a user, including typical access times and types of activity performed. In addition, the latest solutions are also based on a shared services model where risk information is shared between the company's customers, allowing them to use information from one institution to protect the whole community.

Because of the increasing breadth of endpoints available to the user today, many authentication systems are also expanding their reach across multiple origination points. By supporting a wide variety of devices, such as computers, traditional mobile devices and smartphones, and a variety of authentication methods such as certificates, hard tokens, and SMS-based one time passwords, authentication products from vendors like VeriSign and Entrust, to name a few, can make it easier for the institution to manage an enterprise-wide deployment using consistent technology and processes.

THE SURVEILLANCE CAMERA

When all else fails, and the criminal is able to bypass the neighborhood watch and door locks, it is up to real-time surveillance to capture fraud activity as it's happening but before any real loss occurs.

Most of today's fraud detection systems are based on capturing information from authentication all the way to transaction origination and using this and other information to flag any suspicious activity upon which the institution may want to act. While techniques may vary from vendor to vendor, the common goal of these systems is to score the activity as it occurs and deliver a risk score to the online banking application.

An example of the kind of troubling fraud techniques [http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1376286,00.html] anti-fraud systems are up against is the "man-in-the-browser" attack. In this specialized Trojan horse program, the fraudulent software interjects between the end user and the institution. While the Trojan



When all else fails, and the criminal is able to bypass the neighborhood watch and door locks, it is up to real-time surveillance to capture fraud activity as it's happening but before any real loss occurs.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

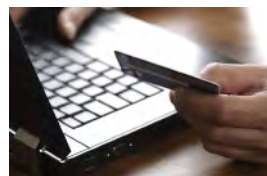
SPONSOR RESOURCES

horse presents what the user sees as a legitimate session in the browser, the program actually sends the institution different instructions altogether, changing transaction types, amounts, and account numbers to the bank. This type of fraud is extremely difficult to catch as it bypasses even some forms of strong authentication and it looks like a normal session to the end user. Even many fraud detection systems can be fooled since the user authentication was successful and the transaction looks normal as well.

But the latest fraud detection software uses behavioral analysis and intra-session monitoring to catch these kinds of attacks. Vendors such as ArcSight and Guardian Analytics provide real-time tracking of behaviors that take place from login to logout, capturing everything from the authentication to all transaction requests, monitoring how the user moves between pages, what business activities are being performed, and even tracking that activity from day to day as the systems “learn” user behavior. These kinds of systems can more easily catch man-in-the-browser attacks by monitoring the entire online banking session and comparing it against known good or normal user behaviors. The suspect sessions are then typically reported to the online banking application in order to either suspend the session or perhaps present a secondary challenge to the user before the transaction is committed.

As Craig Priess, vice president of products at Guardian Analytics puts it, “Sometimes what a user doesn’t do during a session is as important as what they do in order to establish a normal model of behavior.” The company’s FraudMAP product provides a predictive behavior analysis engine that relies less on rules and uses behavioral models instead. This approach allows the system to detect novel threats that have not been witnessed before and signals the institution through a high confidence score to the possibility of a threat. This type of method yields a second benefit to the industry as it inherently requires a smaller overhead to manage than rules-based approaches typically need.

Most of today’s fraud detection solutions are not exclusive to the online channel—they not only monitor for suspicious activity during the whole online banking session, but can also correlate this activity with behaviors from other channels, such as ATM, branch, and call center activity. As fraudsters continue to diversify their attacks, this kind of enterprise approach is critical to preventing more sophisticated threats that span the institution’s delivery network. A criminal may use customer information to call the institution’s contact center for balance or limit information, then use the online channel to transfer funds, and ultimately use card information to access funds at the ATM.



**“Sometimes
what a user
doesn’t do
during a session is as important
as what they do in order to
establish a normal model of
behavior.”**

—CRAIG PRIESS, vice president of products, Guardian Analytics

TUNED FOR BUSINESS

If the man-in-the-browser attack represents the increasing height of the fraud ladder, then certainly the increasing attacks against small businesses represents the building of more

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

ladders. More and more fraudsters are recognizing that there is profit to be made by seeking out the small business community and getting credential information through phishing, pharming, and malware. The result of this activity is that more of the fraud [http://search.financialsecurity.techtarget.com/news/article/0,289142,sid185_gci1411123,00.html] is moving from consumers to small business and from the top tier institutions into the regional and large community bank space.

This phenomenon requires that both technology and business knowledge be used to prevent the increasing danger to the small business market. Rules-based detection systems must have built in to them the concepts of business behaviors that are fundamentally different from consumer activities. The typical steps taken to originate an ACH payment or wire transfer, for example, are not found in the consumer paradigm. In addition, authentication in the small business and corporate cash management worlds are almost always different and stronger than found in the retail banking world—requiring technology solutions to support multiple authentication events during the same session, for example. For fraud detection and prevention solutions that use behavioral analysis, it is also important that the providers understand the business domain in order to architect, deploy, and support systems that can recognize the different behaviors between a \$5 million enterprise and a \$500 million dollar company.

LIMITING FACTORS

For banks, balancing security with customer ease of use is a constant concern. What's interesting is that many anti-fraud systems and initiatives do not seem to be deployed at the detriment of consumer convenience. Some authentication methods such as one-time passwords do inherently force the user to add a step to their normal login process, but few consumers or businesses complain about this added step as long as they understand it is being done for their protection. Likewise, financial institutions are walking a very balanced line when it comes to configuring the trigger point when a suspicious activity is flagged by a detection system. If the trigger is set too low, the user may be wrongfully denied a transaction, but most institutions are either erring on the side of the consumer, letting the users themselves set the appropriate triggers or setting a secondary challenge to the user instead of shutting them off altogether. These steps minimize any negative customer impact.

So why aren't more institutions deploying fraud detection systems today? A recent banking panel on online fraud detection and prevention highlighted the largest issue facing the financial services industry today when it comes to fraud prevention. Four representatives from both security and line of business areas at different institutions were asked if they intended to continue to invest in technologies to prevent the escalation of online banking fraud. The first panelist nodded vigorously, stating that his institution was indeed continuing to invest whatever funds necessary to keep fraud to an absolute minimum. The next two panelists agreed, pointing to customer satisfaction and brand trust as factors that were as important as real funds lost through fraud. The fourth panelist, however, did not only disagree, but he also stated that his institution would not spend a dollar more on fraud detection and prevention technologies until it could be proven that he would make that dollar back through fraud reduction.

At a cost of tens of thousands to millions of dollars to deploy, based on the numbers of active online banking users, few ROI models exist that can point to quantifiable savings

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

from reducing fraud that is escalating but difficult to measure in terms of potential damages. Hesitancy around the sharing of information between institutions on the actual size of the problem also prevents a group-think approach to solving the ROI problem. In response, many vendors are offering their technologies on a “software as a service” basis, reducing the initial capital expenditure needed to deploy anti-fraud programs, and making it easier for smaller banks to protect themselves.

In addition, many banks that do implement fraud detection systems are finding that the actual deployment of technology is usually only one part of a much larger fraud program that should also include system configuration, marketing, customer education, call center support, and enterprise fraud management resources. The total investment necessary in order to get quantifiably meaningful results goes well beyond the licensing of software. Those institutions that do not understand the total commitment are usually dissatisfied with current implementations and are reticent to invest further while many institutions that do understand the size of the commitment necessary to get substantial benefit from anti-fraud programs are understandably overwhelmed by the sheer size of the effort.



**Hesitancy
around the
sharing of
information between institutions
on the actual size of the problem
also prevents a group-think
approach to solving the ROI
problem.**

COMMUNITY EFFORT IS CRITICAL

It is apparent that today's technologies to help combat fraud are more sophisticated than ever, using strong authentication techniques, complex behavioral modeling, rules, shared data and dynamic responses to help the institution prevent losses from fraud. And most of these anti-fraud systems are designed in such a way that any foreseeable threat can be managed by tweaking the rules or configurations, in most implementations.

Many vendors have built anti-fraud solutions that are linked across multiple channels and even across multiple institutions, but only the larger anti-fraud providers such as Actimize have built fraud case management systems that institutions can deploy onsite. Case management systems can be implemented from non-fraud specific vendors like Pegasystems and SAS, but very few financial institutions are in a position to evolve to that step today.

However, in order to make a real dent in fraud reduction, online banking providers, fraud technology vendors, and institutions need to take a wider, shared approach to the problem and commit to combating fraud at the enterprise level and at the industry level.

In order to build an effective gated community, each member has to not only protect each individual home, but also contribute to the protection of the community itself. •

Jerry Silva is a principal at PG Silva Consulting [<http://www.pgsilva.com/>], bringing 25 years of financial services experience, and specializing in the acquisition and implementation of financial services technology serving both providers and institutions. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT
SECURITY

FRAUD PREVENTION

RECOVERY
STRATEGIESSPONSOR
RESOURCES

STRATEGIZING FOR BETTER TIMES

Security teams will continue to focus on efficiency and alignment with business when the economy improves. **BY MARCIA SAVAGE**

DURING THE DEPTHS of the recession last year, a global company with 1,700 employees laid off its three-member security department, along with half of its IT department, recalls Mark Kadrich, CEO of The Security Consortium, a security-services firm. "People who weren't directly associated with producing or supporting products were considered expendable," says Kadrich, who also is president of the Silicon Valley chapter of the Information Systems Security Association (ISSA).

At the other end of the spectrum, growing corporate recognition of the importance of security along with ever-present compliance requirements protected some security teams from the worst effects of the recession. In between, lots of CISOs and security managers were forced to put projects on hold and stretch tight budgets.

Now, with a few spotty signs of an economic recovery, what should security teams be doing to prepare for better times? What should they be focusing on to position themselves for success when a recovery takes full force?

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

Security professionals and industry experts say savvy security managers will take hard-learned lessons from the economic downturn to build better security for the future. The focus will still be on efficiency, with a sharp eye on aligning security efforts with the business and taking a risk-based approach as organizations weigh emerging technologies such as social media and cloud computing.

"The most important thing a chief security officer should be doing is working closely with their business counterparts and prioritizing security initiatives based on operational risk and satisfying compliance requirements," says Jonathan Gossels, president and CEO of security consulting firm SystemExperts. "The days of security for security's sake are past."

Let's take a look at how security teams fared during the recession and what security experts say they'll need to focus on moving forward.

MIXED IMPACT

How much of an impact the recession had on security departments depends on whom you talk to. Gossels says the impact was far ranging.

"Unlike the previous recessions we've seen where security was largely spared, this past recession took a toll," he says. "Many organizations went into survival mode. They hunkered down, froze spending and tried to retain critical staff."

Khalid Kark, vice president and principal analyst at Forrester Research, says the vast majority of security organizations experienced flat budgets and put future plans on hold. For example, companies tended to put the brakes on large-scale, multi-year projects such as identity and access management initiatives. However, many CISOs reported no cutbacks in their day-to-day running of security operations, he says.

"The realization persisted that you need basic security to survive, even during the downturn," Kark says.

In fact, some security professionals say security was largely spared from the ravages of the economic downturn. "One fundamental reason is that security isn't an option," says Jay Arya, a vice president and information security officer at Short Hills, N.J.-based Investors Savings Bank. "The problems—the bad guys and malware—are always going to be there."

The recession took its toll on the banking industry overall but that didn't change the compliance requirements banks face, including Gramm-Leach-Bliley [http://searchcio.techtarget.com/sDefinition/0,,sid182_gci951347,00.html] and the Red Flags Rule, [http://searchfinancialsecurity.techtarget.com/sDefinition/0,,sid185_gci1374703,00.html] says Tony Meholic, information security officer at Philadelphia-based Republic First Bank.

"The good thing was that information security wasn't as drastically affected as other areas, but the information security officer still had to be prepared to maintain compliance and security in the likelihood of not getting more budget," he says.



"The realization persisted that you need basic security to survive, even during the downturn."

—KHALID KARK, vice president and principal analyst, Forrester Research

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

Meholic says a growing recognition by the C-level of the need for security helped provide a buffer: "It's getting more apparent at that level that it's cheaper to have security built in, whether that's devices or staffing, rather than pay for a data breach."

Results from this year's (ISC)² Career Impact Survey illustrate the value placed on security within organizations despite a tough economic environment, says Hord Tipton, executive director of the nonprofit (ISC)², which issues the Certified Information Systems Security Professional (CISSP) and related credentials. More than half of the nearly 3,000 security professionals surveyed worldwide received salary increases last year. Among the survey's 1,800 U.S. participants, 11 percent saw their salaries cut and only 5 percent were laid off (*see "Bucking the Odds," p. 37*).

"There are a lot of good signs showing that security people have gained newfound respect," Tipton says. "They're being listened to, and at this point, compensated and retained."

OUTSOURCING

At the same time, however, half of the survey respondents reported that their information security budgets decreased somewhat or significantly in 2009. In the U.S., about 36 percent expect no change in their budget for this year. That's in line with *Information Security's* Priorities 2010 survey [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1380343,00.html], where 37 percent of respondents expect their budgets to remain flat this year.

Consequently, efficiency will continue to be the name of the game. For many organizations looking for ways to maintain security on a tight budget, outsourcing was a top option during the recession and the trend will likely continue, experts say.

"A lot of companies are focused on figuring out where they can create efficiencies. The first issue that comes up is, 'What is our core skill set and what can be handed over to other people who can do a better job of it?'" Kark says. "The average company may not have the skill set or competency to manage, monitor and respond to security threats on a 24x7 basis. If you have an outsourcer helping you with that, a lot of the minute details of the device monitoring goes to the managed security service provider."

Last year, companies that reduced security staff outsourced tactical and operational positions, leading to an increase in revenue of six to eight percent for managed security services, Kark says. CISOs then had the work of retaining an outsourcer, but managed to maintain specific skills and competency. According to a January Forrester report by Kark, the outsourced security market has grown from email and Web filtering to a holistic set of offerings, including vulnerability management, log aggregations, and analysis.

Organizations made a big push toward outsourcing because they "couldn't afford to not have security," Arya says.



"There are a lot of good signs showing that security people have gained newfound respect. They're being listened to, and at this point, compensated and retained."

—HORD TIPTON, executive director, (ISC)²

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

While outsourcing security operations such as penetration testing or vulnerability assessment was a good way for companies—particularly small and midsize businesses—to boost their security without having to add headcount, there were a couple of pitfalls, Meholic notes. Tight budgets might have forced some companies to look at smaller, less expensive managed security vendors, which can lead to some less-than-solid offerings.

“Everyone thinks they can provide these services,” he says. “The information security officer had to be able to discern quickly who the true professionals are.”

Also, the reliance on third parties made it imperative that companies have a robust vendor management program, and some SMBs were caught without having a repeatable process, Meholic says: “If you don’t have a proper vendor management program, you might engage a vendor that doesn’t have all the safeguards and controls. You’re exposing your company unnecessarily by doing that.”

SURVEY

Bucking the Odds

Security defies recession with salary increases and few layoffs, according to (ISC)² survey.

DESPITE A WORLDWIDE recession, many security professionals actually received raises last year and hiring is on the rise, according to the (ISC)² 2010 Career Impact Survey.

Of the nearly 3,000 survey participants worldwide, about 53 percent got raises in 2009. Among the survey’s 1,800 U.S. participants, 55 percent received pay increases. Only 4.8 percent were laid off globally; 5 percent in the U.S. lost their jobs.

More than 800 respondents with hiring responsibilities participated in the survey, and 40 percent said they will be hiring three or more new permanent or contract security professionals this year. In last year’s (ISC)² survey, only 13 percent said they would be doing so.

Hiring managers said they were looking for candidates with specific skills: operations security; access control systems and methodology; information risk management; applications and system development security; and security architecture and models. More than 90 percent said finding candidates with the right skills and experience was their biggest challenge.

But not all the survey findings were rosy. While 55 percent of U.S. respondents don’t expect layoffs this year, 21 percent do. Fifty-five percent of participants worldwide said the recession cut their security technology spending and 31 percent believe the economy will continue to hold back purchasing in 2010. In addition, 34 percent of U.S. respondents believe the downturn is increasing security risk in their organization.

It’s a good time to be a security professional, but it doesn’t mean there isn’t any weeding out happening in organizations, says Hord Tipton, (ISC)² executive director. “We’re seeing a sharpening in how companies define what they need in terms of skills,” he says. At the same time, companies are using more sophisticated technology that increases efficiency and could result in trimming workforces, he adds. ▀

—MARCIA SAVAGE

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

He recommends that organizations not rely solely on outsourcers who show proof of compliance with a standard such as PCI DSS; rather, they should conduct phone interviews with vendors (or onsite interviews with critical vendors) and ask a lot of questions about their security controls before signing a contract.

BUSINESS ALIGNMENT

If the need for a vendor management program was one lesson the recession taught, the need to align security with business needs was another. While nothing new for the security profession, the recession made it a priority.

"We in information security are still like little kids, where we get excited about a new technology or tool. This [recession] was a reality check to step back and figure out if it makes sense in the business context," Kark says.

In the past, some companies bought security tools that ended up sitting on the shelf due to complicated issues such as integration, but the days of that kind of waste are past, he says. CISOs and security managers are increasingly being asked to justify the business case around security, which is maturing the profession.

"Yes, security may be important and that compliance mandate needs to be met," Kark says. "But you have to figure out whether you want to go with the best tool out there or find other ways to mitigate a risk in a lot cheaper fashion."

The Security Consortium's Kadrach says savvy security professionals will be talking to the business leaders in their organization to understand how business processes are evolving and come up with a plan that grows with the business.

"The security people who are just technologists need to understand more about the business," he says. "They can't just throw technology at this stuff."

As organizations look to restart security projects that were put on hold during the downturn, one tactic they're using to increase efficiency is to take a modular approach with large-scale projects such as identity management, Kark says.

"Vendors are being pushed to deliver the same things in smaller chunks," he says.

FORECASTS

Where's the Recovery?

Economists' reports aren't tremendously encouraging.

The World Bank's [Global Economic Prospects 2010](#) report says the "acute phase" of the economic crisis is past and a recovery is under way but expected to slow in the second half of this year.

The White House predicts modest growth in its [annual economic forecast](#), according to the [Christian Science Monitor](#).

The International Monetary Fund's [World Economic Outlook Update](#), published in January, says the recovery is expected to remain sluggish in most advanced economies. •

—MARCIA SAVAGE

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

"What kind of modularity can be added to the scope of the project to reduce the upfront investment required?"

Overall, a risk-based approach is key to aligning security with business goals, experts say.

"The discussion should really along the lines of 'what are our risks and what could really damage us as a business,' then putting in place programs to protect against that," Gossels of SystemExperts says.

Companies are shifting away from a threat-based security model to a risk-based one, he says: "It's impossible to think of every possible threat because new threats come up every day. It's important to start from the mindset of what it is we're really trying to protect and what controls need to be in place."

Meholic says a well-thought out information security plan is based on a robust risk-assessment process; when gaps are identified, the security officer can take those issues to executive management and justify the need for more staffing or technology. But any time in front of the C-suite needs to spent wisely, he advises. Don't talk about cross-site scripting, which executives don't understand and don't care about.

"Make sure you take advantage of that exposure by showing them the critical issues at a level they understand," Meholic says, adding that he's found that graphical charts help in his bimonthly reports to the board.

EMERGING TECHNOLOGIES

As companies look to gain efficiencies or develop their business, they're looking to newer technologies such as cloud computing, virtualization and social media. Security professionals have a key role to play in educating businesses about the risks associated with those technologies, and experts say smart security pros will hone that role.

"The business leaders are saying, 'All these things I can do with these open platform tools are fantastic,'" says Jack Phillips, chief executive and co-founder of IANs, a Boston-based technology research firm. "That's a huge opportunity for information security to be a real leader, by being the guide to businesses that want to deploy new technologies to drive their business."

"The budget question is certainly there, but it's in the rear-view mirror compared to the challenges of the new technologies," he adds.

Forward-thinking security professionals are reshaping their risk profiles to cover technology game-changers such as collaborative media and the proliferation of portable devices, (ISC)'s Tipton says: "We're not in a position to say, 'We don't like this and were not going to do it.'"

Many enterprises are making a big push toward cloud services as a way to cut costs and become greener, which is putting a lot of pressure on security teams to quickly evaluate cloud services, says Kadrich. Evaluating cloud services is complicated by the fact "there's not enough testing, validation or high-level assurance," on the model, he adds.

"The discussion should really along the lines of 'what are our risks and what could really damage us as a business,' then putting in place programs to protect against that."

—JONATHAN GOSSELS,
president and CEO, SystemExperts

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

"The savvy security people should be talking to their executive staff about this problem and helping understand not just what the problem is now but about how it will evolve over the next six to 12 months," Kadrach says.

Security teams will need to work with corporate legal teams to ensure the enterprise is protected when contracting with a cloud provider, he advises.

"You've got walls and alarm systems and vetted people to reduce your risk, but when you move into the cloud, all you have are promises," Kadrach says.

PEOPLE

But as security executives tackle cloud computing and other technologies, they'll need to make sure their staffers aren't looking for other opportunities as the economy improves.

"If you have a critical security person with expanding employment and compensation options, they may jump ship," Arya says. "Losing talent in this specialized field is always a concern."

According to the (ISC)² survey, more than half of the 800 respondents with hiring responsibilities plan to hire either permanent or contract employees this year. That's an improvement over the 44.5 percent of hiring managers in the U.S. last year who said they expected to hire workers.

In a better economic environment, pay expectations rise with increased job opportunities, making it harder to find talent, Arya notes. However, organizations shouldn't resort to paying less for fewer skills. "The right talent and the right person are the number one criteria for any crucial position," Arya says.

Last year, many security executives spent a lot of time trying to keep their staff motivated and happy so they could emerge from the recession with their teams intact, Phillips says. The addition of temporary workers and consultants by cost-conscious enterprises challenged security managers to maintain staff morale, he adds.

In addition to staff retention, employee education is a focus for some organizations, especially as they move forward with new technologies.

USA Fed will soon roll out a robust mobile banking platform; the implementation plan includes mobile security education. The training investment targets both the credit union's staff and its members on the new platform and how to use it securely, says Carolyn James, senior vice president and CIO at the San Diego, Calif.-based credit union.

Sixty percent of USA Fed's members—many of whom are in the military—don't live near one of the credit union's branches; the organization is rolling out a mobile banking platform for both its overseas and stateside members. Mobile banking is relatively new and it's important that the credit union educate everyone on how safe the new channel is compared to online banking, James says.

"We must invest money in getting our membership up to speed so they understand

"If you have a critical security person with expanding employment and compensation options, they may jump ship. Losing talent in this specialized field is always a concern."

—JAY ARYA, vice president and information security officer, Investors Savings Bank

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

mobile banking is safe and secure," James says.

According to Kark, employee training and awareness is one of the top security strategies enterprises should deploy this year. Companies need to train their employees but also maintain regular communication about the changing threat environment in order to create a culture of information security awareness. One technology company spends 10 percent of its security budget on training and awareness to manage the risks of social media and consumerization, he wrote earlier this year.

APPROACH WITH CAUTION

To be sure, organizations are far from celebrating an economic recovery and many are anxiously awaiting signs of real improvements in the economy. There have been some encouraging signs, but organizations shouldn't let their guard down, Tipton says.

"Not everyone has turned their budgets loose because they share the same concerns: Is this recession really over and how long do we wait before we're comfortable in making changes and investments?" he says. •

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

ADVERTISING INDEX

Sophos 1
www.sophos.com

- Security Threat Report: 2010
- How to protect your critical information easily

McAfee, Inc. 3
www.mcafee.com

- 2010 Threat Predictions
- Top 10 Steps to Protecting Your Organization's Privacy Data

The Academy Pro 7
www.theacademypro.com

- Free infosec videos for the information security community.

Glasshouse Technologies 14
<http://www.glasshouse.com/>

SystemExperts 10
www.systemexperts.com

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

ENDPOINT SECURITY

FRAUD PREVENTION

RECOVERY STRATEGIES

SPONSOR RESOURCES

TECHTARGET SECURITY MEDIA GROUP



EDITORIAL DIRECTOR Michael S. Mimoso

EDITOR Marcia Savage

ART & DESIGN

CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS

Marcus Ranum, Bruce Schneier,
 Lee Kushner, Mike Murray

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
 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

SITE 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

VICE PRESIDENT/GROUP PUBLISHER
 Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
 Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
 Suzanne Jackson

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

SALES REPRESENTATIVES

Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson olson@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

Julie Brown
 Phone 781-657-1336 Fax 781-657-1100

REPRINTS

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



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

All rights reserved. Entire contents, Copyright © 2010 TechTarget. No part of this publication may be transmitted or reproduced in any form, or by any means without permission in writing from the publisher, TechTarget or INFORMATION SECURITY.