HOW TO COUNTER WEB 2.0 THREATS | PCI UPDATE

INFORMATION SECURITY®

SEPTEMBER 2010

Check Point
Check Point
Check Point
Check Point
FORTINET
Version 10.5
Symantec™ Security Information Manager
Symantec™ Data Loss Prevention
Google
ActivIdentity
Security Clients
ActivIdentity SecureLogin Single Sign-On
Blue Coat
Symantec™ Endpoint Protection Mobile Edition
Version 6.0
Kaspersky Open Space Security
IPS

2010 READERS' CHOICE AWARDS

WHICH PRODUCTS MADE THE WINNERS' CIRCLE?

TechTarget

INFOSECURITYMAG.COM

Real-time Security
for the Borderless Network

contents

SEPTEMBER 2010

VOLUME 12 NUMBER 7

FEATURES

ALSO

Intel-McAfee: Wow, or Why?

Embedding security in hardware isn't new, but is it worth an $8 billion investment? Time will tell on the Intel-McAfee acquisition.

BY MICHAEL S. MIMOSO

SO IT FINALLY happened. McAfee, the biggest security-only technology company left out there, has been acquired; and not by HP, nor IBM, nor even Symantec. Chipmaker Intel turned out to be the best suitor and had the biggest dowry, paying a 60-percent premium for the privilege of bringing software security to hardware. Close to 8 billion bucks for McAfee. Wow.

Or is it: Why?

Intel president and CEO Paul S. Otellini says the deal is all about embedding security inside of Internet-enabled devices—everything from processors running PCs and laptops, to smartphones, ATMs, televisions and yes, even, your car (now that's mobile computing). McAfee CEO Dave DeWalt points out that his company's Web reputation and cloud-virtualization security capabilities are a good fit with Intel's chips. Intel software and services VP and GM Renee J. James says the deal makes Intel a security player.

> "The way to think about this is we'll develop enhanced security solutions created only by our unique hardware innovations in combination with the software McAfee sells today."
>
> –RENEE J. JAMES, software and services VP and GM, Intel

"The way to think about this is we'll develop enhanced security solutions created only by our unique hardware innovations in combination with the software McAfee sells today," James says.

So this is how the security revolution really kicks in? You know which revolution I'm talking about: the one where security is embedded in everything. That promise has been festering for many years now as technology companies such as EMC, Microsoft, Google, IBM, HP and many others have scooped up security startups and stalwarts alike. Now Intel comes along and pays a whopping $48 a share for McAfee to integrate software security into hardware, and lunge headfirst into mobile computing and even cloud services.

On the surface maybe there's merit, but dive a few meters down and the water's pretty murky.

Intel has almost no mobile software story to speak of and to spend billions on a security company in order to plunge deeper into mobility sends a guy's jaw downward.

Last year, Intel set the stage for the McAfee deal by picking up embedded and mobile software maker WindRiver. While it's still relatively early to judge the WindRiver deal, it's not like Intel can lean back on a stellar record with software acquisitions—hello, LanDESK.

Otellini and James point out that McAfee has been collaborating with Intel for more than 18 months on product development. Intel has similar relationships with other security and technology companies. And that makes for another big rub here. Intel promises tight integration with McAfee, but what about RSA, Symantec and many others that already have deals in place to access the Intel platform with their respective products?

Just this year, RSA Security, VMware and Intel teamed on a secure cloud architecture which includes the speedy Westmere chips from Intel that feature instructions specifically designed to quicken encryption, decryption and transmission speeds. It also includes secure virtualization capabilities from VMware and SIM and GRC from RSA. Symantec, meanwhile, also has a longstanding partnership with Intel around virtualization and sandboxing. What of those relationships? And how will this impact all that innovation McIntel (IntelAfee?) has planned?

The biggest head-scratcher of a question is why: Why buy McAfee? Why not partner? Financial analysts asked the Intel braintrust just that, and the answer amounted to marketing mumbo-jumbo and how security software integrated into chipsets add value and differentiation for Intel. OK. I guess. As with any large transaction, there are tons of integration and strategic questions to be answered, and the answers are too far down the line for McAfee customers to be worried about now in the short term.

Long term, however, McAfee customers may have some concerns. This hasn't been a good year for the company, despite recent years of post-stock scandal growth and gains against Symantec, its biggest competitor. The company's biggest sin came in April when a faulty McAfee antivirus update shut down Windows XP computers, took them offline and caused constant reboots. Unplanned downtime is a bummer for corporations and any of those up for renewals this time of year now have to worry about acquisition tribulations. What if Intel blows this and McAfee becomes an afterthought in coming years? What if the focus on hardware integration deters from the gains the company has made as a software leader? Legitimate questions lead to legitimate hesitation that only stands to benefit Symantec, Trend Micro, Sophos and the other security software vendors waiting in the wings with discounts and partnership offers.

In the end, maybe Intel is way ahead of conventional thinking here. Maybe security software embedded in hardware is the real revolution and maybe McAfee operating as a wholly owned subsidiary will remain an innovative security provider.

And maybe this Intel-McAfee deal won't take its place in the annals of other shaky acquisitions such as HP-Compaq and Symantec-Veritas. And maybe, in a couple of years, we won't be asking why. ▸

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

SYMANTEC PROTECTS MORE

COMPUTERS
FORTUNE 500 ENTERPRISES
CLIENTS
TEAMS
MOBILE DEVICES
BRANCH OFFICES
VIDEOS
INFORMATION
FILES
SYSTEMS
EMAILS
LAW FIRMS
INTERNATIONAL
NETWORKS
PEOPLE
MEDIUM BUSINESSES
APPLICATIONS
UNIVERSITIES
TEAMS
ORGANIZATIONS
PROFITS
SOCIAL NETWORKS
INDUSTRIES
USERS
DESKTOPS
SERVERS
ASSETS
WEBSITES FILES
NETWORKS
LAPTOPS
BANKS
MANUFACTURERS
INDIVIDUALS
SERVERS
SERVERS
MEDICAL RECORDS
IDENTITIES
CUSTOMERS
DATA
GOVERNMENTS INFORMATION
VIRTUAL ENVIRONMENTS
ENDPOINTS
COMPANIES
DATA CENTERS
WINDOWS ENVIRONMENTS
DATA
NON PROFITS
COMMUNITIES
SMALL BUSINESSES
BLOGS
HOUSEHOLDS

THAN ANYONE.

SYMANTEC IS THE WORLD LEADER IN SECURITY.

Know what it takes to be secure today at go.symantec.com/securityleader

Confidence in a connected world.

symantec.™

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

VIEWPOINT

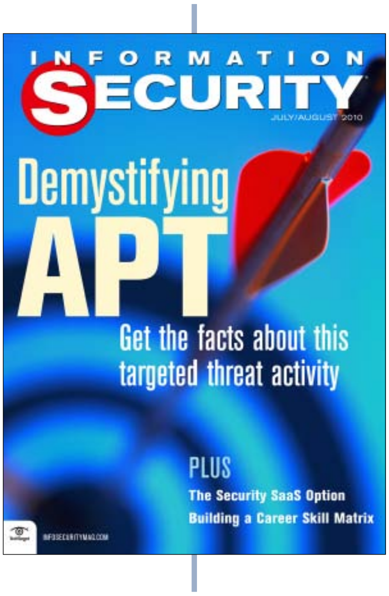
Readers respond to our commentary and articles. We welcome your comments at feedback@infosecuritymag.com.

Beating Back the APT Hype

"What APT is (And What it Isn't)", (July-August issue) is an excellent unbiased article. And I totally agreed with the author that APT is an over-hyped term that vendors and even security practitioners use to "scare" their management into throwing more dollars into security realm. Yes, tools are useful. Unless one knows how to use those tools, they would be useless against any form of attack. Being in IT security for more than 10 years, this is what I have to advise: log, log and log—and have someone to review those logs meticulously. Don't let complacency slip in; always prepare for the unknown.

Lastly, good work to *Information Security* magazine. This is the sort of article that inspires us, the true security practitioners, to work harder and smarter.

—DAVID NG, CISO, Deputy Director



COMING IN OCTOBER

SECURITY 7 AWARDS

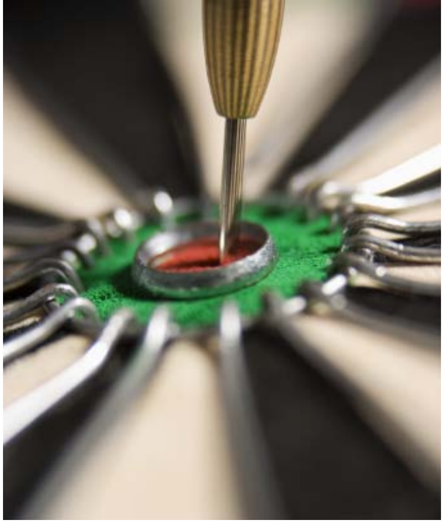
Information Security magazine will announce its sixth annual Security 7 Award winners. The awards recognize the achievements and contributions of security practitioners in seven vertical markets: financial services, health care, manufacturing, telecommunications, government, manufacturing, and education. Past winners include industry luminaries such as Dorothy Denning and Gene Spafford. Last year's winners include: Melissa Hathaway, former acting senior director for cyberspace; Jerry Freese of American Electric Power; Bruce Jones of Kodak; and Jon Moore of Humana.

DATABASE AUDIT TOOLS

Auditing is a core component to compliance and security programs of all types, and a generally accepted practice by IT operations. Regulatory compliance demands accurate and complete records of transactions, and relational database audit trails produce just that. In this article, we'll define database auditing, provide use cases, explain what are the four basic platforms used for creating, collecting and analyzing database audits, and offer some advice that will help you when buying database auditing tools.

PEOPLE AND SECURITY

Once people start interacting with a computer, its risk exposure is exponentially increased. Humans read email, click on links, download files and open file attachments. People, not technology, are the weakest link–and attackers know it. In this article, expert Lance Spitzner will examine why humans are bad at judging risk and how this impacts computing and information security processes, policies and technology. Spitzner will also explain the importance of awareness training and offer some advice on how to implement a successful training program.



What To Do If Your Intellectual Property Is Stolen

Targeted attacks on corporations and their crown jewels have become routine. Companies need to be prepared.

BY KIM GETGEN AND JOHN W. WOODS

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

WHAT HAPPENS WHEN your company experiences a data breach involving intellectual property or valuable trade secrets? In the last year, there's been a significant uptick in the number of corporations seeking legal advice around the protection of their high value intellectual property—particularly organizations with large overseas operations. While this type of data may not be as regulated as personally identifiable information (PII), its loss can be more financially damaging.

Take, for instance, the real-life example of an organization in the process of closing a deal in the hundreds of millions of dollars. The entity with whom the organization was negotiating had a suspiciously high amount of privileged information, right down to references made by key executives in their emails. A forensics investigation determined that the organization, and its outside advisors, had indeed been the victims of a breach where emails and intellectual property relevant to the deal were accessed.

While CEOs might think this type of industrial espionage sounds like the fiction found in a Tom Clancy novel, most security professionals now are very aware how commonplace these types of threats are, in part due to the public disclosure Google made earlier this year about a security incident dubbed Aurora. Aurora was an important security consciousness-raising event, moving what has long been thought of as an issue of concern for only the defense industrial base to the forefront of thinking for executives in almost any vertical. So what would you do if your organization becomes a victim to this type of breach? Here are a couple of suggestions.

Develop a Disclosure Strategy

There are a number of reasons why your organization will want a disclosure strategy if you think you've been breached. These are strategies either your legal team or outside legal experts on data breach regulations can put together on your behalf, and should take these issues into account:

1. In this day and age of heightened regulations, publicly traded companies are under tighter scrutiny from auditors who are asking increasingly pointed questions around how an intrusion may intersect with the IT controls relevant to Sarbanes-Oxley. While your company may not have a legal obligation to disclose the event publicly,

more and more our legal and security teams are called upon to answer these auditor questions. Understanding how an intrusion event may or may not have impacted controls around financial reporting before engaging in that dialogue is a key to success.

2. Even if the attackers were after intellectual property (whether or not they succeeded), it doesn't mean they didn't touch any other systems holding PII. Frequently, advanced malicious intruders do not have any desire to steal PII, but in the course of their intrusion may have placed malicious software on servers or databases that contain such protected data. Companies conducting investigations into these types of intrusions need to understand that state attorney generals have taken a very broad construction of the term "access" when it comes to PII. Some states may take the position that even if PII theft was not the intended target, to the extent it was exposed the organization needs to consider whether it has an obligation to notify employees or customers in accordance with state, federal or country-specific regulations.

A critical lesson from breach investigations is that frequently a disconnect exists between the legally important questions, such as the type of data "accessed" and the "root-cause" analysis conducted by forensic and network security specialists. By working with the in-house or outside legal experts who are knowledgeable in data breach notification regulations, your organization will benefit by focusing your forensics team on what you will need to disclose and report.

By working with the in-house or outside legal experts who are knowledgeable in data breach notification regulations, your organization will benefit by focusing your forensics team on what you will need to disclose and report.

Cooperate with Law Enforcement

It's important to realize that if your company has its intellectual property stolen, regardless of whether the culprit is a state actor or criminal gang, you are the victim of a crime. A critical question that breached companies need to confront early is whether to involve law enforcement. What many lawyers don't realize is that they (and the security and forensics teams) can work smarter by working collaboratively with law enforcement. Sharing what you know about how you've been breached can allow law enforcement to compile a case against those who broke in and accessed your systems.

We have also observed that law enforcement can help contain an incident by providing valuable "missing link" information, allowing corporations to find hidden backdoors the intruders used that would have otherwise gone unnoticed. They can also provide knowledge of important aspects of the intrusion based on past experience that can not only be extremely helpful, but also allow you to save time, when every second counts.

In addition, working with law enforcement can allow a breached entity to receive a "delay notification," giving them more time to accurately understand what data may have been accessed and/or acquired. This is important because some organizations have been able to significantly reduce the number of customers for which notification was required. There are a number of instances where a breached entity over-reported the number of customers exposed, incurring much greater scrutiny than otherwise required. While law enforcement can't always give out delay notifications, they are more likely to do this for corporations who are cooperative.

Due to the increased risk, now is the time to take a hard look at what data is valuable to your organization and consider what your organization would do if compromised. Start the conversation and incident response planning today before your organization is responding to a crisis tomorrow. ▸

Kim Getgen, principal at consulting firm Trust Catalyst, has authored a data breach prep kit for organizations looking for free tools to help them prepare for a breach.

John W. Woods is a partner at Hunton & Williams LLP, where he focuses on conducting internal investigations and advising corporations in the legal response to network security intrusions and data breaches. Send comments on this column 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.

INFORMATION SECURITY®

www.SearchSecurity.com

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

SearchSecurity.com

www.SearchSecurity.com

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

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

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

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

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

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

Analysis | PRIVACY

Surveillance Society

Tools help protect privacy but safeguarding personal data in the age of Google and Facebook is getting harder.

BY ROBERT WESTERVELT

EARLIER THIS DECADE, public criticism halted the Big Brother-esque initiative from the U.S. government to create a massive database of personal information collected from a wide range of sources, everything from emails to credit card purchases. And we've certainly come a long way from the infamous and long-ago abandoned government plan to embed surveillance chips in consumer electronics.

Or have we?

Moxie Marlinspike, a noted independent security researcher, says the private sector has taken up the cause. Websites like Google, Facebook and others offer free services that are designed to help people take part in society, but at a hefty cost: You volunteer your personal information to companies and that valuable data accumulates.

"If there's one thing Google has excelled at doing, it's making sense of large repositories of data," says Marlinspike. "Make no mistake about it, they are in the surveillance business and the effect is the same."

Managing online privacy was one of the themes that surfaced at Black Hat 2010, with a session track devoted to the issue. In a Black Hat presentation, Marlinspike railed against Google and other firms that collect personal data for analytical purposes as part of using their services. Technology has changed the fabric of society, he says. People volunteer to use cell phones that can now be used to pinpoint a person's location; meanwhile people never have to delete an email message using Gmail and can archive messages there for eternity. The alternative to using Web-based services and other technologies is to ditch the cell phone, disconnect from the Internet and live like a hermit, he says.

But there may be a better alternative. Marlinspike has introduced several tools that help people concerned about privacy avoid giving up personal information. GoogleSharing, a Firefox add-on, acts as an anonymizing proxy service and is designed to evade Google analytics and prevent Google from tracking searches. As co-founder of WhisperSystems, Marlinspike introduced two open source mobile applications for the Android platform that address privacy. RedPhone provides encryption for cell phone calls while TextSecure encrypts text messages and stores them securely on the phone.

But privacy issues go beyond cell phone tracking and Internet analytics. Tom Cross, a research manager with IBM's X-Force research team, talked about ways the faulty programming in routers, designed for law enforcement to conduct lawful intercept operations, can be used illegally by an attacker to collect traffic from people. The techniques needed to tap into the traffic are sophisticated, Cross says, but they are a cause for concern. Design issues do little to stop insiders from spying on someone. Cross says turning on audit logs can prevent insider abuse, while deploying some level of encryption could help further reduce the threat.

> "If you want to reduce the amount of illegal wiretapping, improving link layer encryption in wired and wireless systems could be the answer."
>
> –TOM CROSS, research manager, IBM's X-Force research team

"If you want to reduce the amount of illegal wiretapping, improving link layer encryption in wired and wireless systems could be the answer," Cross says.

While the tools presented by Marlinspike are useful, they are not likely to be used by many people, says Graham Cluley, a senior technology consultant at UK-based security vendor, Sophos. GoogleSharing is currently used by about 80,000 people, a far cry from the estimated 300 million people that use Google every day. Still, researchers like Marlinspike, Cross and others are helping educate users about the information they are freely giving up online.

"People are giving up an astonishing amount of information to the Web because a lot of people aren't really conscious of what they're doing," Cluley says. "They haven't joined all the dots together and don't understand the serious consequences of what they're doing."

In the UK, for example, Cluley says he walks by closed-captioned cameras every day. The average person is seen on camera dozens of times there. Vehicle registration plates are logged. But most people don't seem to care or have embraced it for safety reasons, he says.

"There are people who are worried about this gradual erosion of our privacy and want to disconnect altogether," Cluley says. "But there are others who say we have to try and find some sort of happy medium, because at the moment people like what technology is doing for them. I think we need to find that middle ground."▸

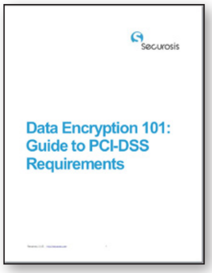
Robert Westervelt is the news editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

Lost on the road to PCI Compliance?

Let Prime Factors help you find the way with EncryptRIGHT, our new, cost-effective encryption and key management software suite. Leveraging 30 years of experience, we have designed EncryptRIGHT from the ground up to meet security threats, simplify deployments, and satisfy auditors that payment card data is safeguarded. EncryptRIGHT includes:

- PCI approved cryptography and key management for one price
- Reports and audit trails for assessment & verification processes
- Broad platform support from PC to Mainframe
- A simple desktop application, or API for application integration
- Wizards that help you get running quickly.

Visit our website to find out how EncryptRIGHT can put you on the road to PCI compliance.


Securosis

Data Encryption 101: Guide to PCI-DSS Requirements

The new white paper Data Encryption 101: Guide to PCI-DSS Requirements, written by Securosis, cuts through the techno-babble and discusses how to select the most appropriate encryption solution for your situation. Download it today.

541-345-4334 www.PrimeFactors.com

PRIME FACTORS, INC.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

Poisoned Results

By *Information Security* staff

With online crime a vast, money-stealing business operation, it's no surprise that criminals are exploiting search engines for their ill-gotten gains. Researchers at Barracuda Networks studied popular search terms, conducted searches, retrieved the results and analyzed the sites for malware. Their study, conducted over a 57-day period, involved Google, Bing, Yahoo, and Twitter and more than 25,000 popular topics. Released at the Black Hat 2010 conference in July, the results include:

Total malware by search engine:

69 percent	Google
18 percent	Yahoo
12 percent	Bing
1 percent	Twitter

Top trending topics on sites hosting malware:

26 percent	news
23 percent	entertainment
11 percent	forums, news groups

Top search terms used by malware:

Scott+Sicko (football player)

Indrani (photographer)

Graciela+Beltran (singer)

Chrishell+Stause (actress)

Emma+Caulfield (actress)

Mark+Souder (politician)

OVER-HEARD

> "Despite these being security devices, it seems that they're just as prone to having trouble as any other piece of software."

–JEFF JARMOC, researcher at SecureWorks, speaking at Black Hat 2010 about vulnerabilities in Cisco firewalls and McAfee consoles

Everything you want in an AV solution.

ESET®

Internet Security

NEW Remote Administrator 4 features:

- Intelligent group manager
- Firewall rules merge wizard
- Improved policy manager
- Simplified remote administration
- Cross-platform management

Protection, speed and flexibility.

ESET NOD32 Antivirus 4 + Remote Administrator

ESET NOD32® Antivirus 4 Business Edition is more than simply powerful Internet security. It's a comprehensive network-wide solution. And, when paired with ESET Remote Administrator, it takes the headaches out of IT management. Light on client resource consumption and easy to manage, ESET NOD32 + Remote Administrator (RA) saves money that might otherwise be wasted upgrading computers running sluggish AV. And because it's so easy to manage, your IT department gets back what it values most — hours in the day.

Proactive protection

We scan all incoming and outbound network traffic, email attachments and removable media — but that's not enough. We compare unknown code to millions of database signatures — but that's not enough either. We even have frequent ultra-small updates that incorporate signatures from threats encountered across ESET's 100-million user network — but you still need more.

Superior protection doesn't depend on updates at all. In comparative testing using outdated signatures, ESET consistently outperforms other AV solutions. "ESET offers the highest proactive threat detection," independent AV-Comparatives May 2009.

The difference? Advanced heuristics. Proactive protection that doesn't just passively look for existing features of malware — it actively predicts strains that haven't been written yet and sandboxes them in a controlled disk environment where they can do no harm. And when a block of code seems suspicious — it is immediately repaired or quarantined. Smoothly. Efficiently. Seamlessly.

Unmatched speed

On the user end, ESET runs just two processes — the scanning kernel and the user interface — and together sip just about 44 MB of RAM. Typically, that's less than an instance of Word, Communicator, Excel, Explorer or Firefox. And with minimal interruptions or pop-ups and no scanning slowdown at file open or startup, your users won't even notice its running. But they will notice they no longer need to phone IT for lagging startups or malware infections.

On the server side, mirrored downloads and small signature updates mean your network traffic will never lag because of your antivirus solution. Mail scanning happens in the blink of an eye and compatibility with a variety of protocols and systems, from Cisco NAC to Microsoft Exchange means that you'll never have to deal with multiple antivirus solutions for your mixed network.

Flexible management

For mixed networks, ESET NOD32 delivers comprehensive protection — working natively in Windows XP, Vista and 7; Linux / BSD / Solaris; Mail Server; Exchange; and soon Linux Desktop and Apple Mac OS X.

Vast multiplatform protection doesn't have to be a management nightmare. ESET Remote Administrator allows for simple push-installation of preconfigured NOD32 packages to client computers and now with RA4 – allows Active Directory management of dynamic networks.

The combination of ESET NOD32 + Remote Administrator means simple, powerful management of a network of 10 computers or 10,000 with protection for every system and every platform. Each computer is an attack surface — and you need the best available protection on all of them.

Solutions to fit all your business needs

- File server security
- Mail server security
- Gateway server security
- Mobile phone security

www.eset.com/business/products

Request your free trial at www.eset.com/business-trial

Should enterprises give in to consumerization at the expense of security?

POINT *by* MARCUS RANUM

SOME COMPANIES ARE apparently adopting a policy of allowing employees to do their computing work on personal devices—a trend that, I suspect, is a result of mainstream IT departments not being quite sure how to accommodate their growing user-base of Apple Computer addicts. Our industry appears to be of two minds about this topic: On one hand, we're worried about data leakage, and on the other, we take steps to make said leakage as easy as possible.

I was on a conference call last week, in which a senior technical executive asked me if I had any suggestions for what kind of data leakage system could be put between their Exchange server and their BlackBerry users to detect and block attempts to export sensitive data. As our conversation continued, he said, "Of course, these are corporate-issued BlackBerries. So at least we can do remote-wipe in case of loss." I was struck dumb for a second, trying to sort through the inherent contradiction in simultaneously giving employees a tool for exporting data from the safety of the corporate WAN, and worrying about data leakage. It seems silly—like giving a teenage boy a BB gun and expecting nothing to get shot full of holes. And, apparently, some companies are doing the full monty and encouraging employees to bring to work whatever IT gear they want and use that.

> "On one hand, we're worried about data leakage, and on the other, we take steps to make said leakage as easy as possible."
> —MARCUS RANUM

I think that all this new technology is great—heck, I even think all you tweeters, Facebook users and MySpace users are cute. It's important to know the mundane details of your life and your important marketing messages—but what I absolutely do not want to hear is your managers scratching their heads five years from now and saying "Why can't we keep our data from appearing in weird places?" One thing I can predict for sure is that in another five years, customers will be complaining that data leakage products don't work. From my long-term viewpoint, the trend-line looks like: 1995) install firewalls; 1996) punch big holes through them; 1997) announce "firewalls are dead"; 1998) install intrusion detection systems; 1999) turn off all the signatures; 2000) announce "intrusion detection is the pet rock of computer security"; 2001) install log aggregation systems; 2002) ignore them; 2003) complain that intrusion detection still doesn't work; 2004) worry about data leaking from the network; 2005–2010) give employees mobile devices; 2006–2010) give employees direct-from-desktop

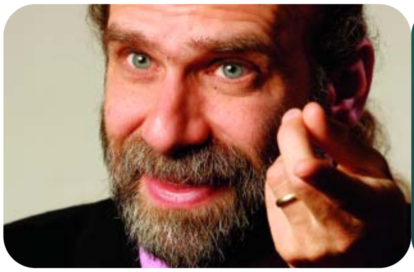
TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

Internet publication capability via Facebook, Twitter, etc.; 2010) give employees control of their own IT—when is it all going to sink in?

My father used to tell a joke about a married couple riding a tandem bicycle up a steep hill. They pedaled and pedaled and sweated and struggled and finally got to the top. The rider in front turned to the one in the back and said, "We made it! I wasn't sure we'd be able to do it!" And the rider in the rear said, "Yeah, I was on the brake the whole way, I was so afraid we'd roll backwards." Corporate IT's attitude toward security seems to be "Now that we've finished trying to do something smart, let's do something really stupid!" Except that, a lot of the time, we leave out the first part.

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



IF YOU'RE A typical wired American, you've got a bunch of tech tools you like and a bunch more you covet. You have a cell phone that can easily text. You've got a laptop configured just the way you want it. Maybe you have a Kindle for reading or an iPad. And when the next new thing comes along, some of you will line up on the first day it's available.

So why can't work keep up? Why are you forced to use an unfamiliar, and sometimes outdated, operating system? Why do you need a second laptop, maybe an older and clunkier one? Why do you need a second cell phone with a new interface, or a BlackBerry, when your phone already does e-mail? Or a second BlackBerry tied to corporate e-mail? Why can't you use the cool stuff you already have?

More and more companies are letting you. They're giving you an allowance and allowing you to buy whatever laptop you want, and to connect into the corporate network with whatever device you choose. They're allowing you to use whatever cell phone you have, whatever portable e-mail device you have, whatever you personally need to get your job done. And the security office is freaking.

You can't blame them, really. Security is hard enough when you have control of the hardware, operating system and software. Lose control of any of those things, and the difficulty goes through the roof. How do you ensure that the employee devices are secure and have up-to-date security patches? How do you control what goes on them? How do you deal with the tech support issues when they fail? How do you even begin to manage this logistical nightmare? Better to dig your heels in and say "no."

> "Security is on the losing end of this argument, and the sooner it realizes that, the better."
>
> –BRUCE SCHNEIER

But security is on the losing end of this argument, and the sooner it realizes that, the better.

The meta-trend here is consumerization: cool technologies show up for the consumer market before they're available to the business market. Every corporation is under pressure from its employees to allow them to use these new technologies at work, and that pressure is only getting stronger. Younger employees simply aren't going to stand for using last year's stuff, and they're not going to carry around a second laptop. They're either going to figure out ways around the corporate security rules, or they're going to take another job with a more trendy company. Either way, senior management is going to tell security to get out of the way. It might even be the CEO, who wants to get to the company's databases from his brand new iPad, driving the change. Either way, it's going to be harder and harder to say no.

At the same time, cloud computing makes this easier. More and more, employee computing devices are nothing more than dumb terminals with a browser interface. When corporate e-mail is all webmail, when corporate documents are all on GoogleDocs, and when all the specialized applications have a web interface, it's easier to allow employees to use any up-to-date browser. It's what companies are already doing with their partners, suppliers, and customers.

Also on the plus side, technology companies have woken up to this trend and—from Microsoft and Cisco on down to the startups—are trying to offer security solutions. Like everything else, it's a mixed bag: some of them will work and some of them won't, most of them will need careful configuration to work well, and few of them will get it right. The result is that we'll muddle through, as usual.

Security is always a tradeoff, and security decisions are often made for non-security reasons. In this case, the right decision is to sacrifice security for convenience and flexibility. Corporations want their employees to be able to work from anywhere, and they're going to have to loosen control over the tools they allow in order to get it.

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.*

Trend Micro Ranks #1 Again

Real Malware, Real Test, Real Solution,
Real Protection for the Real World.

The industry's best protection just got better.

Trend Micro OfficeScan again ranked #1 in the June 2010 independent, real-world test of corporate endpoint solutions by NSS Labs.

Why is Trend Micro a good choice to protect your data

- **Best Overall Protection.** Blocked over 95% of all threats vs. the industry average of 84%
- **Best Time-To-Protection.** Protected against unknown zero-day threats in under 5 hours–4X faster than the closest competitor and nearly 10X faster than the industry average
- **Best Web Threat Blocking.** Blocked 88% of web infections at their source vs the industry average of 65%
- **Consistent Results.** Trend Micro ranked #1 for second consecutive time in NSS Labs Corporate results.

Corporate Test Results

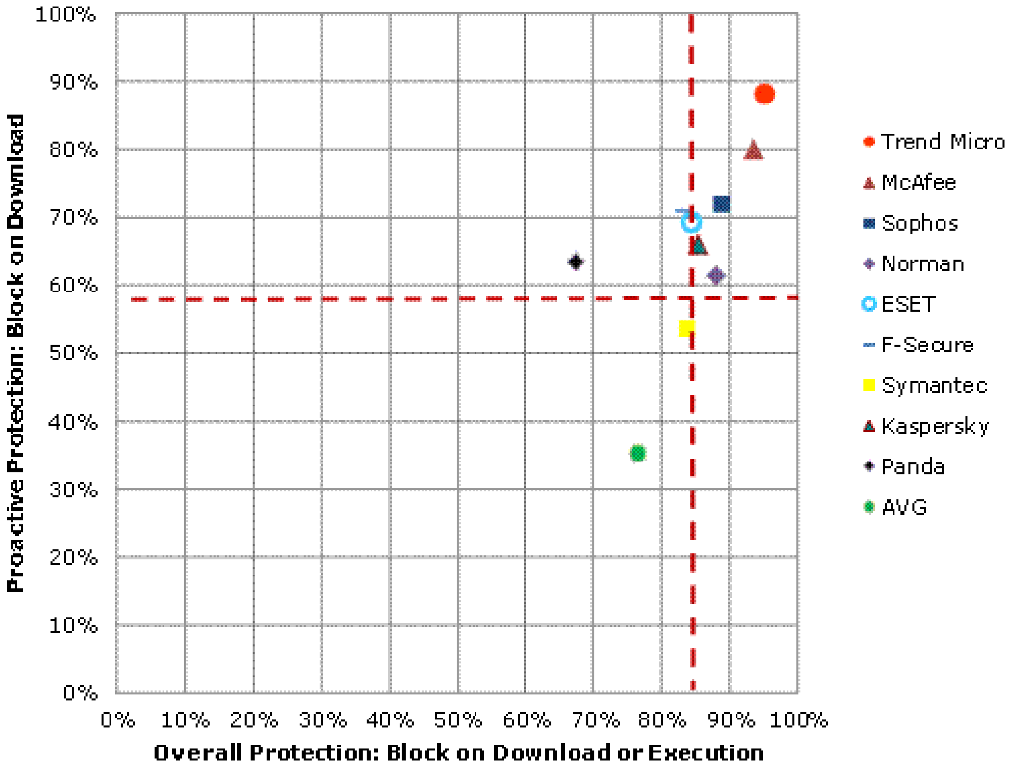
>>LEARN MORE

Try Trend Micro™ OfficeScan Client-Server Suite

>>FREE TRIAL

Contact Us: 877-252-2065

In NSS Labs real-world, independent test, Trend Micro scored top in protection—blocking more threats at the source and overall.



Contact Trend Micro

877-252-2065

facebook.com/fearlessweb

twitter.com/trendmicro

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

2010 READERS' CHOICE AWARDS

WHICH PRODUCTS MADE THE WINNERS' CIRCLE?

For the fifth consecutive year, INFORMATION SECURITY readers voted to determine the best security products. Nearly 1,500 voters participated this year, rating products in 14 different categories. Click through to see which products took top honors:

METHODOLOGY *Information Security* magazine and SearchSecurity.com presented nearly 1,500 readers with dozens of security products and services, divided into 14 categories.

Respondents were asked to rate each product based on criteria specific to each category. For each criteria, respondents scored the product on a scale of one (poor) to five (excellent). In addition, each criteria was given a weighted percentage to reflect its importance in that category.

Winners were based on the cumulative weighted responses for each product category criteria. Editors arrived at a product's overall score by calculating the average score it received for each criteria, applying the weighted percentage and adding the adjusted scores. ▸

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

ANTIMALWARE

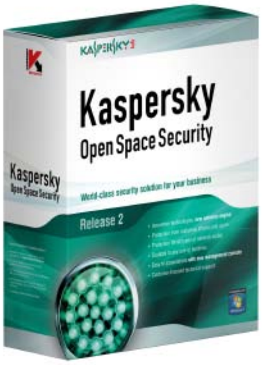
Business-grade desktop and server antivirus and antispyware, using signature-, behavior- and anomaly-based detection, whitelisting. Includes suites bundled with host-based intrusion prevention and client firewalls.

GOLD

Kaspersky Open Space Security

Kaspersky Lab

http://www.kaspersky.com



Kaspersky Lab's Kaspersky Open Space Security took top honors, winning high marks for effectively detecting, blocking and cleaning malware, and in the speed and frequency of signature updates. Readers also liked the product's reporting and alerting capabilities. Kaspersky Open Space Security is a suite of antimalware protection for the gateway and endpoint. It includes: Business Space, which provides file server protection and was designed for servers that operate under heavy loads; Enterprise Space, which adds mail server security and components for the protection of workstations; and Total Space, which adds gateway protection to the previous offerings.

SILVER

Cisco Security Agent

Cisco Systems

www.cisco.com

Cisco Systems' Cisco Security Agent was designed to protect servers and desktops. It provides signature-based antivirus and data loss prevention in a single agent. Content scanning capabilities detect credit card numbers, Social Security numbers and can be customized to detect local files. The software protects against both user actions and targeted malware and has a predefined compliance and acceptable use policy engine that can be used for reporting and auditing activities. It received high marks for its ability to detect and block unknown malware and zero-day exploits as well as its reporting and alerting capabilities. Cisco announced in June that it would stop selling the software in December.

BRONZE

Symantec Endpoint Protection

Symantec

www.symantec.com

Symantec Endpoint Protection includes a protection suite with endpoint and messaging security, backup and recovery capabilities, and antivirus protection for laptops, desktops and servers. The software also integrates with existing network infrastructure to provide access control and enforce endpoint security policies. Readers awarded Symantec's product with the bronze, giving it high marks for providing fast signature updates, its reporting and alerting capabilities, and effectiveness in detecting, blocking and cleaning up malware.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

AUTHENTICATION

Digital identity verification products, services, and management systems, including PKI, hardware and software tokens, smart cards, knowledge-based systems, digital certificates, biometrics, cell phone-based authentication.

GOLD

ActivIdentity SecureLogin Single Sign-On

ActivIdentity

http://www.actividentity.com

When implementing authentication tools, organizations often struggle with bringing the technology to a large and evolving number of end users. Scalability, however, is what gave ActivIdentity SecureLogin Single Sign-On top honors in this year's authentication category. Readers praised its ability to adapt to increasing demands and also noted the product's effectiveness in securing credentials against cracking or discovery. The tool enables password management, enforces password policies and offers SSO authentication for both local and remote users.

SILVER

RSA SecurID

RSA, The Security Division of EMC

http://www.rsa.com

RSA SecurID, this year's silver medalist, provides two-factor authentication using hardware token authenticators, software authenticators, authentication agents and appliances. Tokens generate authentication codes at fixed intervals (every 60 seconds, according to RSA). Aside from nods to the product's scalability, survey respondents especially appreciated SecurID's ability to keep credentials from being compromised. A handful of those voting also agreed that the product was easy to integrate and had few compatibility issues.

BRONZE

VeriSign Identity Protection Authentication Service

VeriSign

http://www.verisign.com

Like users of the previously mentioned products, readers familiar with the VeriSign Identity Protection Authentication Service felt confident that their valuable credentials were secure from external attackers looking to crack passwords. Users gave the VeriSign product the bronze this year, mainly noting its credential security capabilities, but also mentioning its scalability, ease of use and return on investment. The cloud-based service keeps the end user's identity information within the enterprise, sending a security code and credential ID to VeriSign for authentication.

DATA LOSS PREVENTION

Network, client and combined data leakage prevention software and appliances for enterprise and midmarket deployments, as well as "DLP light" email-only products.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

GOLD

Symantec Data Loss Prevention

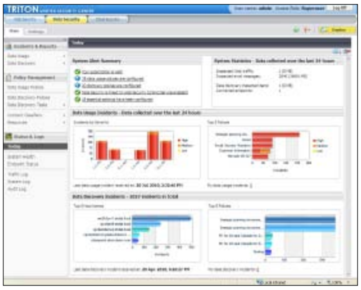
Symantec
www.symantec.com

Symantec Data Loss Prevention software, based on its acquisition of Vontu in 2007, contains data discovery, data monitoring and data protection capabilities. The software discovers and creates an inventory of sensitive data and then monitors how sensitive data is being used. It has policy enforcement capabilities and can remediate and report on incidents that it detects. Readers gave Symantec Data Loss Prevention high scores in every category, including effectiveness in detecting and/or preventing unauthorized user activity, service and support, and ease of installation.

SILVER

Websense Data Security Suite

Websense
www.websense.com



The Websense Data Security suite contains four modules, including Websense Data Monitor which examines the network for data loss via the Web, instant messaging applications, email and FTP, and Websense Data Protect which automatically blocks, quarantines, encrypts, audits and logs and notifies users when it detects policy violations. The Websense Data Security Suite was given high marks for flexible policy definition/management, detecting and preventing unauthorized user activity, and comprehensive and flexible reports.

BRONZE

Trend Micro Data Loss Prevention

Trend Micro
www.us.trendmicro.com

Trend Micro's Data Loss Prevention software family contains Trend Micro DLP for Endpoint, which monitors and enforces policies, Trend Micro DLP for Network, which monitors the network for security policy violations, and the Trend Micro DLP Management Server, which provides central management capabilities for reporting policy violations. Readers gave Trend Micro Data Loss Prevention high marks for ease of integration with applicable software and hardware, and ease of installation, configuration and administration.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

IDENTITY AND ACCESS MANAGEMENT

User identity access privilege and authorization management, single sign-on, user identity provisioning, Web-based access control, federated identity, role-based access management, password management, compliance and reporting.

GOLD

Microsoft Identity Lifecycle Manager

Microsoft

http://www.microsoft.com/en/us/default.aspx

Forefront Identity Manager 2010

Welcome, Administrator

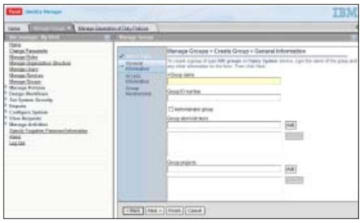
Despite a large field of battle-tested competitors, Microsoft's legacy identity product narrowly surpassed IBM for our No.1 ranking. Identity Lifecycle Manager 2007, which is being replaced this year by Forefront Identity Manager 2010, features identity synchronization, user provisioning, and management of certificates and smartcards; it requires Windows Server 2003 or 2008 and SQL Server. Readers gave it solid marks across the board, particularly for ease of use, integration with associated products and comprehensive and flexible reports.

SILVER

IBM Tivoli Identity Manager

IBM

http://www.ibm.com/us/en/



Big Blue's user provisioning and role management software offers automated provisioning and self-service interfaces, discrepancy discovery comparing access to privileges, simulated policy verification assessment, centralized Web-based administration and compliance-focused auditing and reporting. Readers especially liked IBM Tivoli Identity Manager's integration and compatibility with associated products, as well as its scalability and extensibility—the breadth of platforms, applications, and domains it covers. The product received only average marks for overall ROI.

BRONZE

RSA Access Manager

RSA, The Security Division of EMC

http://www.rsa.com/

RSA Access Manager

Finishing a close third, RSA Access Manager governs access to Web applications and consumer-facing applications with features such as centralized identity and privilege management, single sign-on, user authentication and authorization and support for APIs including Java and WSI. Readers gave 2009's gold winner high marks for its ease of use, and also liked its integration with associated products, scalability and ease of installation, configuration and administration. The product's reporting and vendor support received only average marks.

READERS' CHOICE AWARDS '10

Information Security

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

INTRUSION DETECTION/PREVENTION

Network-based intrusion detection and prevention appliances, using signature-, behavior-, anomaly- and rate-based technologies to identify denial-of service, malware and hacker attack traffic patterns.

GOLD

Check Point IPS-1

Check Point Software Technologies

http://www.checkpoint.com

Check Point IPS-1 intrusion detection and prevention system features an IPS-1 centralized interface with graphical management tools that allow a system administrator to quickly identify malicious activity, enhancing administrative efficiency and providing rapid-response mitigation. The product received high marks from the voters in all categories, but its intrusion detection and prevention capabilities, as well as its threat response time and easy installation received particularly favorable reviews, ultimately garnering it the gold medal.

SILVER

Sourcefire Intrusion Prevention System (IPS)

Sourcefire

http://www.sourcefire.com/

Sourcefire Intrusion Prevention System, built on the widely deployed Snort rules-based detection engine, combines vulnerability- and anomaly-based inspection methods to analyze network traffic and prevent critical threats from damaging the network Readers gave the product solid grades for its intrusion detection and prevention capabilities, frequency of updates and threat response times, as well as reporting and alerting features. However, readers weren't as fond of its vendor service and support capabilities

BRONZE

Cisco Intrusion Prevention System

Cisco Systems

http://www.cisco.com

The Cisco Intrusion Prevention System received commendable marks across the board, and brought home the bronze, mostly attributed to its ability to effectively and accurately detect and prevent attacks, its update frequency and response to new threats. Readers also rated the product highly for vendor support, reporting and alerting capabilities and return on investment. The Cisco Intrusion Prevention System is a network-based IPS that identifies, classifies and stops known and unknown threats.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

MESSAGING SECURITY

Antispam, antiphishing, antimalware and antivirus filtering software and appliance products, as well as hosted "in the cloud" messaging security services.

GOLD

Google Message Security

Google

http://www.google.com/postini/

Google Message Security
powered by Postini

Long the king of search engines, Google assumed the throne in messaging security in this year's survey. While giving Google (Postini) Message Security service high marks across the board, readers particularly singled out its ability to detect and block spam, phishing attempts, viruses and spyware in messaging traffic, as well as its end-user transparency. Ease of integration with existing messaging applications, and ease of installation were also noted as high points.

SILVER

Barracuda Spam & Virus Firewall

Barracuda Networks

http://www.barracudanetworks.com

This year's second place finish goes to Barracuda Networks' Barracuda Spam & Virus Firewall. Respondents were impressed with the intangible features of this product, recognizing its return on investment and vendor service and support as high points. But its technical features are also strong: According to readers, it trailed Google only slightly in the categories of spam detection and blocking, and end-user transparency. Also of note were its solid scores for comprehensive and flexible reporting.

BRONZE

Websense Email Security

Websense

http://www.websense.com

Taking home the bronze this year is Websense Email Security with respectable scores across the board. Of all categories, readers noted the service's integration with existing messaging capabilities as its strongest point, followed closely by its spam detection and blocking, and its end-user transparency. Archiving support was also a stand-out feature for the software-as-a-service email security, and readers seemed generally pleased with its reporting capabilities and ease of installation.

READERS' CHOICE AWARDS '10 *Information Security*

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

MOBILE DATA SECURITY

Hardware- and software-based file and full disk laptop encryption, removable storage device (CD/DVDs, USB drives, digital music players) control, and smart phone and other handheld device data protection.

GOLD

Symantec Endpoint Protection Mobile Edition

Symantec

http://www.symantec.com/index.jsp

Symantec's security software for Windows Mobile and Symbian devices trounced the competition in this year's survey. Version 6.0 offers antivirus, antispam and firewall capabilities, and supports over-the-air management via Symantec Mobile Management. Readers gave Symantec high marks in numerous categories, including data and malware protection, central management, vendor service and support, and overall ROI, though the results indicated some would like to see support for a broader range of operating systems.

SILVER

Trend Micro Mobile Security

Trend Micro

http://us.trendmicro.com/us/home/

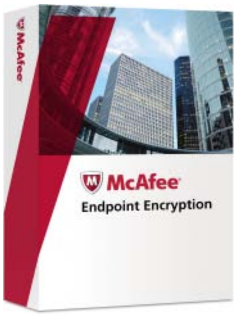
Trend Micro's product, which comes in SMB and enterprise editions, provides antivirus, firewall and intrusion detection capabilities, plus optional central management and at-rest data encryption. In earning this year's runner-up spot, readers gave the product its best marks for data and malware protection, and ease of installation, configuration and administration. They were somewhat less enthusiastic about the range of devices it supports—Symbian S60 and Windows Mobile—and its central management ability.

BRONZE

McAfee Endpoint Encryption

McAfee

http://www.mcafee.com/us/



McAfee's mobile security product, formerly known as Safeboot Encryption, rounds out the top three. As its name suggests, its marquis feature is encryption, covering everything from standard application databases and emails to other sensitive data types stored on Windows Mobile devices. Readers liked its central management features and data and malware protection, but were lukewarm on other features, and the product took hits on its ease of installation/configuration/administration and its vendor support.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

NETWORK ACCESS CONTROL

Appliance, software and infrastructure user and device network access policy creation, compliance, enforcement (802.1X, client-based, DHCP, etc.) and remediation products.

GOLD

Juniper Networks Unified Access Control

Juniper Networks

http://www.juniper.net

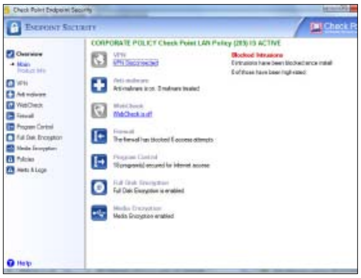
When users deploy NAC, they face the challenge of merging the technology into an existing infrastructure of legacy hardware and software. Luckily, this year's gold-medal winner, Juniper Networks Unified Access Control, received high marks from readers, particularly for its scalability and ease of integration. The Unified Access Control product is composed of centralized network access policy management servers, a downloadable agent that collects credentials and evaluates device status, and enforcement points that allow visibility of network and application traffic.

SILVER

Check Point Endpoint Security

Check Point Software Technologies

http://www.checkpoint.com



CORPORATE POLICY Check Point LAN Policy (283) IS ACTIVE

VPN
VPN Disconnected

Blocked Intrusions
0 intrusions have been blocked since install
0 of those have been high-rated

Anti-malware
Anti-malware icon. 0 malware treated

WebCheck
WebCheck is off

Firewall
The firewall has blocked 0 access attempts

Program Control
10 program(s) secured for Internet access

Full Disk Encryption
Full Disk Encryption is enabled

Media Encryption
Media Encryption enabled

The Check Point Endpoint Security product won second-place honors this year, and readers had high praise for its technical capabilities. Many respondents were impressed with the range of policy checks that the product could perform, its logging and reporting capabilities, as well as the ease of installing, configuring and administering the single-agent tool. Check Point Endpoint Security's integrated endpoint and network security capabilities, aside from NAC, include remote access VPN and optional event correlation and reporting.

BRONZE

TippingPoint Network Access Control

Hewlett-Packard

http://www.tippingpoint.com

Although the product finished just behind this year's gold- and silver-medal NAC products, readers applauded TippingPoint Network Access Control, specifically noting its enforcement options, its granular policy capabilities, as well as the variety of policies themselves. A few happy readers also felt strongly that they were getting their money's worth from the NAC tool. TippingPoint uses its NAC Enforcer to provide inline enforcement. The Network Access Control tool also offers out-of-band options using 802.1x or DHCP.

NETWORK FIREWALLS

Enterprise-caliber network firewall appliances and software, and stateful packet filtering firewalls with advanced application layer/protocol filtering.

GOLD

Fortinet FortiGate-1240B

Fortinet

http://www.fortinet.com/

Fortinet's FortiGate-1240B appliance provides a comprehensive and high-performance array of security and networking functions including protection against network, content, and application-level threats without degrading network availability and uptime. Readers praised FortiGate's ability to block intrusions, attacks and unauthorized network traffic, and its application-layer/protocol/HTTP controls, earning the product the gold medal. FortiGate also received high marks for its ease of installation, confirmation and administration. The FortiGate-1240B features a purpose-built processor, the FortiASIC Network Processor, to provide security throughput at switching speeds.

SILVER

Juniper Networks SSG, ISG appliances

Juniper Networks

http://www.juniper.net/us/en/

Earning the silver this year, Juniper Networks' SSG (Secure Services Gateways) and ISG (Integrated Security Gateways) appliances provide a comprehensive set of threat management security features. Readers rated the products highly for vendor service and support, ability to block intrusions, attacks and unauthorized network traffic, and central management. The SSG and ISG appliances also scored well for their application-layer/protocol/HTTP controls. The SSG series is designed for remote branch offices to large enterprises; the ISG series is designed for large enterprise, carrier and data center networks.

BRONZE

Cisco ASA 5500 Series

Cisco Systems

http://www.cisco.com/

The Cisco ASA 5500 Series Adaptive Security Appliances garnered the bronze this year, winning high marks from readers for their ability to block intrusions, attacks and unauthorized network traffic, along with their application layer controls. Cisco ASA 5500 also earned high ratings in the area of vendor service and support. The appliances, built on the Cisco PIX security appliance technology, provide application-aware firewall services with identity-based access control and denial of service protection.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

REMOTE ACCESS

IPsec VPN, SSL VPN (stand-alone and as part of application acceleration and delivery systems) and combined systems and products, as well as other remote access products and services.

GOLD

SonicWALL SSL VPN series

SonicWALL

http://www.sonicwall.com/us/index.html

The SonicWALL SSL VPN Series was well received by readers, scoring high marks across the board, most notably for its authentication support and investment ROI. The product line includes the SonicWALL Secure Remote Access (SRA) 4200 and SRA 1200 appliances, which provide easy-to-use, secure and clientless remote access for small and midsize organizations, and the SonicWALL Aventail E-Class SRA EX7000 and EX6000 appliances, which are designed to meet the needs of midsize and large enterprises.

SILVER

SA Series SSL VPN Appliance

Juniper Networks

http://www.juniper.net

Juniper Networks' SA Series SSL VPN appliances won the silver. Readers were impressed with the products' ease-of-use and transparency, as well as their compatibility with existing platforms and authentication; the appliances received a lower grade for vendor services and support. The appliances come in a range of models to meet the cost-effective requirements of small and midsize businesses up to large enterprises that require high-volume secure access and authorization.

BRONZE

Connectra

Check Point Software Technologies

http://www.checkpoint.com/

Readers awarded Check Point Software Technologies' Connectra with the bronze medal, giving the product high marks for end user transparency/ease of use and ease of installation, configuration and administration. The product also scored well in the areas of authentication support, integration and compatibility with existing applications, and vendor service and support. Connectra is a secure remote access gateway that integrates SSL VPN, IPSec VPN, and intrusion prevention. It's available as a turnkey appliance, as software for installation on open servers or as a virtual appliance.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

SIEM

Security information and event management and log management software, appliances and managed services for SMB and enterprise security monitoring, compliance and reporting.

GOLD

Symantec Security Information Manager

Symantec

http://www.symantec.com

After last year's second place finish in the SIEM category, Symantec took home the gold this year with its Security Information Manager. The product garnered top marks from readers for its ease of integration and compatibility with existing systems—an important feature for a product type known to require a longer deployment timeline. It also scored highly for its granular and flexible policy definitions, event correlation capabilities and data archiving, making it a solid standout.

SILVER

Trend Micro Control Manager

Trend Micro

http://us.trendmicro.com/us

Perhaps known more for its antivirus and anti-spam products, Trend Micro broke into the top three this year with its Control Manager. The product earned solid marks for its ease of installation—a feature for which SIEM is not generally known—and ROI. In addition, readers were generally pleased with its effective dashboard and ease of integration, and gave respectable marks for the product's ability to map data to policy or compliance requirements.

BRONZE

ArcSight ESM

ArcSight

http://www.arcsight.com

Coming in a close third was ArcSight's Enterprise Security Manager (ESM), which was singled out for its ability to map network and application data to security policy or compliance regulations: a key driver for many enterprise SIEM implementations. Readers also gave the product high marks for event correlation and the effectiveness of the dashboard in visualizing status and implementing policy, with only slightly lower marks than Symantec for data archiving.

UNIFIED THREAT MANAGEMENT

Unified threat management appliances for small and midmarket organizations, including firewall, VPN, gateway antivirus and other security capabilities, such as URL Web filtering and antispam. services for SMB and enterprise security monitoring, compliance and reporting.

GOLD

Check Point UTM-1, Safe@Office

Check Point Software Technologies

http://www.checkpoint.com/

Readers awarded the gold medal to Check Point Software Technologies' UTM-1 security appliances and Safe@Office UTM appliances. UTM-1 includes integrated centralized management, security updates, and hardware support. Safe@Office appliances provide small businesses with comprehensive protection, including firewall, IPS and anti-malware. Readers gave the products high scores across the board, but particularly liked their breadth of security functions/features, and depth of security provided by individual functions. The appliances were also rated highly for choice of optional security applications.

SILVER

SonicWALL NSA Series, E-Class Network Security Appliance Series

SonicWALL

http://www.sonicwall.com/us/

The SonicWALL Network Security Appliance (NSA) Series and E-Class Network Security Appliance Series won the silver, earning especially high marks for form factor effectiveness, but also strong ratings for breadth of security functions/features and ease of installation, configuration and administration. Readers also felt strongly that they're getting their money's worth with the products. The SonicWALL NSA Series, which replaced the PRO Series, combines several functions, including a deep-packet inspection firewall, intrusion prevention and Web content filtering. The E-Class series is designed to provide integrated gateway security without degrading network performance.

BRONZE

Cisco ASA 5500 Series Adaptive Security Appliance

Cisco Systems

http://www.cisco.com/

The Cisco ASA 5500 Series Adaptive Security Appliance picked up the bronze medal, winning readers over with its form factor effectiveness and breadth of security functions and features. Readers also rated the product highly for its return on investment. The appliance provides advanced intrusion prevention services, an adaptable architecture for speedy deployment, and secure remote access and unified communications. The ASA 5500 Series features a range of models to meet the needs of small businesses and branch offices to data centers.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

VULNERABILITY MANAGEMENT

Network vulnerability assessment scanners, vulnerability risk management, reporting, remediation and compliance, patch management, vulnerability lifecycle management.

GOLD

GFI LANguard

GFI Software

http://www.gfi.com

GFI LANguard™
Network Security Scanner and Vulnerability Management Tool

The GFI LANguard network security scanner and vulnerability management tool won top honors, garnering high marks from readers in most categories. Readers particularly liked the product for its ease of installation, configuration and administration, comprehensive and flexible reports, and remediation capabilities. GFI LANguard performs network scans using vulnerability check databases based on OVAL and SANS Top 20, providing over 15,000 vulnerability assessments. The tool allows administrators to deploy and manage patches on all machines across different Microsoft operating systems.

SILVER

FortiScan

Fortinet

http://www.fortinet.com/

Fortinet's FortiScan snagged the silver this year, winning praise from readers for its ease of installation, configuration and administration and for effectively and accurately identifying vulnerabilities in a timely matter. The appliance also received high scores for its scalability, remediation capabilities, and vendor service and support. FortiScan integrates endpoint vulnerability management, patch management, remediation, and auditing and reporting. A centralized administration console provides management of multiple FortiScan appliances.

BRONZE

Nessus

Tenable Network Security

http://www.tenablesecurity.com/solutions/

The Nessus vulnerability scanner, which Tenable Network Security offers in conjunction with its Security Center and Passive Scanner products, won the bronze medal. Readers gave the product high marks for effectively and accurately identifying vulnerabilities in a timely matter, and for ease of installation, configuration and administration. Survey participants also said they feel they're getting their money's worth with Nessus. The product features high-speed discovery, configuration auditing, asset profiling and sensitive data discovery.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
FACE-OFF
READERS' CHOICE
WEB 2.0
PCI
SPONSOR RESOURCES

WEB SECURITY GATEWAY PRODUCTS

Software and hardware products, hosted Web services for inbound and outbound content filtering for malware activity detection/prevention, static and dynamic URL filtering and application control (IM, P2P, etc.).

GOLD

Blue Coat ProxySG, ProxyAV

Blue Coat Systems
http://www.bluecoat.com/

Blue Coat Systems' ProxySG and ProxyAV products beat out the competition with high marks from readers for their ease of installation, configuration and administration plus their granular, flexible policy creation and enforcement. Readers also were impressed with the products' return on investment and vendor service and support. ProxySG appliances enable policy control over content, users, applications and protocols to protect users and networks from Web threats. ProxyAV appliances are designed for use with the ProxySG Full Proxy Edition appliances to provide inline threat protection and malware scanning at the gateway.

SILVER

McAfee Secure Web Gateway

McAfee
http://www.mcafee.com/us/

For the second year in a row, McAfee ranks in our top three with its McAfee Secure Web Gateway appliance. Earning the silver this year, the product was cited for its granular, flexible policy creation and enforcement, detection of known Web-based threats, and comprehensive and customized reporting features. The McAfee Secure Web Gateway integrates numerous protections from Web filtering and anti-malware to SSL scanning and content control, all with a simplified management footprint and a flexible policy engine.

BRONZE

SonicWALL Content Filtering Service

SonicWALL
http://www.sonicwall.com/us/

The SonicWALL Content Filtering Service garnered the bronze, receiving favorable reviews from readers for its granular, flexible policy creation and enforcement, ability to detect both known and unknown Web-based threats, and vendor service and support. SonicWALL CFS is built around a Web site caching and rating architecture that allows administrators to automatically block sites by category for easier administration. The appliance categorizes millions of URLs, IP addresses and domains in a continuously updated database to ensure high levels of protection.›

FAST & EASY
DATA LOSS PREVENTION

Enterprise DLP Without the Complexity

If you are looking for a complete data loss prevention (DLP) solution **(network, end-point, and discovery)** with a scalable architecture that is **fast-to-deploy** and **easy-to-manage**, then you need to look at Code Green Networks TrueDLP. Unlike other enterprise data loss prevention solutions, Code Green Networks enables the largest global organizations to **cost effectively start solving their data leakage problems in days not months**.

"Overall, we were impressed with the scalable and flexible performance of the tool and the all-inclusive nature of the [dlp] solution." SC Magazine, May 2010

Sign up now to see a TrueDLP product demo and enter for a chance to WIN a free Apple iPad:
www.codegreennetworks.com/demo/

CODE GREEN
NETWORKS

The drawing for the iPad will be held on December 1, 2010, no purchase required. Must be a United States resident to win.

NEW WEB, NEW THREATS

The collaborative nature of Web 2.0 introduces myriad threats to data that must be proactively countered.

BY DAVID SHERRY

THERE IS AN old Chinese proverb that reads "may you live in interesting times." For security professionals, this does not ring hollow because a security career is always evolving and responding to emerging threats; "interesting" is our daily mission.

While our charge is broad, from architecture and policy, through awareness and compliance, much of what we do is defending against threats to the security of the information we protect. As the proverb tells us, this is where the interesting portion of our role gets defined. We have witnessed the evolution of threats migrate from attacking the vulnerabilities of the Web, through the weaknesses of messaging, on to data protection, and now into the realm of Web 2.0.

What exactly is Web 2.0? You would find myriad answers to this if you asked all of your security (and non-security) friends. It is the Internet as we now know it, and is known as the second generation of the World Wide Web. Web 2.0 refers to Web design, development and use that foster interactive information sharing, interoperability and collaboration on and via the Internet. Examples include Web-based communities, Web applications, social-networking sites, video-sharing sites, wikis, and blogs. A Web 2.0 site allows users to interact with other users, or even change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is served to them.

With this next iteration come additional business opportunities, and security concerns. Chances are, your enterprise is either utilizing its power, or wondering how it can take advantage of it. Security needs to part of the conversation, no matter where you are in the process.

WEIGH BUSINESS NEED AGAINST WEB 2.0 RISKS

The collaborative, interactive nature of Web 2.0 has great appeal for business from a marketing and productivity point of view. Companies of all sizes and vertical markets are currently taking full advantage of social networking sites such as Facebook, Twitter and LinkedIn to connect with colleagues, peers and customers, or free online services such as webmail, Google Docs, and other collaborative platforms to share documents, best practices and message one another. "Ignore these technologies at possible business peril," says Diana Kelley, partner at SecurityCurve. "Not only are these technologies useful, but companies that don't adapt could well find themselves left behind the social revolution."

CISOs must find the delicate balance between security and the business need for these tools, and enable their use in such a way that reduces the risk for data loss or reputational harm to the corporate brand.

Companies are leveraging these sites for more than just communicating. Through Web 2.0 and social networking areas, enterprises are exchanging media, sharing documents, distributing and receiving resumes, developing and sharing custom applications, using social networks as a business strategy vehicle, leveraging open source solutions, and providing forums for customers and partners.

While all this interactivity is exciting and motivating, there is an enterprise triple threat found in Web 2.0: losses in productivity, vulnerabilities to data leaks, and inherent increased security risks.

I informally surveyed more than three dozen security colleagues across all verticals and found that 90 percent are concerned about these threats, and many have addressed (or are addressing) them through policy and technology. CISOs must find the delicate balance between security and the business need for these tools, and enable their use in such a way that reduces the risk for data loss or reputational harm to the corporate brand. While a sound security policy is a necessity in proactively responding to Web 2.0, policies must be enforced by technology.

The cost of dealing with a data breach continues to rise. In late January, the Ponemon Institute released its fifth annual study on the data breaches. The study reveals that the

average cost to an enterprise from a data breach rose from $6.65 million in 2008 to $6.75 million in 2009. In addition, the average cost per compromised record also went up to $204, from $202 the previous year.

With the increasing value to data, and the numerous conduits that it can be breached, it's no wonder that increasing regulatory mandates and constraints have been enacted. Enterprises now have a list of laws to comply with, including Gramm-Leach-Bliley, the Health Insurance Portability and Protection Act, Sarbanes Oxley, and the U.S. Patriot Act to name just a few. Many states are also enacting stringent protection and encryption laws, such as California's SB 1386, and Massachusetts' 201 CMR 17.00, and businesses may be subject to these state-specific laws even if they are not based in either state.

The industry is starting to respond by developing and marketing standalone tools—or integrating protection into secure Web gateways, antimalware suites or UTMs—that filter for sensitive content and alert or block the action. Many have received excellent feedback, and industry analysts are quickly evaluating the tools and solutions available. One size does not fit all, however, and holistic thinking and documenting your expectations and success factors are critical.

NEW PARADIGM OF WEB 2.0 SECURITY THREATS

As with any evolution of a product or service, the old ways of performing a task or providing a solution simply may not work. This is also true in reducing and mitigating Web 2.0 threats. Time tested security solutions are no longer the key defense in guarding against attacks and data loss. Some characteristics of Web 2.0 security that are being discussed are:

- Traditional Web filtering is no longer adequate
- New protocols of AJAX, SAML, XML create problems for detection
- RSS and rich Internet applications can enter directly into networks
- Non-static Web content makes identification difficult
- High bandwidth use can hinder availability
- User-generated content is difficult to contain

Security teams must be aware of the need to address Web 2.0 threats in their desktop clients, protocols and transmissions, information sources and structures, and server weaknesses. While none of these attack vectors are new, how we respond to them may be.

Very rarely does a week go by where we do not hear news of the negative aspects of social networking sites and collaborative platforms. Whether it is violence and lawlessness, cyber-bullying and harassment, or legitimate breaches of confidential data, it is apparent that this brave new world poses risks to companies. Many of the threats that lead to confidential data loss hijack employee credentials without their knowledge. While there are obvious threats that would not surprise even the most casual user of the Internet, others are more subtle and benign, and need to be addressed in our enterprises.

Direct posting of company data to Web 2.0 technologies and communities is the most common. No vulnerability need be exploited or malicious code injected when employees (whether as part of their responsibilities or not) simply post protected or restricted information on blogs, wikis, or social networking sites. According to many security companies, the attacks on these technologies are on the rise as well, knowing that their growth and fast maturation can be a jackpot for insider information. Many of these attacks also come via malicious payloads, which are downloaded when spam and phishing scams are utilized. According to Sophos, 57 percent (an increase of more than 70 percent from the previous year) of people who use social networks report receiving spam and phishing messages. This number will surely continue to rise.

However, what about the risks posed by insiders who choose to utilize free webmail services, such as Gmail, Yahoo, Hotmail, and others? While allowing employees to access these services during the workday most likely aligns with an acceptable use policy that allows "reasonable and limited personal use," the risk is what they are sending to these free mail services. They may be thinking that they are being good stewards of the company and sending data home to work on at night or over the weekend, but they are also placing the company at great risk. Not only are the transmissions not encrypted, but the security of the servers may not be up to security requirements for the protection and value of the information. The data may be residing on several servers, and may not even reside in the country of origin or destination.

INCLUDE WEB 2.0 SECURITY IN ACCEPTABLE USE POLICY

Most enterprises already have a form of an acceptable use policy, which should govern the use of all resources in the enterprise computing environment. While it may be implicitly implied in your current policies that public Web 2.0 sites are covered (blogs, wikis, social networks), because of the nebulous nature of this technology, a more explicit rendering of the expectations and policies is necessary.

Critically read your current policy in a context of Web 2.0 technologies, and identify gaps that need to be addressed. For instance, because of the risks and inherent difficulty managing the use of social networking applications, many enterprises have made the decision to not allow access to social networking services and Web 2.0 powered sites from inside the corporate perimeter (often with the exception of human resources departments for recruiting purposes). This is an important decision because the information gained from these sites may be of corporate use. One security manager from a global manufacturer told me "there is no way we are going to design new ingredients for client products, and then prevent our employees from the public forums that enable us to gather the consumer experience."

> One security manager from a global manufacturer told me "there is no way we are going to design new ingredients for client products, and then prevent our employees from the public forums that enable us to gather the consumer experience."

Of greatest importance is a clear and unambiguous warning in the policy about sharing confidential corporate information. Enforcement of the policy can be made though analysis of Web logs for use during business time (if not allowed), or through automated searches of websites for corporate information. Many organizations have included Web 2.0 and data protection sections to their training on protecting corporate information. Ensure that the

policy indicates the prohibitions against this, and clearly spells out the ramifications, including the levels of discipline that could occur. As always, when the acceptable use policy has been modified, ensure that all employees are made aware.

MAINTAIN YOUR TECHNICAL DEFENSES

Security success is all about combining the right combination of people, process, policy and technology. The same holds true when it comes to addressing Web 2.0 concerns. Utilizing this combination in a rapidly evolving area is difficult though. "This space is a reality and tough to fully monitor as there is a fine balance to levels of security rigidity and the inherent pervasive openness to Web 2.0," says Tim Young, director of technology at Resource Systems Group. Intrusion detection and intrusion prevention systems (IDS and IPS) need to be kept current to address the risks of this traffic, and bandwidth-shaping technology should be deployed in order to not only both maintain proper network speed, but also identify abuse or compromised machines.

AWARENESS

Leverage Risks to Teach Web 2.0 Security

REACH OUT TO BUSINESS UNITS TO BUILD AWARENESS AROUND WEB 2.0 THREATS.

Web 2.0 security risks may threaten confidential data, but smart security managers can also leverage them to enhance security awareness throughout an organization, and build convergence with key decision makers and leaders.

Web 2.0 and social networking are familiar terms, but may not conjure up risks to the enterprise. Many other areas of the corporation, while focusing on risk and some aspects of security, may need to be educated and consulted when creating a policy and modifying an appropriate use policy. Include senior representatives from human resources, risk management, privacy, physical security, audit, and legal in your preparations and response to these risks. A stronger partnership, and ultimately a stronger policy and process, will surely result from reaching out to them.

Establish a working group to meet periodically to discuss how this technology is emerging and evolving, and how the enterprise as a whole can address it. In addition, use formal training, newsletters, "lunch and learns," or any avenue possible to make employees aware of the proper and improper use of social networks, at work and at home.

As with many security issues and risks, a higher level of awareness points to a higher level of compliance. Use data protection as an essential teaching tool, and increase your education and awareness beyond passwords and acceptable use. Using your working group, encourage cross-functional responses for awareness, and speak with data. ›

—DAVID SHERRY

In addition, many popular Web-based social network services have an increasing number of applications available to download locally. While many are benign, a significant number of these small apps carry malicious payloads, hacking tools or marketing software. This can be combated by having a standard desktop image that does not allow local installation of applications, or changes to the registry keys or operating systems. Lastly, firewall rule sets can be granularly defined to monitor, catch or block social network traffic, and of course, always ensure that antivirus products are up to date as a last line of defense.

Finally, even with all of these controls in place, data and information will inevitably find its way to the Internet. Enterprises should remain vigilant in scouring the Internet regularly for any information that may be sensitive in nature. Using third-party reputation protection services, internal monitoring programs, or simply performing Web searches for keywords and phrases can be essential in identifying and addressing instances when company information is made available via social communities, either inadvertently or intentionally.

DATA PROTECTION VIA OUTBOUND CONTENT MANAGEMENT

There are many vendors and solutions that promise to mitigate and solve the threat of data loss in Web 2.0 environment. While this technology area has shown great promise, and continues to deliver, it is oftentimes misunderstood as a CISO reviews the morass of materials and reviews available.

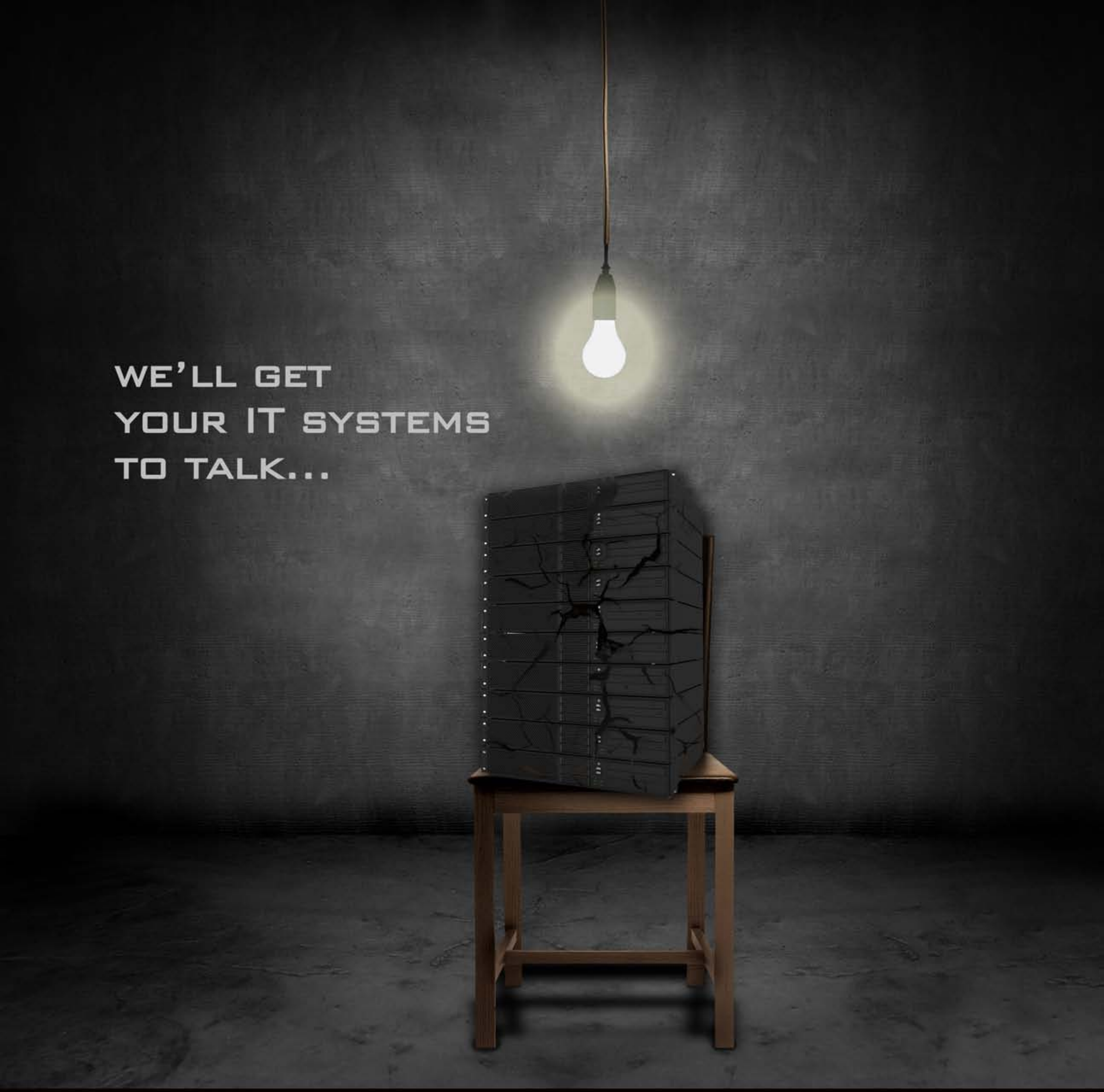
Data loss prevention, for example, is a solution, as well as a generic term that is an umbrella for many different technologies and strategies. Data loss can be prevented by encryption. It can also be mitigated or prevented by port blocking or content fiiltering. And there are software suites and appliances that can help in this area. Every security vendor of any size or maturity will gladly let you know of their DLP solution, and will use the term to cover just about all of their products. This doesn't make it any clearer.

A clearer definition can be simply stated as implementing an outbound content management program that reduces, mitigates, and eliminates data loss.

A clearer definition can be simply stated as implementing an outbound content management program that reduces, mitigates, and eliminates data loss. The trick is how a company deploys systems capable of successfully detecting your highly sensitive information in the outbound mail system.

Also be aware of the types of DLP solutions, which fall into three broad categories: network based, host-based, and data identification. All three have their positives and negatives, and a CISO must remember that a performance hit will be observed on the network when a company runs any such solution inline. As with all security solutions, you need to strike a balance between speed, accuracy, and adequate coverage.

DLP solutions must be made aware of what a company lists as sensitive content if they are to be successful. Upon the sensitivity being listed, there are several ways in which the content can be identified, but first the solution must be able to open and understand numerous file types, and be able to detect content in nested and zipped documents as well.


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

Once the files are opened and reviewed by the solution, content analysis is begun to identify any sensitive data. Content analysis techniques include:

- Pattern-based searches using regular expressions
- Fingerprinting by searching elements of actual databases
- Exact file matching
- Statistical analysis to search for content that may resemble sensitive data, or contain pieces of it
- Document matching for complete files
- Analysis of lexicons (e.g., employment opportunities, insider trading, harassment)
- Solution supplied categories, to address regulatory mandates such as HIPAA and GLBA

WEB 2.0 SECURITY STRATEGY MUST MIX TECHNOLOGY, POLICY

Security teams must be aware of the need to address Web 2.0 threats in their desktop clients, protocols and transmissions, information sources and structures, and server weaknesses. While none of these attack vectors are new, how we respond to them may be. Our enterprises ask us to eliminate malware and protect our company's data, all while allowing productivity, improving IT efficiency, and proving compliance. We should be encrypting our data and protecting our endpoints, but not hinder the process of how we do business. Add in the realities of an evolving Web and its use, and our task is a large one. The good news is, with preparation and process, we can be successful.

> Our enterprises ask us to eliminate malware and protect our company's data, all while allowing productivity, improving IT efficiency, and proving compliance.

The first step is to embrace Web 2.0 and create a strategy and toolset to maximize its benefits. A CISO must proactively identify the risks, but use this information to increase awareness and inform the business of their possibility. Gone are the days of "fear, uncertainly, and doubt" because board level management now looks to security for business success.

Next, document a strategy that is based upon business objectives, and clearly indicate what to allow, what to block, and who should have access and when. New policy should be developed, or a current policy set be updated, and they should be clear and enforceable. Ensure that your policies address Web 2.0 technologies, and consider subjective policy setting, group level access, and productivity based sections to give your policy strength. Revisit your acceptable use policy, and look at it from a Web 2.0 lens, and be sure to cover new technologies such as anonymizing proxies. Include other groups for support such as HR, legal and audit.

After the policy set is in place, focus on data loss protection, and stopping any information from exiting your network before it happens. You need to protect and comply with regulatory mandates, all without disrupting the business processes. A solution that monitors, prevents, alerts, encrypts, and quarantines as needed is necessary. Deploy a solution that is capable of stopping sensitive data from leaving via your outbound mail system. Your filtering system should analyze and act on outgoing email in real time, in order to not impact productivity, and be able to perform searches in nested and zipped files and attachments.

A DLP solution should be part of an overall, integrated security architecture that includes a vigilant antivirus program, a robust anti-malware protection program, and the capabilities of an AJAX-aware analysis platform. In addition, make sure your browsers (and their plug-ins) are patched, and do not simply focus on the critical patches, because all vulnerabilities are targets in Web 2.0.

WEB 2.0: WITH PROGRESS COME RISKS

As with all emerging technologies, Web 2.0 and its related components are advancing rapidly, and security professionals need to remain aware of the risks and defenses associated with it. There is a generation entering the workforce ("digital natives") that assumes this technology will not only be available for their use, but is also essential to the way they communicate with colleagues and business partners. In addition, businesses are realizing the reach and depth they can achieve with a social media marketing strategy.

While there are many benefits that come with this new Web internally and externally, the policy, technology, people, and architecture to defend against the risks must be addressed proactively and not taken lightly. CISOs are the vanguard of their organizations in this regard, and through this effort, further solidify their value to the business.

Interesting times, indeed.▸

David Sherry is CISO at Brown University. Send comments on this article to feedback@infosecuritymag.com.

HELP NET SECURITY
PCI Compliance for DUMMIES
FREE GUIDE
SECURITY NEWS
Spotlight
Are hackers finding a way into your network?
FREE BOOK
Receive daily security news by e-mail

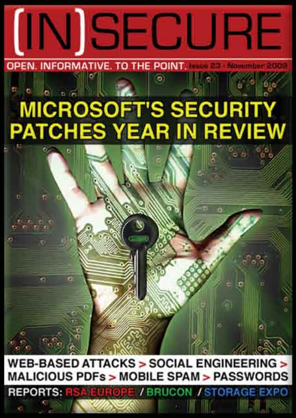

(IN)SECURE
OPEN. INFORMATIVE. TO THE POINT. Issue 23 - November 2009
MICROSOFT'S SECURITY PATCHES YEAR IN REVIEW
WEB-BASED ATTACKS > SOCIAL ENGINEERING > MALICIOUS PDFs > MOBILE SPAM > PASSWORDS
REPORTS: RSA EUROPE / BRUCON / STORAGE EXPO

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

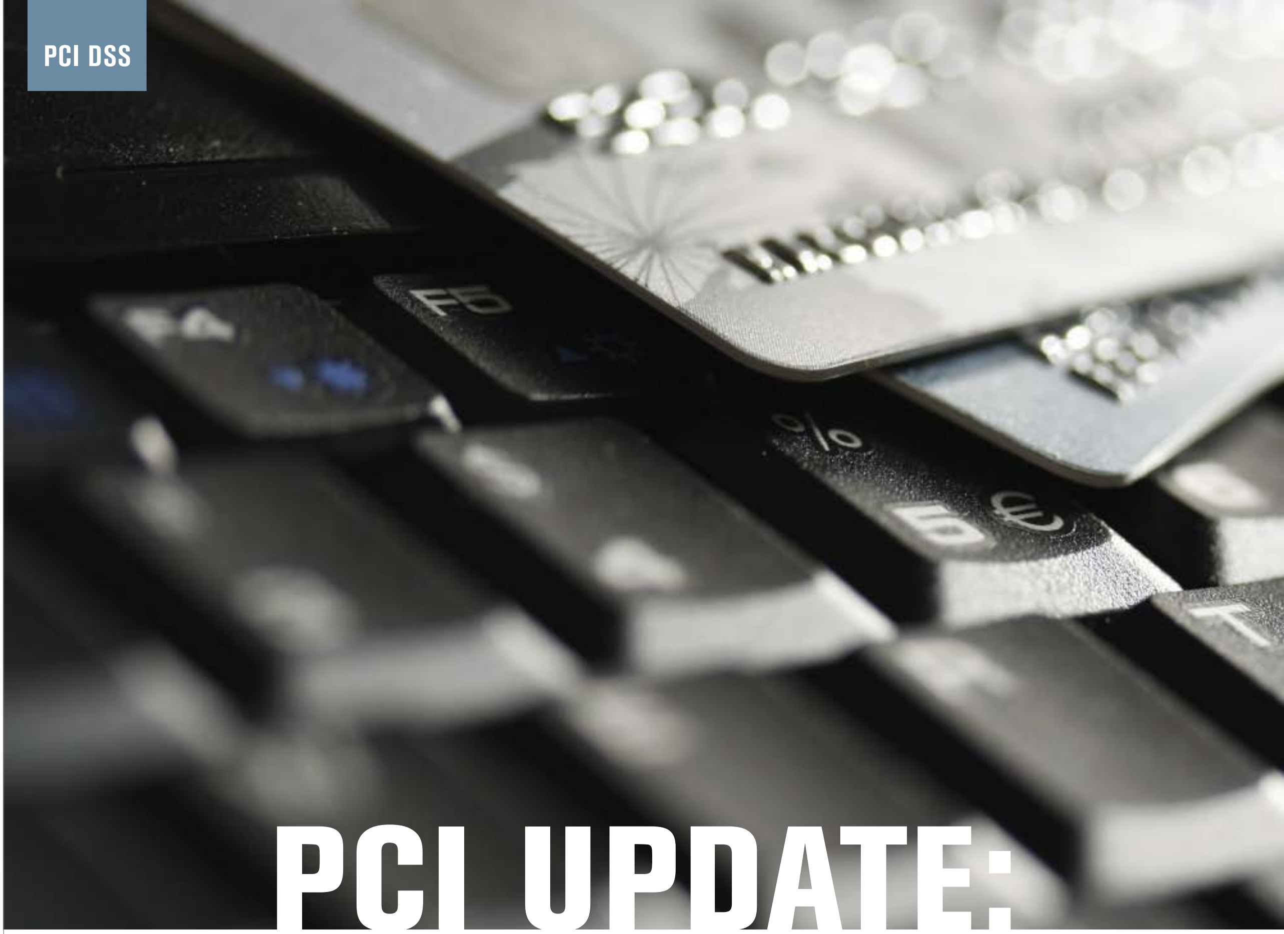
FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES



PCI UPDATE: CLARITY OR CONFUSION?

What you can expect from this fall's update to the Payment Card Industry Data Security Standard.

BY GEORGE V. HULME

PCI DSS has become one of the most controversial standards on the books. Many argue that PCI DSS has made great inroads in improving credit card security. Others contend the standard is a distraction from true security, and that the effort is too prescriptive, confusing, and artificially sets the bar for security and compliance too low. This fall, the PCI Security Standards Council is expected to release a series of updates to the standard.

PCI VIRTUALIZATION AND IN-SCOPE GUIDANCE COMING

What can retailers, merchants and others who handle credit card data expect? Most are hoping for a number of updates that will remove perceived overly subjective interpretations, questions of scope and answer long-awaited virtualization security questions. In August, the PCI SSC released a high-level summary of changes to appear in PCI DSS 2.0. A detailed summary and pre-release version of the standard is scheduled for release in September with a final version published Oct. 28. According to Bob Russo, general manager, PCI Security Standards Council, most of the updates this year will come in the form of standard clarifications, as well as the release of guidance.

The virtualization update, led by the virtualization special interest group (SIG), is expected to clarify existing ambiguity around how merchants can utilize virtualization technologies and still maintain compliance.

"The council does need to provide a supplementary guide for virtualization as there has been plenty of confusion in the marketplace," says Anton Chuvakin, Ph.D, independent security consultant and co-author of *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance.* "Section 2.2.1 states that there can only be one function per server. If the council means physical server, then that would, in effect, ban virtualization. But it could also mean virtual servers; and in that case merchants can use one physical server running separate, but dedicated virtual servers," he says. "But they have yet to officially explain what is allowed, and how that all fits together."

"The council does need to provide a supplementary guide for virtualization as there has been plenty of confusion in the marketplace."

–ANTON CHUVAKIN, Ph.D,
independent security consultant and author

How is such haziness in the standard currently clarified should retailers deploy virtualization? Those that do must assert to their Qualified Security Assessor (QSA) that each virtual machine is, in fact, a dedicated server. And, unfortunately, the outcome boils down to the interpretation of the standard by their individual QSA.

"Some merchants are moving forward and adopting virtualization, while others have put off embracing it around payment systems," says Josh Corman, research director, for research firm 451 Group's enterprise security practice. But the question remains why, with virtualization hitting stride back in 2006, has it taken the PCI Security Standards Council so long to address virtualization?

"Everyone initially thought virtualization guidance was coming out in October 2008, and it didn't. We had to wait another two years to adopt cost savings technology? That is just ridiculous," says Corman.

Scott Crawford, managing research director, Enterprise Management Associates, however, argues that developing the appropriate level of virtualization security controls isn't as straightforward as it may seem. "Virtualization technology, for example, can be deployed in a number of different ways. And some approaches are vendor- or implementation-specific to boot. Defining an approach that is too prescriptive may not address the full scope of the issue, or may add substantially to the sheer volume of requirements if regulators attempt to cover all of the potential bases," he warns.

Another highly anticipated update this year is expected to be clarification surrounding what systems are in, and out, of PCI DSS regulatory scope. "I would argue some of the clarifications coming from the scoping SIG are going to be the most important," says Michael Dahn, PCI principal at Verizon Business, and member of both the virtualization and scoping SIGs. "That's where people find the most gray areas under the mandate." Generally, PCI DSS scope is defined as any system that stores or processes unencrypted credit card data. Sounds clear-cut. Yet while a business may separate all systems that store or process credit card data, they still may use a shared Active Directory, or perhaps a shared administrative LAN to manage other areas of their infrastructure as well as those systems dedicated to payments.

"There's nothing to say that the Active Directory or administrative LANs are in scope, but there's nothing to say that they aren't, either. And it's a gray area that continuously comes up," Dahn says.

According to Russo, proposed changes will recommend that merchants use data discovery tools or data leakage protection technology to discover where cardholder data resides on their systems prior to a PCI assessment.

Proposed changes also address secure coding and vulnerability discovery, including a recommendation that merchants apply a risk-based approach for addressing vulnerabilities.

What is not expected to be in the update is any further guidance when it comes to cloud computing. "Ultimately, it is the merchant's responsibility to make sure that they have the right contracts in place, and make certain that their providers are working in a compliant manner," says Russo. "As part of their due diligence, merchants need to make sure they are dealing with someone reputable," he adds. "The council will continue to rely on section 12.8, which governs the use of third-party providers, and states that the merchant must ensure that the provider is compliant to PCI DSS," says Chuvakin.

"Ultimately, it is the merchant's responsibility to make sure that they have the right contracts in place, and make certain that their providers are working in a compliant manner."

–BOB RUSSO, general manager, PCI Security Standards Council

For many, that's not enough clarity, and will continue to be a sticking point for some time to come. "There are too many vagaries associated with making sure service providers are compliant," says Gartner IT security, fraud, and PCI compliance analyst Avivah Litan. "What's needed and warranted is specific advice on how to make sure service providers are compliant, and what that means to the compliance status of the service providers."

PCI'S UPDATE TIMETABLE UNDER SCRUTINY

Some contend that PCI DSS moves too slowly to adapt to rising new technologies and attack trends. For instance, years ago a number of high-profile retail breaches were blamed, at least partially, on insecure wireless LANs such as the famous TJX Companies attack discovered in December 2006. But it wasn't until July 2009 when the PCI Security Council released a 28-page wireless security guide that provided guidance on how merchants could safely utilize wireless LANs in their operations.

"There is turbulent, rapid change in the IT industry, and to have a list of static controls

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

FACE-OFF

READERS' CHOICE

WEB 2.0

PCI

SPONSOR RESOURCES

IMPACT

For Better or Worse?

Experts debate whether PCI has improved credit card security.

Is PCI DSS a merchant security savior or antagonist? Strong arguments are made on both sides of the debate. Some contend prior to PCI DSS that retailers and payment processors did hardly anything to ensure credit card security. "PCI has improved security," says Gartner IT security, fraud, and PCI compliance analyst Avivah Litan. "Unfortunately, compliance typically drives implementation of security solutions and the fact that merchants have had to comply with PCI has forced them to pay attention to the security in their environments and work on improving it," she adds.

That was certainly the spirit of PCI DSS when, by 2004, it became clear that when it came to securing credit card data something had to improve. Roughly a year after California enacted its data breach notification act, SB 1386, reports of breached credit card and other financial information were beginning to flow furiously. Among the breaches in that era included one of the largest of all time, CardSystems Solutions, encompassing 40 million credit card records in 2005.

Going into effect in 2004, the Payment Card Industry Data Security Standard (PCI DSS) aimed to stem the tide of credit card breaches and lower the costs of fraud on the industry and consumers. PCI's 12 discrete security requirements establish common procedures and security practices for handling, processing, storing and transmitting credit card data. Those mandates call on retailers and payment processors to create a risk management program that includes: segmenting cardholder data; encryption; vulnerability management; running antivirus software and intrusion detection systems; among other requirements.

However, many merchants argue that the standard has been confusing to comply with, and excessively expensive to maintain. That's a contention many PCI DSS experts disagree.

"I say PCI DSS 'done wrong' is usually expensive," says Anton Chuvakin, Ph.D, independent security consultant and co-author of *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance.* "For instance, securing a flat network is very hard and expensive, and securing card data on legacy systems is expensive. In those scenarios, it is usually cheaper to reconsider business processes that utilize card data and streamline them," he says.

Scientific data as to whether those efforts have increased overall merchant security is difficult, if not impossible, to uncover. However, according to the DataLoss Database, run by the Open Security Foundation, there were 24 incidents involving credit card data in 2005, while for all of 2009 there were 86.

"There's no doubt that the frequency of credit card breaches, and the number of cards involved in those breaches, has been increasing," says Josh Corman, research director, for research firm 451 Group's enterprise security practice. Still, that data doesn't necessarily mean that PCI DSS has failed, as the trend could be attributed to an increase in the number of states with database breach disclosure laws on the books as well as more merchants accepting online payments.

When it comes to the overall impact PCI DSS has had on retailer security, some argue that the standard actually creates a disincentive among some businesses to get by with less security than they would have otherwise.

"I think a lot of people miss the point that PCI was really intended to be the floor, not the ceiling. It was intended to define at least a minimum standard. Many organizations subject to it, however, too often see it as the ceiling. "If I'm in compliance, then I don't need to do more," says Scott Crawford, managing research director, Enterprise Management Associates. ▸

—GEORGE V. HULME

just doesn't seem to make sense," says Corman. "You can regulate things such as car seat belts because the laws of physics don't change, but attack techniques change all of the time, and PCI DSS moves too slowly to adapt to the threats," Corman says.

Others argue that compliance to PCI DSS should be agnostic of technological change. "If we constantly wait for someone to be prescriptive about how we are going to apply a control, then we are thinking about it the wrong way," says Dahn. "Each of the PCI DSS requirements—restricting access, access controls, audit logging, network segmentation, antivirus, two-factor authentication, and others—can all be applied to any technology," he says.

However, some businesses have shied away from innovative technologies out of the simple fear that they may not pass a PCI DSS audit. "Sometimes these mandates can stop innovation," says Corman. "If your business wants to change and outsource or embrace cost-saving technology, PCI DSS mandates can force them to put on the brakes," he says.

Those who would like to see a more agile, rapidly updated standard could be in for disappointment since the council decided this summer to move to a three-year update cycle for the standard. "We are always looking for ways to improve the standard, and one of those is how to improve the update cycle. Some feel the standard is changed too often, others feel it's not updated enough," says Russo. "But if you look at the standard over the past number of years, it's stood the test of time and hasn't changed much."

No matter what the final updates to the standard look like later this fall, chances are they won't be detailed enough for some while too detailed for others.

"You can regulate things such as car seat belts because the laws of physics don't change, but attack techniques change all of the time, and PCI DSS moves too slowly to adapt to the threats."

–JOSH CORMAN, research director, 451 Group

"The notion of being prescriptive can be both good and challenging," says Christofer Hoff, director, cloud and virtualization solutions, Cisco Systems STBU (Security Technology Business Unit). "Just consider the business ecosystem involved with what the PCI DSS affects. When you make a change to something like that, it cascades down through hundreds of thousands if not millions of merchants. So one seemingly simple change to security folks could affect the operational capabilities of lots of businesses," he says. "I'm not making an excuse for it, but it is a very delicate situation."

Analyst Crawford agrees. "Particularly in IT security, compliance is a bit like trying to correct astigmatism. A lens that sharply focuses on one area may distort the focus elsewhere. Make requirements too prescriptive and you may be forcing organizations to comply with something that may no longer be relevant, especially if attack trends have moved on since the requirement was defined," he says. "Make them less prescriptive, and you make it difficult to hold subject organizations to a well-defined standard," adds Crawford.

No doubt even after the final updates are published this fall, the debates surrounding PCI DSS won't subside any time soon. However, the council's Russo is sure of this about the standard: "If you are a retailer, and you want to stay secure, becoming compliant to PCI DSS is the best thing you can do." ▸

George V. Hulme is a freelance writer in Minnesota. Send comments on this article to feedback@infosecuritymag.com.

ADVERTISING INDEX

INFORMATION SECURITY®

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 DIRECTOR Robert Westervelt

ASSISTANT EDITOR Maggie Sullivan

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Greg Smith

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 Nick Dowd

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER
Allyson Kinch

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Andrew McHugh, Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@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 Jeff Wakely

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

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

TechTarget
Where Serious Technology Buyers Decide