PLUS: Truth, Lies and Fiction about Encryption

INFORMATION SECURITY®

SEPTEMBER 2009

2009 READERS' CHOICE AWARDS

YOUR CALL ON THE INDUSTRY'S BEST

ALSO

Schneier-Ranum Face-Off:
Is perfect access control possible?

TechTarget
The Technology Media ROI Experts

INFOSECURITYMAG.COM

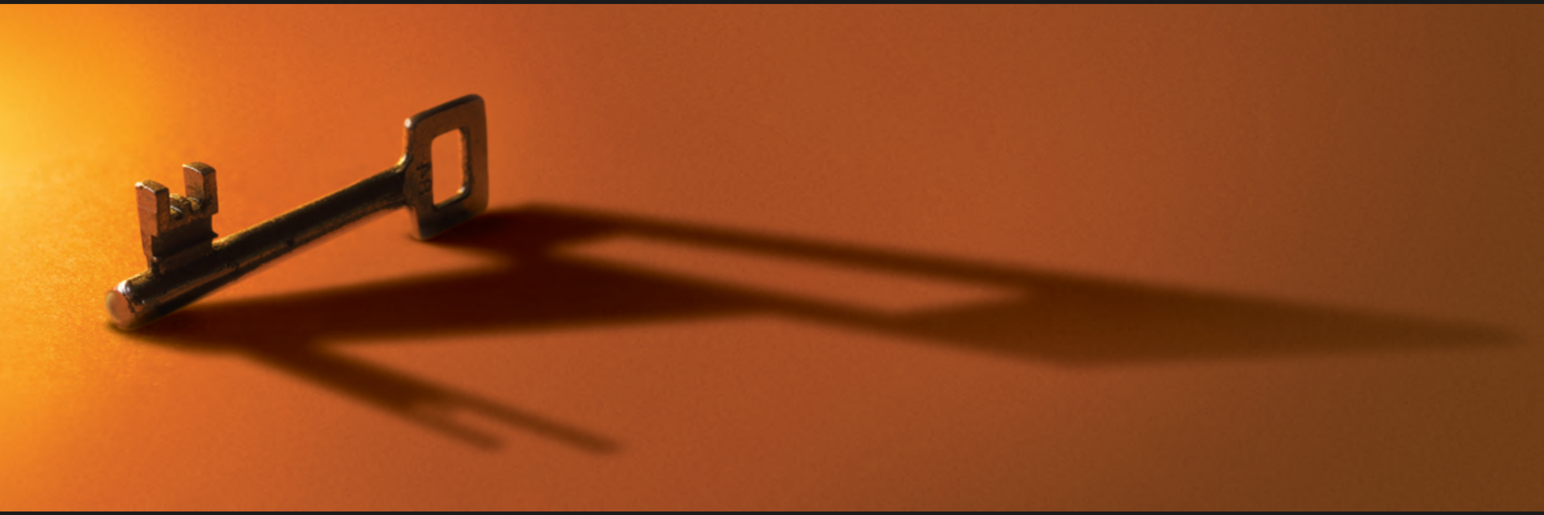
contents

SEPTEMBER 2009

VOLUME 11 NUMBER 8

FEATURES

ALSO



What Does PCI Compliance Really Mean?

BY KELLEY DAMORE

Passing an audit can lull an organization into a false sense of security.

WHILE PCI HAS PROBABLY HELPED fund many a security project and infused lots of dollars to security vendors in the last three to four years, why are companies that are PCI-compliant getting compromised?

The problem lies in the fact that security professionals and their bosses are still under the false impression that compliance equals security.

Interestingly what some originally found as refreshing (clear language and guidance) are now the things that hinder the standard. Because PCI is very prescriptive and lays out exactly what needs to be done, it can lull an organization into a false sense of security.

Just look at Hannaford and Heartland Data Systems. Both were PCI-compliant but both were compliant at *one particular moment* in time.

Recently, Heartland Data Systems CEO Robert Carr blamed the QSA for its huge data breach woes. The problem is a seal of approval from an auditor does not in any way shape or form ensure that your organization is secure.

Many in the security industry were up in arms over his statements, arguing that Carr was shirking his responsibility as the CEO. And while he may not have understood security per se, he should have understood the risk his company faced and made a business decision based on Heartland's risk threshold.

While we'll never know the conversations that occurred before the breach, his comments prove that something was very broken. Either top Heartland business executives were told or believed that if they were PCI compliant, that they would be safe or they did not have a strong risk management program in place to begin with. Now Heartland is the poster child for shoddy security and will pay the consequences.

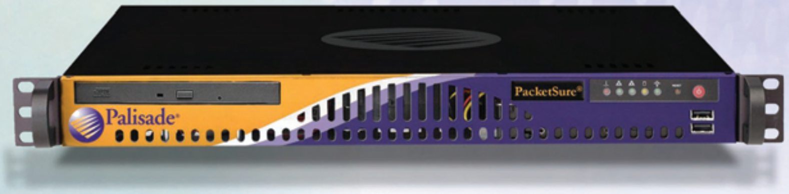
As a security professional, there are lots of lessons to be learned by the Heartland breach.

First, organizations need to articulate risk to their top leaders and in terms they understand. They need to be crystal clear that a passed audit is just that. And meeting something a standards body or a legislator puts together is not a security program. While compliance can help get money, it should be a justification for dollars on projects that you really need to get done to protect the organization (and meet a particular compliance mandate.)

Regulations and industry standards are not going away. PCI, which began as a standard, is getting even more powerful. Recently Nevada lawmakers made it legally binding for businesses accepting payment cards to be PCI compliant.

The challenge for security pros is to use these mandates as a budget lever but also clearly articulate what an organization is getting from those investments. And while a good security and risk management strategy is very important, no organization is hack-proof.▸

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


Palisade
PacketSure

VIEWPOINT

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

Cloud Computing or Outsourcing, Take Your Pick

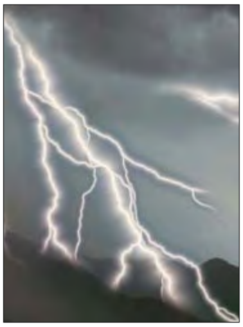
This is in response to "Tread Carefully into the Cloud" (Perspectives, June 2009). Several issues highlighted topics related to cloud computing, especially its information security risk implications.

A trend arose in recent years, which is IT outsourcing, where many organizations have their data centers, information security, operations processing, etc., outsourced outside to specialized third parties. With the discussions regarding cloud computing, I can see many similarities between the two that might make cloud computing an old business that was started some time ago, however under a different name.

Part of these many similarities is coming from the risks they expose, along with regulations and compliance issues.

I would appreciate if you can include in your coming issues a article that sorts out the differences between the two topics: outsourcing vs. cloud computing.

—Bassil Mohammad, Information Security Assistant Manager, Arab Bank Plc



> "I can see many similarities between the two that might make cloud computing an old business that was started some time ago, however under a different name [outsourcing]."
>
> —Bassil Mohammad, Information Security Assistant Manager, Arab Bank Plc

COMING IN OCTOBER

Security 7 Awards

Information Security magazine will announce its fifth 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; education; and utilities. Past winners have included luminaries such as Dorothy Denning and Gene Spafford, a 2008 winner. Other winners from year included: Guardian Life Insurance's Mark Sokol; Stanford Hospital's Michael Mucha; Rogers Communications' Martin Valloud; the California Office of Information Security and Privacy Protection's Mark Weatherford; Gaylord Entertainment's Mark Burnette; and Motorola's Bill Boni.

Application Security

Application developers and information security teams usually don't encounter one another unless an incident has occurred. And even then, vulnerabilities are usually patched and the hunt for the root cause of the problem is short lived. This article will offer nine tips to help you improve application security after an incident.

Easing the Burden of SOX

The cost of Sarbanes Oxley compliance for thousands of smaller public companies is disproportionate, both in terms of percentage of revenue and cost per employee, as opposed to large enterprises. This article will look at how to approach SOX compliance in a midmarket organization, who internally needs to be involved and what resources are at your disposal.

IN EVERY ISSUE: Expert opinions, news analysis and lots more available for download and online at www.searchsecurity.com.

Personal Responsibility

Accountability for Internet security should be placed on users, not service providers such as hotels. BY RICK LAWHORN

OVER THE PAST YEAR, I have read about multiple security breaches encountered by celebrities and business travelers at hotels and resorts around the globe. I have seen the research and assessments that try to gauge the hospitality industry's security posture. Most of the reports tend to label the industry as one of the worst with regard to information security. However, it's time to place accountability where it needs to be: with each of us.

To better understand the security issues in the hospitality industry, we need to examine two distinct parts: the hotel network that processes payments, stores personal information about guests and conducts routine services as a part of everyday business, and the Internet connectivity offered as an amenity to guests.

Hotel networks typically are made up of many different proprietary systems in order to offer services and track expenses for each guest. These systems also provide service continuity throughout different departments or areas of the hotel or resort. The goal is to provide an easy, natural flow of identification and responsiveness to guest needs as they use different areas within the establishment. The greater the speed in identification and awareness of personal preferences associated with the guest, the more personal the experience will be; we can all remember the places we have stayed where we felt recognized. These are the systems that hotels or resorts are responsible for securing.

The Internet services hotels offer their guests as an amenity is similar to their offer of an indoor heated swimming pool: It is available to guests and there are certain rules that should be followed to enjoy it safely. But just as the hotel or resort should not be held accountable if someone decides to do a triple gainer in the shallow end, they shouldn't be held responsible if a guest logs onto his company's webmail without SSL on the hotel's Internet service. It is our responsibility as guests to protect our assets and our data while using it. Hotels and resorts are not in the business of being technology people, lifeguards or the police. They provide amenities and it's up to us to use them with common sense.

If we bring a laptop with us to a hotel or resort, we are responsible for making sure it is secure before it is on the network. If we use the business office computer at their location, we need to make sure that we clean up after we are done. This can involve not forgetting disks and flash drives, and cleaning out the private data in the browser. If we connect wirelessly, we need to make sure that our sensitive communications are using strong encryption. The hotel provides the service just like your home Internet service provider; normally, the security provided with the service is set to a bare minimum and always requires you to add security controls to protect your data. It's up to each of us to have updated patches, antivirus, a firewall, intrusion prevention, secure communication and to turn off services that would provide access to files and service on our equipment.

There is no excuse or reason to rely on a service provider to protect us. To do so can cause a great deal of problems later and could impact your work or home upon returning.

Now if a hotel business network utilizes the same network that guests use, there is cause for concern. Not only would that violate general best practices in information security, but it would also violate PCI regulations and potentially impact Sarbanes-Oxley compliance in public companies. In many businesses across the hospitality industry, guest Internet services are available on the guest network only, which is completely isolated from the hotel business system. Unfortunately, today there is no way to ensure this separation exists. This is a great opportunity for the industry to offer assurance by adopting an industry label, disclaimer or certification that the systems are isolated.

In short, if the hotel guest network—or the swimming pool for that matter—is wide open with no protective services and is something you need to use, make sure that you have done everything in your power to protect yourself. Please do not leave common sense at home.

Rick Lawhorn, CISSP, CISA, CHP, CHSS, has more than 19 years of experience in information technology, including extensive security, compliance, and privacy work. He served as the CISO for two Fortune 100 companies and in IT leadership and security roles within multiple law firms and the National White Collar Crime Center. Send comments on this column to feedback@infosecuritymag.com.

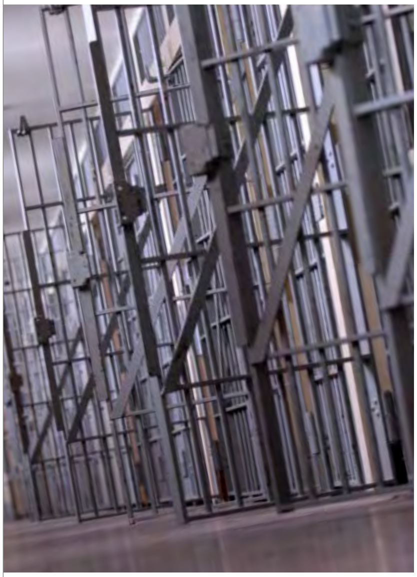
TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
READERS' CHOICE AWARDS
ENCRYPTION
SPONSOR RESOURCES

Analysis | VIRTUALIZATION

Threats to Virtualization Less Theoretical, More Practical

The demonstration of a hacking tool at Black Hat that allows attackers to escape from virtual machines to attack their guest OS elevates the seriousness of security threats to virtualization.

BY MICHAEL S. MIMOSO



JAILBREAKING a virtual machine has always been sort of a black op. But slowly the practice is emerging from the shadows.

The whispers are getting louder of researchers studying malware samples captured in the wild that can leap from a virtual guest machine to the host. So is the work being done on exploits for vulnerabilities that would also allow an attacker to escape a virtual machine.

One of the latest was outlined in late July at Black Hat 2009 USA. Immunity, an assessment and penetration testing company, provided details on a tool called Cloudburst, developed by senior security researcher Kostya Kortchinsky. Cloudburst, available to users of Immunity's CANVAS testing tool, exploits a bug in the display functions of VMware Workstation 6.5.1 and earlier versions, as well as VMware Player, Server, Fusion, ESXi and ESX [see CVE 2009-1244 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1244 for exact version numbers].

Tangible exploits, such as Cloudburst, threaten the sanctity of virtualization projects that are so en vogue today with many companies for their server consolidation and power consumption benefits.

Kortchinsky went a little outside the box with Cloudburst, choosing to exploit the dependencies between virtual machines and devices such as video adapters, floppy controllers, IDE controllers, keyboard controllers and network adapters to gain access to the host. During his Black Hat presentation, he explained how he attacked vulnerabilities in the way VMware emulates a video device; he demonstrated how he exploited host memory leaks into the guest, and arbitrary memory writes from the guest to anywhere in the host.

"The video adapter parses the most complex data," he says. "It has a huge amount of shared memory."

Kortchinsky says the same code emulates devices on every VMware product. "If the vulnerability is there, it's there on every VMware product and can be accessed from the guest through port i/o or memory-mapped i/o." Immunity says Cloudburst's ability to corrupt memory allows it to tunnel a MOSDEF connection over the frame buffer of the guest to communicate with the host. MOSDEF is an exploit tool in the CANVAS arsenal written by Immunity founder Dave Aitel.

VMware has patched these vulnerable versions of its products, doing so on April 10 [http://www.vmware.com/security/advisories/VMSA-2009-0006.html], four days after Cloudburst was released to CANVAS. And that's what makes Cloudburst different; it's not a proof of concept, unlike most VM malware.

So what does it mean for you as a security manager, someone with buying power and decision-making responsibilities? Well, a little bit more than it did say two years ago before the economy tripped over itself and your justifications for spending relied less on the bottom line and more on threats that could impact your IT environment and that you could touch and squeeze.

> "The video adapter parses the most complex data. It has a huge amount of shared memory."
>
> –KOSTYA KORTCHINSKY, Cloudburst

Virtualization threats have always been abstract, more theory than practice. Sure there was the supposed undetectable virtual rootkit, Blue Pill [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1266502,00.html], but that required such innate technical understanding that it hardly seemed feasible for attackers to weaponize something so intricate. Experts, meanwhile, warned that tangible threats to virtual environments were coming, but still you're unlikely to strategize and buy on the theoretical. What you are likely to do is jump headfirst into virtualization because the benefits are too sweet not to take a lick from the mixing bowl. Securing it probably comes later.

Well, it's later.

Attacks are progressing slowly out of the theoretical into the practical. Right now there are five CVE alerts based on VM escapes and certainly more to come as researchers and other attackers build on work done by Kortchinsky, Greg McManus of iDefense [http://www.vmware.com/security/advisories/VMSA-2007-0004.html] and the research teams at Core Security [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004034].

Experts say networks shouldn't rely on traditional security measures because they don't counteract every VM threat. Until now, most organizations have been reactive about securing virtual environments and with the swell of new attacks, exploits and proof-of-concept projects, VM security is front and center.

Two years ago, security expert and current Cisco director of cloud and virtualization solutions Chris Hoff wrote: "It doesn't help that we're trying to build business cases to start thinking about investing in securing virtualized environments when the threats and vulnerabilities are so esoteric and by manner of omission executives are basically told that security is something they do not need to focus on any differently in their virtualization deployments."

With Cloudburst being the most recent attack as the backdrop, experts such as Hoff and many others who have been beating the drum for security in virtual environments are starting to look pretty bleeding edge with their prognostications and pleadings.

So a final word from Hoff, again from two years ago writing about a flaw that enabled at the time an attacker to run arbitrary code on a VMware GuestOS: "This will be the first of many, of that you can be sure. … You can use something like this to start having discussions [with management] in a calm, rational manner…before you have to go reconfigure or patch your global virtualized server farms, that is…"

Later has arrived.▸

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

SNAPSHOT

Zero Day

ADOBE IS JOINING THE ZERO-DAY FRAY—and in a big way. Critical Flash and PDF vulnerabilities have elevated Adobe security issues to Redmond-like levels. And in true Microsoft tradition, Adobe has been slow with fixes and clumsy in its messaging to users.

—*Information Security* staff

WAITING GAME

On July 22, Adobe warns the world of a critical Flash Player flaw, as well as a serious bug in an authplay.dll in Adobe Reader and Acrobat, that could crash the applications or allow a hacker remote control of a system. Adobe also confirmed active exploits against the vulnerabilities. Adobe's Product Security Incident Response Team said it would have a fix by July 30. In the meantime, Adobe suggested users delete authplay.dll as a workaround.

ZERO-DAY? REALLY?

Reports point out that Adobe was first informed about the Adobe authplay.dll issue on Dec. 31 of last year and originally classified as a data loss/corruption problem before it was reclassified as a security bug.

CHINA CONNECTION

Hackers exploited the violence in Urumuqi, China, spiking PDFs with a filename related to the Urumuqi incidents. Once users opened the PDFs, infected with a foul SWF object, two files executed, temp.exe and suchost.exe. Analysts at Viruslist say the exploits were created in early July and were in fact a pair of Trojan horses.

NOT TO BE LEFT OUT

Microsoft shipped a pair of out-of-band patches to fix critical bugs in IE and Visual Basic, including a vulnerability in IE that had previously been patched. But after some digging by hacker Halvar Flake concluded that additional security issues may have been introduced by the patch, Microsoft decided to reissue the patch.

OVER-HEARD

> "DNS has been doing cross-organizational address management for 25 years; it works great. DNS is the world's largest PKI without the 'K.' All DNSSEC does is add keys."
>
> –DAN KAMINSKY, director penetration testing, IOActive

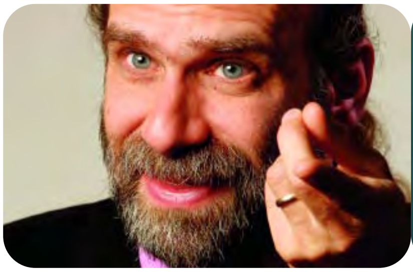


TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
READERS' CHOICE AWARDS
ENCRYPTION
SPONSOR RESOURCES

Is perfect access control possible?

POINT *by* BRUCE SCHNEIER

ACCESS CONTROL IS DIFFICULT in an organizational setting. On one hand, every employee needs enough access to do his job. On the other, every time you give an employee more access, there's more risk: he could abuse that access, lose information he has access to, or be socially engineered into giving that access to a malfeasant. So a smart, risk-conscious organization will give each employee the exact level of access he needs to do his job, and no more.

Over the years, there's been a lot of work put into role-based access control [http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm, http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf] [http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/kuhn-98.pdf, http://technet.microsoft.com/en-us/library/cc780256(WS.10).aspx]. But despite the large number of academic papers and high-profile security products, most organizations don't implement it—at all—with the predictable security problems as a result.

> "In the end, a perfect access control system just isn't possible; organizations are simply too chaotic for it to work.
> —BRUCE SCHNEIER

Regularly we read stories of employees abusing their database access-control privileges for personal reasons: medical records [http://articles.latimes.com/2009/may/09/local/me-hospital9], tax records, passport records, police records. NSA eavesdroppers spy on their wives and girlfriends. Departing employees take corporate secrets when they leave [http://www.thetechherald.com/article.php/200924/3849/Trust-still-an-issue-in-IT-as-insiders-abuse-access-rights].

A spectacular access control failure occurred in the UK in 2007. An employee of Her Majesty's Revenue & Customs had to send a couple of thousand sample records from a database on all children in the country to National Audit Office. But it was easier for him to copy the entire database of 25 million people onto a couple of disks and put it in the mail than it was to select out just the records needed. Unfortunately, the discs got lost in the mail, and the story was a huge embarrassment for the government [http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1318850,00.html].

Eric Johnson at Dartmouth's Tuck School of Business has been studying the problem, and his results won't startle anyone who has thought about it at all. RBAC is very hard to implement [http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/DataFinancial.pdf] correctly. Organizations generally don't even know who has what role. The

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

employee doesn't know, the boss doesn't know—and these days the employee might have more than one boss—and senior management certainly doesn't know. There's a reason RBAC came out of the military; in that world, command structures are simple and well-defined.

Even worse, employees' roles change all the time—Johnson chronicled one business group of 3,000 people that made 1,000 role changes in just three months—and it's often not obvious what information an employee needs until he actually needs it. And information simply isn't that granular. Just as it's much easier to give someone access to an entire file cabinet than to only the particular files he needs, it's much easier to give someone access to an entire database than only the particular records he needs.

This means that organizations either over-entitle or under-entitle employees. But since getting the job done is more important than anything else, organizations tend to over-entitle. Johnson estimates that 50 percent to 90 percent of employees are over-entitled in large organizations. In the uncommon instance where an employee needs access to something he normally doesn't have, there's generally some process for him to get it. And access is almost never revoked once it's been granted. In large formal organizations, Johnson was able to predict how long an employee had worked there based on how much access he had.

Clearly, organizations can do better. Johnson's current work involves building access-control systems with easy self-escalation [http://weis2008.econinfosec.org/papers/Zhao.pdf], audit to make sure that power isn't abused, violation penalties (Intel, for example, issues "speeding tickets" to violators), and compliance rewards. His goal is to find the right set of incentives and controls that manage access without making people too risk-averse [http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/wise_v1.pdf].

In the end, a perfect access control system just isn't possible; organizations are simply too chaotic for it to work. And any good system will allow a certain number of access control violations, if they're made in good faith by people just trying to do their jobs. The "speeding ticket" analogy is better than it looks: we post limits of 55 miles per hour, but generally don't start ticketing people unless they're going over 70. ›

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

COUNTERPOINT *by* MARCUS RANUM

I DON'T LIKE REASONING by analogy, Bruce, because it often obscures as much as it illuminates. While the "speeding ticket" analogy *sounds* sensible, that's only because it leaves out a whole lot of detail, such as what happens when someone is violating the speed limit and causes another person injury. If you're going 55 in a 30 miles-per-hour zone and cause an accident with injury, "screwed" doesn't begin to describe the situation. I could extend your analogy to access control, but we'd be increasingly moving away from the real topic at hand while arguing about cars; it's pointless.

Here's the problem: if you are supposed to be guarding some data, and don't, and it causes someone injury, "screwed" should be the starting point for describing your situation. I know that talking about morality and computer security is pretty retro, but someone has to point out that data leaks can represent huge headaches or worse for the victims—and by "victim," I don't necessarily mean the holder of the data.

Many organizations are stuck in between letting everyone who wants it download a copy of customer databases to their laptop (which they then lose) or re-designing all their databases to add controls which may or may not help. It's very difficult to get management to invest in re-implementing systems against the threat of something that hasn't happened before. But, it's unacceptable, both technically and morally, to give an expansive shrug and say "It's impossible to get access control right" (with the implication that leaks are just going to happen) when two things are obvious:

- We're dealing with the tip of an iceberg
- Current approaches are what got us to where we are now

As you say, over-entitlement is the norm, and usually makes sense, but that's simply because we are only, just now, beginning to pay the costs for mistakes made years ago. Perhaps 10 years ago it seemed like a big cost-saving to move critical databases to departmental servers, and to make it easy and allegedly more cost effective to grant full database access to those who asserted (sufficiently loudly) they needed it. Now, we are finding that those cost savings may not have been estimated correctly—too bad and too late.

> "I don't think any of the models we're working with are particularly good, and simply wishing we had better ones doesn't mean that better ones exist.
> —MARCUS RANUM

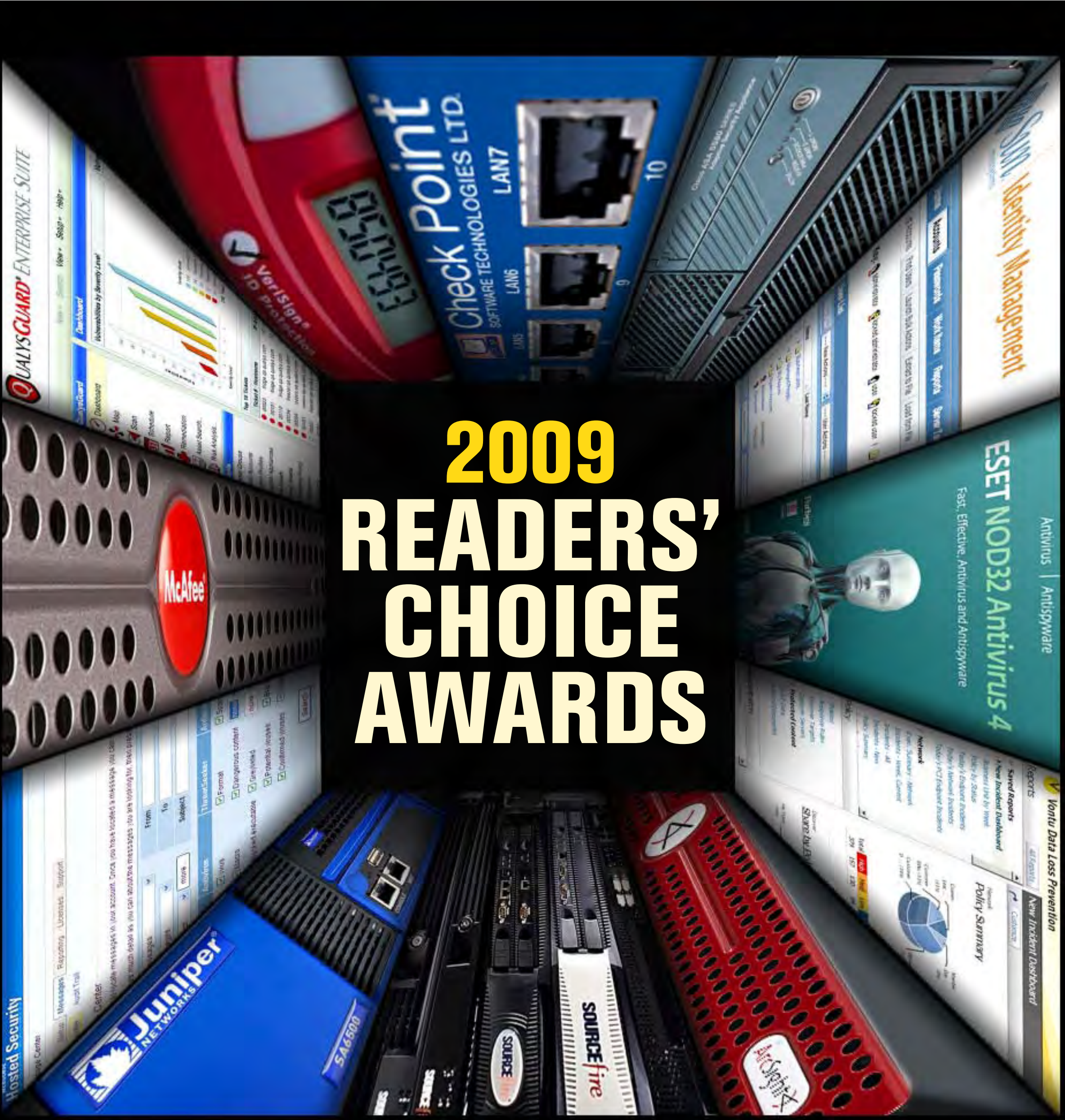
The current trend in data management seems to be to outsource it to places where it can be managed more cheaply—meaning, by definition, that it's being positioned where it's relatively more valuable. Then, they're actually surprised to discover that someone in the call center sold the customer database. I'd be perfectly comfortable testifying that whoever made that decision, which was tantamount to exposing the data, was both incompetent and negligent.

The great, big, lurking disaster that nobody wants to talk about is national security data. You and I both know how much pressure there has been to shift from "need to know" to "need to share"—i.e., increase access rather than limit it. And, again, people hear about Joint Strike Fighter technical plans leaking, and react with shock and awe. To incompetent and negligent, we can add dangerous and threatening to national security.

I don't think any of the models we're working with are particularly good, and simply wishing we had better ones doesn't mean that better ones exist. Consider digital rights management (DRM)—ultimately, that was about controlling access to data, as well. Companies wanted to control who ("only people who paid") could access media, but still have it be exposed and available.

Whenever I think of access control as a technology problem, instead of a personnel issue, I think about DRM and how badly it has worked; other than straightforward approaches such as controlling who gets to databases, access control systems would have to succeed where DRM has failed. The question we are really asking is "Can we have our data widely exposed, but still safe?" That sounds, to me, a lot like "Can I have my cake, and eat it too?" The only answer that works in the real world is "Pick one." ▸

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.



2009 READERS' CHOICE AWARDS

YOUR CALL ON THE INDUSTRY'S BEST

For the fourth consecutive year, INFORMATION SECURITY readers voted to determine the best security products. A record 1,721 voters participated this year, rating products in 17 different categories. Click through to which products took top honors:

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

ANTIMALWARE

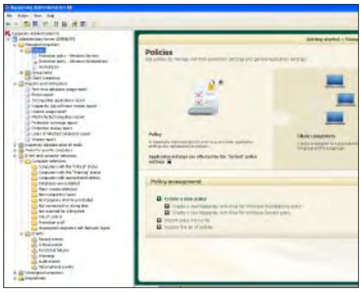
Business-grade desktop and server antivirus and antispyware protection, using signature-, behavior- and anomaly-based detection, whitelisting. Includes suites bundled with host-based intrusion prevention and client firewalls.

GOLD

Kaspersky Open Space Security

Kaspersky Labs

http://usa.kaspersky.com/



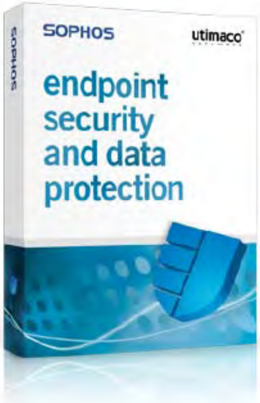
Kaspersky Labs' Kaspersky Open Space Security is the company's suite of antimalware protection for the gateway and endpoint. It includes: Work Space, which keeps workstations secure; Business Space, which adds file server protection; Enterprise Space, which adds mail server security; and Total Space, which adds gateway protection to the previous offerings. It received high marks for detecting, blocking and cleaning malware, and in the speed and frequency of signature updates.

SILVER

Sophos Endpoint Security and Data Protection

Sophos

http://www.sophos.com/



Sophos' Endpoint Security and Data Protection wraps antivirus, firewall, network access control and encryption into a neat package that voters liked for its quick signature updates, and reporting and alerting capabilities. You can also centrally manage the security status of your endpoints from one console; the product supports Windows, Unix and Linux.

BRONZE

ESET NOD32 Antivirus

ESET

http://www.eset.com/

ESET NOD32 Antivirus offers not only antivirus and antispyware protection, but a personal firewall and antispam capabilities. Voters were keen on the product's ease of installation, configuration and administration. NOD32 requires 44MB of memory, less than other similar products. Voters also said they were able to get a significant ROI from this product.

trends

"Generally speaking, antimalware is antimalware; what you get from one vendor is not much different than what you get from another. Where the market is changing is that there are lots of components required to have a comprehensive strategy. Antimalware alone is not going to cut it. It's hard to buy antimalware alone; vendors are almost forcing you to buy a client suite."

Natalie Lambert,
analyst,
Forrester Research

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

APPLICATION SECURITY

Web application firewalls (standalone and part of application acceleration/delivery systems), static and dynamic Web application vulnerability scanning and source code analysis products and services.

GOLD

Barracuda Web Application Firewall

Barracuda Networks

http://www.barracudanetworks.com

If application developers don't employ secure coding practices, a Web application firewall can help pick up some of the slack, protecting against unseen flaws that attackers can exploit with SQL injection attacks, cross-site scripting or worse. In fact, that's why readers gave the Barracuda Web Application Firewall top honors this year, citing the device's particular effectiveness in detecting and reporting known attacks and vulnerabilities. Ease of installation also scored high with readers.

SILVER

BIG-IP Application Security Manager

F5 Networks

http://www.f5.com/

The BIG-IP Application Security Manager (ASM) uses automated, adaptive policies based on the traffic patterns that it observes. The straightforward policy implementation, according to F5 Networks, allows companies to reduce overall operational costs. The readers seem to have agreed. Those surveyed gave it high marks for its return on investment and integration with other security tools.

BRONZE

Citrix Systems NetScaler Application Firewall

Citrix Systems

http://www.citrix.com

Readers had a strong appreciation for the NetScaler Application Firewall's vendor service and support, as well as its ability to stop attacks and flaws. The Citrix Systems firewall blocks application-layer attacks based on behaviors—not signatures—that deviate from its security model. NetScaler's learning engine also generates policy recommendations using similar analysis.

trends

"[The consolidation (IBM/Watchfire, HP/SPIDynamics)] we've seen so far is largely on the testing side. There will be a natural shift from the testing gear to more proactive automated prevention products like WAFs, technical frameworks and development tools, which stop vulnerabilities at an earlier phase."

Diana Kelley,
cofounder,
Security Curve

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

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

VeriSign Identity Protection Authentication Service

VeriSign
http://www.verisign.com

VeriSign takes top honors for its standards-based, partially hosted multifactor authentication product. Respondents lauded its secure credentials and scalability. Recently VeriSign has made strides on mobile authentication, supporting 200-plus devices, and added self-service features, such as password retrieval. "Customers value the idea of self-service capabilities and heterogeneous mobile device support," said Burton Group Senior Analyst Mark Diodati.

SILVER

RSA SecurID

RSA, The Security Division of EMC
http://www.rsa.com

The venerable SecurID line scored highly across the board, with the exception of vendor service and support. Today the product family includes software- and hardware-based authenticators (tokens), request-management agents and various servers. RSA claims it's the only vendor that automatically changes user passwords every 60 seconds, and publicizes its use of AES encryption.

BRONZE

Entrust IdentityGuard

Entrust
http://www.entrust.com

When engaging competitors, Entrust touts IdentityGuard's affordability, but respondents' ranked it highest for integration and compatibility; it lagged in vendor service and support. The enterprise product line features a range of strong authentication options (physical, non-physical and mobile) authenticators (e-grids, digital certificates and tokens), native 802.1X wireless support and compatibility with BlackBerrys and iPhones.

trends

Even in 2009, it's rare for any multifactor authentication product to meet all of an organization's needs. Diodati says three vexing issues—varied user constituencies; emerging Web applications; and mobile platform support—are forcing companies to mix and match technologies. Success demands clearly defined business problems. "If an organization doesn't have the intestinal fortitude to do that, it'll have to wait."

Mark Diodati,
senior analyst,
Burton Group

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

DATA LOSS PREVENTION (DLP)

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

GOLD

Websense Data Security Suite

Websense

http://www.websense.com/

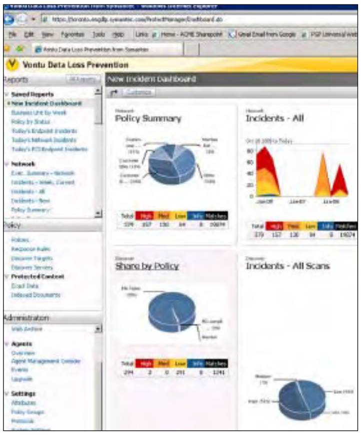
Receiving top scores in all categories, the Websense Data Security Suite was lauded by readers for its ease of installation, configuration and administration, its scalability, and its comprehensive and flexible reporting. Perhaps most notable were its top scores for vendor service and support, as well as ROI.

SILVER

Symantec Data Loss Prevention (Vontu)

Symantec

http://www.symantec.com



Symantec's Data Loss Prevention product, incorporated from its Vontu acquisition, ranked highly for its granular and flexible policy definition and management, and its effectiveness in detecting and/or preventing unauthorized user activity. While vendor support fell shy of Websense's, its marks for ease of integration, comprehensive reporting and scalability made it a top choice.

BRONZE

McAfee Total Protection for Data

McAfee

http://www.mcafee.com

McAfee's Total Protection for Data scored highest for its ease of installation, configuration and administration. A solid overall product, it was also noted for its granular and flexible policy definition, its effectiveness in detecting and/or preventing unauthorized user activity, its ease of integration and its scalability.

trends

> *"The data loss prevention market is finally making the transition from early adopters to the early mainstream. Most of the major security vendors have completed their acquisitions of smaller DLP vendors and are rounding out the products into full suites that protect data on the network, in storage and on endpoints."*

Rich Mogull,
founder,
Securosis, LLC

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

EMAIL SECURITY

Antispam, antiphishing, email antivirus and antimalware filtering, software and appliance products, as well as hosted "in-the-cloud" email security services. Includes email archiving and e-discovery products and services.

GOLD

Sophos Email Security and Data Protection

Sophos

www.sophos.com

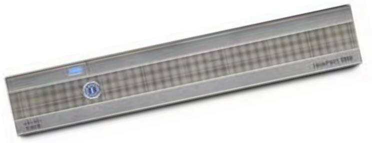
Sophos Email Security earned top grades across the board, with users giving it high marks where it counted most, detecting and blocking spam, phishing, viruses and spyware. Available as software or an appliance, the product is now bundled with email encryption. Readers also praised its ease of use and integration with messaging applications.

SILVER

IronPort appliances

Cisco Systems

www.ironport.com



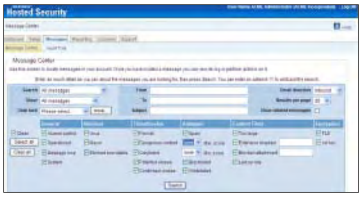
Cisco's line of IronPort appliances was a strong contender. Long a leader in enterprise email security, IronPort particularly impressed readers with its integration capabilities. The C-series and high-end X-series appliances also performed exceptionally in antispam and threat detection, and was well regarded in every evaluation criteria.

BRONZE

Websense Email Security

Websense

www.websense.com



Finishing third in this competitive category is no mean feat, as Websense Email Security earned high marks across the board, with no discernable weak points in readers' judgments. As with the other two email security winners, Websense's product impressed with its ability to block spam and phishing attacks and detect email-borne viruses and spyware.

trends

> *"Both enterprises and SMBs are turning to hosted email security services. Thus far, SMBs more than enterprises, but there is definitely a growing interest in enterprises to outsource email security. In terms of products, still antispam is of the greatest demand. For enterprises, we see more demand for deep content filtering and DLP functionality."*

Chenxi Wang,
principal analyst,
Forrester research

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.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

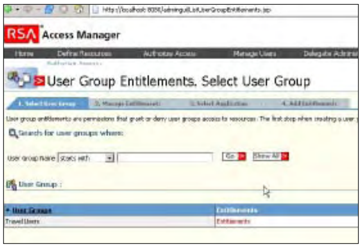
SPONSOR RESOURCES

GOLD

RSA Access Manager

RSA

www.rsa.com



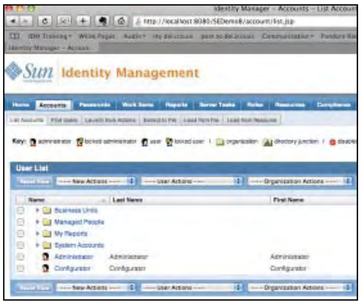
RSA Access Manager, formerly known as ClearTrust tackles the enormously complex challenge of Web access management, with single sign-on and other key access management features for complex internal, external and extranet environments. Users were particularly impressed with its integration with associated products and directories, its scalability across the extended enterprise and ease of use.

SILVER

Sun Microsystems Identity Manager

Sun Microsystems

www.sun.com



Sun's Identity Manager, as well as companion products Identity Compliance Manager and Role Manager, was second by the narrowest of margins. Its role-based user provisioning and other capabilities make it a powerful tool for identity management and auditing across the enterprise and extranet. It earned its highest reader marks in extensibility and end user transparency.

BRONZE

Citrix Password Manager

Citrix Systems

www.citrix.com

Citrix Password Manager, now bundled as a feature of its application virtualization product, helps organizations tackle the persistent headache of dealing with hundreds and thousands of user passwords, including self-service to ease help desk burdens. Readers gave it solid grades in all categories, including end user transparency, scalability, and ease of installation, configuration and administration.

trends

> *"Suites aren't as integrated as many clients believe. There is considerable effort on the part of suite vendors to provide better integration. Most suites (an exception is Novell) were acquired product by product over time, so many of them have completely different underlying architectures. Enterprises tend to be responsive to the suite idea because of the relationship it creates with the vendor."*

Earl Perkins, research vice president, Gartner

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

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

Juniper Networks IDP

Juniper Networks

www.juniper.net

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances won top honors from readers with high marks for effectively and accurately detecting, preventing and/or blocking attacks and suspicious activity. The appliances also received raves for their frequency of signature updates and reporting and alerting capabilities. Juniper Networks IDP uses signatures and other detection mechanisms.

SILVER

3Com/TippingPoint Intrusion Prevention Systems

3Com

www.3com.com

3Com/TippingPoint Intrusion Prevention Systems snagged the silver, drawing strong ratings in a number of areas, including frequency of signature updates, response to new threats and for effectively and accurately detecting, preventing and/or blocking attacks. The 3Com/TippingPoint IPS, an inline device, and is built on the TippingPoint ASIC-based Threat Suppression Engine to provide protection at gigabit speeds.

BRONZE

Sourcefire IPS

Sourcefire

www.sourcefire.com

Sourcefire IPS, which is built on the open source Snort engine, earned the bronze with high scores from readers for its ability to effectively and accurately detect, prevent and/or block attacks. The product also scored well for frequency of signature updates and response to new threats. Sourcefire IPS combines vulnerability-based and anomaly-based inspection methods to analyze traffic.

trends

"It's a good time to be an IDS/IPS provider because network equipment manufacturers are scrambling to partner with threat management vendors as they work to incorporate embedded network security features and intelligence into the network infrastructure for better visibility and enforcement for enterprises. Expect to see more partnerships like the one between HP and McAfee."

Charlotte Dunlap,
senior analyst,
Synergy Research

MOBILE DATA SECURITY

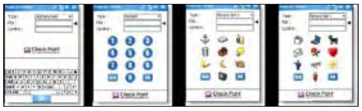
Hardware- and software-based file and full disk laptop encryption, removable storage device (CD/DVDs, USB drives, digital music players) control, and smart phone and other handheld device data protection.

GOLD

PointSec Mobile, Media Encryption, Full Disk Encryption

Check Point Software Technologies

www.checkpoint.com



Check Point's mobile data security products came out on top in a strong field in this critical category, as organizations are moving swiftly to secure data on their endpoints and mobile devices. Readers were particularly impressed by the Check Point's granular and flexible policy controls, and central management tools, including its handling of those troublesome encryption keys.

SILVER

Symantec Mobile Security Suite for Windows Mobile

Symantec

www.symantec.com

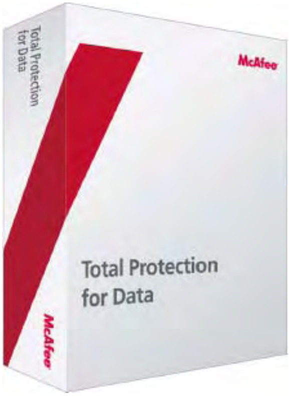
Symantec mobile device security products, including the Windows suite and Mobile Security for Symbian, tackle the growing challenge of security in an environment in which smart phones and PDAs are holding and exposing more and more corporate data. Readers were most impressed with Symantec's policy controls, and also liked its central management and data protection capabilities.

BRONZE

McAfee Endpoint Encryption

McAfee

www.mcafee.com



Reader response to McAfee Endpoint Encryption, as well as Total Protection for Data, which incorporates additional capabilities, such as endpoint DLP, device and application control, shows that McAfee's acquisition and product development choices are resonating well among users. They liked the granular and flexible policies controls and were very pleased with their return on investment.

trends

> *"Disk encryption for laptops is taking hold, and making inroads into the smartphone market. Every large security vendor either offers a disk encryption product (usually full-disk) that they own themselves, or offer via OEM relationship. Deployments are being fueled by disclosure laws like MA-201, and the American Recovery and Reinvestment Act (ARRA), which focuses on health care."*

Andrew Jaquith,
senior analyst,
Forrester Research

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
READERS' CHOICE AWARDS
ENCRYPTION
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.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
READERS' CHOICE AWARDS
ENCRYPTION
SPONSOR RESOURCES

GOLD

Juniper Unified Access Control

Juniper Networks

http://www.juniper.net

Juniper UAC mixes user identity, device security state, and network location information to create unique access control policy, per user and per session. UAC scored high in virtually every category, but was exceptionally strong in its policy-based network access control and its enforcement options. Last year, UAC finished second among readers.

SILVER

Cisco NAC Appliance

Cisco Systems

www.cisco.com

The Cisco NAC Appliance is designed to be the first point of contact for users entering a corporate network, and enables administrators to authenticate and authorize users and enforce organizational security policies before network access is granted. Readers praised its integration with existing infrastructure and its vendor service and support.

BRONZE

Symantec Network Access Control

Symantec

www.symantec.com

Symantec NAC controls access to corporate networks, enforces endpoint security policy and easily integrates with existing network infrastructures. Regardless of how endpoints connect to the network, Symantec evaluates endpoint compliance status, provisions the appropriate network access and provides automated remediation capabilities. Readers ranked Symantec high in scalability as well as praising the ease with which one can install, configure and administer the product.

trends

"NAC hasn't struggled anymore than any other overhyped technology at the beginning of its buying curve. Right now, we're in the over-committing phase of the technology. In the last year, vendors have been coming together and come up with a plan for interoperability, and Microsoft is leading that. We've seen Microsoft's investment in NAC with Vista."

Joel Snyder,
senior partner,
Opus1

Information Security '09 READERS' CHOICE AWARDS

NETWORK FIREWALLS

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

GOLD

Cisco ASA 5500 Series Firewall Edition

Cisco Systems

www.cisco.com

While this was a very tight race, Cisco, the leader in networking infrastructure, took top honors from readers in this category. Building on its existing technology expertise, readers were especially pleased with ASA 5500's ability to effectively block intrusions, attacks and unauthorized traffic and its vendor service and support.

SILVER

FireWall-1

Check Point Software Technologies

www.checkpoint.com

As pioneers in the commercial firewall market, Check Point came in a close second with its FireWall-1 product. Readers were particularly pleased with the product's centralized management and its logging, monitoring and reporting capabilities. Their users also felt the product adequately protected their organizations as seen with the high scores in the ability to block intrusions.

BRONZE

McAfee Enterprise Firewall

McAfee

www.mcafee.com

McAfee, another leader in the security market fared very well with its Enterprise Firewall, formerly Secure Computing's Sidewinder firewall. In particular it scored high marks for its centralized management capabilities and its ability to block threat. Users were also generally pleased with its ease of installation, vendor support and ROI.

trends

"There is some innovation with firewall-plus solutions that bring together firewalling with some IDP functions. The network firewall market continues to move toward multifunction/purpose-specific firewall usage such as Web application firewalls, database firewalls and the virtual machine-aware firewalls."

Diana Kelley, partner, SecurityCurve

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

POLICY AND RISK MANAGEMENT

Risk assessment and modeling, and policy creation, monitoring and reporting products and services. IT governance, risk and compliance products. Configuration management.

GOLD

Symantec Control Compliance Suite

Symantec
www.symantec.com

Symantec Control Compliance Suite garnered the gold, winning high marks from readers for its ease of installation, configuration and administration. The product also drew raves for vendor service and support. Symantec Control Compliance Suite is a group of integrated products that combines point-in-time controls assessment and real-time monitoring of risks and threats to reduce compliance costs.

SILVER

Tripwire Enterprise

Tripwire
www.tripwire.com

Readers rated Tripwire Enterprise highly for its granular and flexible policy management definition capabilities. The product also scored well in several other areas, including its ability to effectively identify policy violations and its reporting and alerting capabilities. Tripwire Enterprise combines configuration assessment and change auditing in a single infrastructure management system.

BRONZE

ArcSight Network Configuration Manager (NCM)

ArcSight
www.arcsight.com

ArcSight Network Configuration Manager (NCM) earned the bronze, winning praise from readers for its granular and flexible policy management definition capabilities. Readers also liked the product for its ease of installation and administration and its return on investment. ArcSight NCM is an appliance to centrally manage network configurations, monitor compliance, and reduce workload through task automation.

trends

> *"In general, policy and risk management are still two separate areas and both are showing quite a bit of promise. Policy management is further along in maturity. More maturity in risk management practices will ultimately be necessary to help move security [professionals] up the chain of command and give them more exposure and higher priority in the business."*

Chris McClean,
analyst,
Forrester Research

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
READERS' CHOICE AWARDS
ENCRYPTION
SPONSOR RESOURCES

REMOTE ACCESS

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

GOLD

Cisco Systems VPN Concentrator Series

Cisco Systems

www.cisco.com

Readers rated authentication support, integration and compatibility with existing platforms/applications and vendor service and support highest in the category. This product delivers application access, endpoint security, data integrity protection, infrastructure access, and network compliance validation controls. It is available in nonredundant and redundant configurations, allowing customers to customize their builds.

SILVER

SA Series SSL VPN Appliances

Juniper Networks

http://www.juniper.net

Readers like Juniper's authentication support, end-user transparency/ease of use and vendor service/support. The product family includes models sized for the needs of small businesses with limited IT experience to high-capacity products for large enterprises requiring the utmost authentication, authorization, and auditing (AAA) capabilities for employee, partner (extranet) and customer access.

BRONZE

Citrix Access Gateway

Citrix Systems

http://www.citrix.com

Readers valued the extensibility, authentication support, and end-user transparency/ease of use of Citrix Access Gateway. The product is a secure application access solution that provides administrators granular application-level control while empowering users with remote access from anywhere. SmartAccess technology allows administrators to manage access control and set policies of acceptable actions based on user identity and the endpoint device.

trends

"Five years ago, remote access began to shift towards Web-based "clientless" VPNs. Today, that evolution has come full-circle, with contemporary platforms offering a range of customizable secure access methods, from "anywhere" Web access to rich install-on-demand SSL VPN clients. New innovations focus more extensively on the data center and reducing TCO through streamlined, unified management tools and cloud-based software-as-a-service delivery models."

Lisa Phifer,
president,
Core Competence

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

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

ArcSight ESM

ArcSight

www.arcsight.com

ArcSight earned the gold with its ArcSight ESM/ArcSight Logger. Readers were most notably pleased with the product's ability to perform robust event correlation when compared to other SIM product. ArcSight got top marks for the effectiveness of its dashboard and did particularly well on data archiving and for its policy engine.

SILVER

Symantec Security Information Manager

Symantec

www.symantec.com

Symantec scored well for its data archiving and integration and compatibility with existing systems, devices and applications. Users were also pleased with the product's dashboard and its ability to visualize security status and implement policy. Readers also like its ability to map information to security policy and regulations.

BRONZE

RSA enVision

RSA, The Security Division of EMC

www.rsa.com

A leader in the authentication market, RSA did well with its SIM offering dubbed RSA enVision. EnVision took third place and users were generally pleased with the product's ability to integrate well with other systems, devices and applications. It also scored relatively well on the data archiving and event correlation.

trends

"SIMs are evolving from intelligent log aggregators to operational business tools where SIMs can help uncover/identify business improvement opportunities. For example SIMs can identify excessive login failures, and with that information, a security team could alter its password policy or have a cost-justification for an SSO solution. SIMs are also integrating with "newer" technologies such as wireless IDS/IPS and virtual machines."

Diana Kelley,
partner,
SecurityCurve

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

UTM

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.

GOLD

Cisco Systems ASA 5500 Series Adaptive Security Appliance

Cisco Systems

www.cisco.com

Networking behemoth Cisco got the nod for gold in the UTM category. Readers were pleased with the breadth of functionality offered on their ASA 5500 devices. Users of the UTM were also very satisfied with the vendor service and support they received as well as the form factor of the device.

SILVER

IBM ISS Proventia Network Multi-Function Security (MFS)

IBM-ISS

http://www.iss.net/

ISS Proventia offers gateway and network protection in combining firewall, IDP, antimalware, URL filtering and application protection in one box. Users rated highly the product's security depth and form factor, as well as the choice of available additional add-ons. Service and support also rated highly with users.

BRONZE

Check Point Software Technologies UTM-1, Safe@Office

Check Point Software Technologies

www.checkpoint.com

Check Point users were pleased with the breadth of security functionality for their UTM offerings. They scored the higher than Cisco and IBM in the category of ease of installation, configuration and the administration of the UTM devices. Users felt they are getting their money's worth, an important consideration in today's difficult economy.

trends

"Selecting a UTM solution is like a box of chocolates… you never know what you are going to get. Baseline UTM functionality includes firewall, AV, IPS/IDS and VPNs. New UTM functionality is turning to capabilities to help [users] address many "channels" including email, web, instant messaging, peer-to-peer file sharing and voice over IP, for the potential loss or exposure of sensitive data."

Derek E. Brink, vice president and research fellow, IT security, Aberdeen Group

Information Security '09 READERS' CHOICE AWARDS

VULNERABILITY MANAGEMENT

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

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

GOLD

QualysGuard Vulnerability Management

Qualys

http://www.qualys.com/

For the third year in a row, Qualys has come out on top in the vulnerability management category. QualysGuard Vulnerability Management is the company's automated vulnerability management and network auditing product. Readers were most pleased with its ease of installation, the accuracy in which it identifies vulnerabilities, as well as the breadth of applications and devices covered.

SILVER

Nessus

Tenable Network Security

http://www.tenablesecurity.com

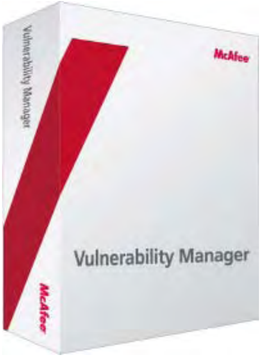
Nessus, offered by Tenable Network Security in conjunction with the company's Security Center and Passive Scanner products, placed second this year. Readers were especially enthusiastic about the product's accuracy, as well as its ability to integrate with threat management or early warning systems. Other notable features include configuration auditing, asset profiling, and high-speed discovery.

BRONZE

McAfee Vulnerability Manager

McAfee

http://www.mcafee.com



McAfee Vulnerability Manager offers a priority-based approach to vulnerability management. Other features include broad content checks, threat correlation and asset-based discovery, management, scanning and reporting. Readers highlighted the product's comprehensive and flexible reporting system as one of the best features.

trends

"The sweet spot of the market now is ASV scanning for PCI compliance. Some of the big players have been acquiring application security scanning vendors, so you'll see [the scanning tools] tied much more tightly into other parts of the software development lifecycle. More of the traditional scanning tools are incorporating web application scan, and that's again being driven by PCI."

John Kindervag,
senior analyst,
Forrester Research

Information Security
'09
READERS' CHOICE AWARDS

WEB SECURITY GATEWAYS

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

McAfee Web Gateway

McAfee

http://www.mcafee.com/

McAfee Web Gateway is designed to protect against Web-borne threats by eliminating unwanted Web access, and detecting and blocking malicious programs with an easy-to-use browser-based management system. Garnering the gold, the product earned high marks for its threat detection capabilities, which uses McAfee's antispam technology and scan engine to block spyware and clean viruses. Also favorable among readers is the product's comprehensive reporting system and vendor support features.

SILVER

Trend Micro InterScan Web Security Appliance

Trend Micro

http://us.trendmicro.com

Trend Micro's InterScan Web Security Appliance boosts Internet gateway defense with a combination of antivirus, antispyware and cloud-based Web reputation features. This advanced edition analyzes ActiveX and Java applets and filters URLs to mitigate threats. Easy installation, configuration and administration of the product, as well as its detection capabilities of both know and unknown threats earned the product a silver medal among consumers.

BRONZE

Websense Web Security

Websense

http://www.websense.com

Websense Web Security, provides extensive, multilayered protection from Web-based threats with a combination of Websense Web Protection Services and ThreatSeeker Network to guard websites and servers and continually scan the Internet for emerging threats. The product has comprehensive reporting capabilities, detailed policy creation and enforcement features and impressive threat detection capabilities, according to consumers, who touted it as a bronze medal winner.

trends

"The trend is definitely toward multifunction one-box appliances as everyone is looking to save power and space, as well as reducing the need for administrators experienced with a range of different vendors' products. There are now so many threat vectors and Internet-based communication channels that being able to manage policy settings and generate reports from one device makes life simpler for security teams. The clients I talk to are interested in data leak prevention functionality as sensitive data-in-motion has become a big concern with the growth of social networking sites. Real-time reporting of potential policy abuse is being used to deliver direct warnings to culprits so users are aware that policies are being enforced."

Mike Cobb,
managing director,
Cobweb Applications

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
READERS' CHOICE AWARDS
ENCRYPTION
SPONSOR RESOURCES

WIRELESS SECURITY

Wireless firewalls and UTM devices, wireless access control products, WLAN intrusion and detection systems, and security-enabled wireless infrastructure products.

GOLD

Cisco Wireless Security Suite

Cisco Systems

www.cisco.com

Cisco's Wireless Security Suite won a tight completion for its capabilities, which include intrusion detection, an integrated authentication framework and scalable centralized security management. WPA and WPA2 security is supported for authentication and data encryption. The suite was well regarded in all criteria, but readers gave their highest marks for its access control and scalability.

SILVER

SonicWALL Distributed Wireless Solution

SonicWALL

www.sonicwall.com

SonicWALL's Distributed Wireless Solution, embodied in its SonicPoint Secure Wireless Series and TZ Wireless-N UTM appliances, narrowly missed the gold. Reflecting a SonicWALL strength, readers gave outstanding marks to the products for their ease of installation, configuration and administration, and also valued their integration with wired security systems and vendor service and support.

BRONZE

Check Point UTM-1 Edge W

Check Point Software Technologies

www.checkpoint.com

UTM-1 Edge W appliances integrate a WiFi access-point (802.11b/g) supporting multiple security protocols, including 802.1x, IPSec over WLAN, RADIUS, WEP, WPA and WPA2 authentication to provide unified threat management protection for remote and branch offices. Readers gave it solid ratings across the board, with access control and integration with wired security systems earning its best marks.

trends

> *"It's been increasingly difficult for wireless LAN vendors to differentiate based on security, because if you achieve standards-based security, what more do you need? That might be a little shortsighted, because there are a lot of other security concerns when you start to field converged networks and start to look at dual-mode devices entering the network."*

Michael King,
principal analyst,
Gartner

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

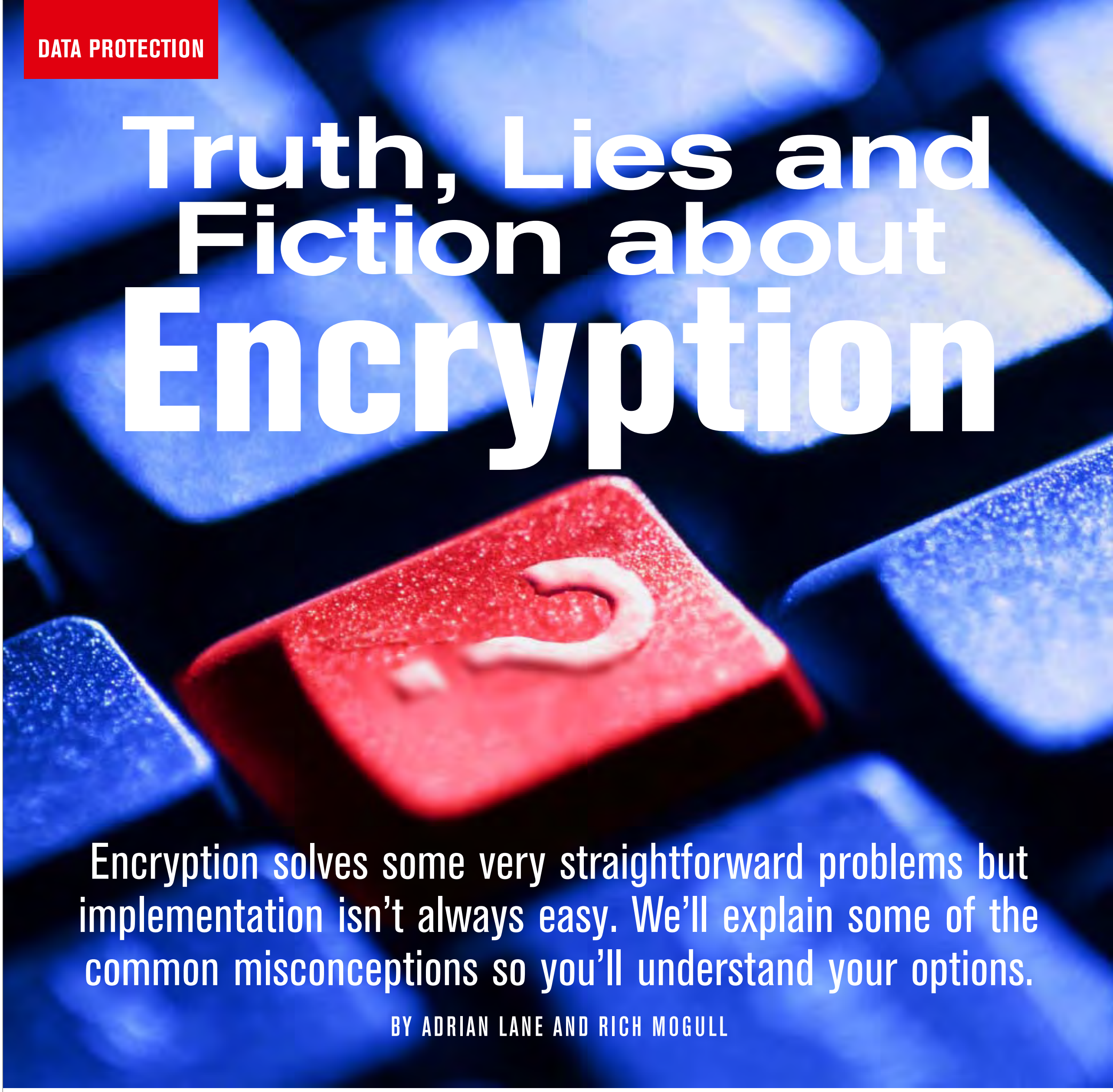
SPONSOR RESOURCES

Selecting the 2009 Readers' Choice Awards

Information Security magazine and SearchSecurity.com presented more than 1,700 readers with some 380 security products and services, divided into 17 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.›



Truth, Lies and Fiction about Encryption

Encryption solves some very straightforward problems but implementation isn't always easy. We'll explain some of the common misconceptions so you'll understand your options.

BY ADRIAN LANE AND RICH MOGULL

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

IT'S A SECURITY PRACTITIONER'S DREAM to deploy a technology that ensures perfect data protection 100 percent of the time. Short of unplugging a computer and locking it in a vault, few technologies come as close as encryption to nearly unbreakable data security; take the data, run it through an encryption algorithm, and it's unreadable to anyone who doesn't possess the right key to reverse the process. It can be mathematically demonstrated that retrieval of encrypted data without the encryption keys is computationally impossible within the expected lifetime of the universe.

And while many strive for this level of certainty, practical issues in the use and deployment of encryption often limit benefits and negatively impact business operations. Reality has a very rude habit of shattering our security dreams.

Encryption is everywhere in IT, from network communications and stored data, all the way down to smartphones and thumb drives. When applied correctly, it's incredibly effective at preserving data privacy and integrity. When misapplied, either because it was poorly deployed or is expected to solve a problem it cannot, an organization does not get added security, but instead spends unnecessary money and slows down operations.

In reality, encryption solves only three problems: first, protecting data that moves physically or virtually; second, protecting data-at-rest; and finally, restricting access when access controls aren't sufficient. It seems simple, but misapplication or misimplementation of encryption occurs time and time again.

Why? Because there are assumptions, myths and even urban legends surrounding encryption. We'll debunk conventional wisdom and explain what is true, what is almost true and what is completely false.

Claim No. 1: "We need encryption because access controls aren't good enough."

This statement is fiction. Access controls are very effective at separating those who should and should not have access to data. Set up properly, with users assigned only to specific accounts dedicated to an explicit job function, they can even provide separation of duties. It is only when the access control system is subverted or policies are misapplied that it fails. What separates this statement from being an outright lie is in the case where encryption is used to enforce access rights as data moves outside a domain of control, or when available access controls aren't granular enough.

Authorization policies may not be the same, controls may not be fully enforced, and without encryption the data is vulnerable.

One such example is sharing data between partner sites, where you do not control the destination systems. Authorization policies may not be the same, controls may not be fully enforced, and without encryption the data is vulnerable. Several IT executives we have spoken with use encryption in this way to limit who sees shared data. Separating keys from the encrypted data files, and providing keys only to a select subset of partners who need access, maintains some control over who can use the data (assuming your partner doesn't share the keys). Another example is the use of transparent database encryption (TDE), where the database contents are encrypted prior to being written to the file system. In this model, the database administrators and users have access to encryption keys, but the IT administrators do not. The IT staff cannot view or alter the contents of the database by reading/writing data files, providing separation of duties between privileged administrative roles.

If traditional access control options exist, use them first! They are easier to use, easier to deploy, faster and more efficient. Using encryption to augment access controls and provide separation of duties should be considered only when you have exhausted other available options.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

Claim No. 2: "Encryption thwarts Internet hackers and data breaches."

Security vendors state this in their press releases, regulatory bodies endorse it, and company spokespeople attempt to instill confidence in their customers with this message. In reality, it's little more than a lie.

Attackers will leverage every available system and resource they can to access data, including the very users and systems responsible for safeguarding the information: breaking into user accounts, rummaging through trash and stealing computers, just to name a few. The attacks come in every type imaginable, and nothing is off limits. Systems and networks are so complex, with so many entry points, that the bad guys don't need to bother attacking encryption. They can take advantage of all the other ways to get to our data. Let's review a couple of the common attacks:

1. User account compromise: If an application user account or automated service is compromised by guessing a password or leveraging another account, then the attacker has access to all of the features and functions that the legitimate user did. If that includes encryption keys or data stored under some form of 'transparent' encryption, the system will decrypt data for them.

> Systems and networks are so complex, with so many entry points, that the bad guys don't need to bother attacking encryption. They can take advantage of all the other ways to get to our data.

2. SQL injection: Subversion of application or database logic through a SQL injection attack gives the attacker access to everything the application sees, sometimes including administrative functions. It may stop data theft if the encryption keys are protected outside of the database, but the attacker may be able to leverage the database to gain access to the keys.

3. Circumvention: With the Heartland Payment Systems breach, communications were encrypted, but data was decrypted at the merchant and payment processor sites along the way. Compromise of a system that accessed data in the clear circumvented encryption entirely.

4. Poor implementation: It has been demonstrated that AES, when used to encrypt browser cookies, can be broken due to poor implementations — not by breaking the algorithm, but rather by taking advantage of the way Web servers use encryption. WEP is another classic encryption implementation failure.

5. Trojan horses: Insertion of malicious code, such as keystroke loggers, can collect user credentials and, through the inspection of user activity, locate valuable data. In this type of attack, the encryption is bypassed through the use of legitimate credentials.

All of these attacks are against systems and legitimate user accounts. Most information systems are designed to make data access, even encrypted data access, as easy as

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

possible. Hijacking user accounts or programs provide hackers the same ease of use. All of these attacks can be mitigated through good key management practices, separation of duties, or alternative security controls, but they cannot be eliminated entirely.

Claim No. 3: "Full-drive encryption for laptops is easy and should be mandatory."

The single greatest cause of reported data breaches in the last decade was due to lost media, specifically through lost backup tapes and lost or stolen laptops. As encryption is ideally suited to protect data at rest, this statement is absolutely true.

We talked to numerous senior IT managers at several Fortune 500 companies and these organizations have embraced encryption of the endpoint. Almost universally, they have implemented disk encryption for laptops. Still not everyone is satisfied. A large segment of security and IT staff are hesitant to encrypt laptops due to failures by encryption vendors to adequately support common IT tasks. The perception still exists that key management is difficult use, it does not work well with backup software, and resetting forgotten user passwords is completely broken. Despite being an effective solution, the feeling is it creates other headaches that make it unmanageable.

While the claim was true in years past, endpoint encryption vendors have addressed these issues through multiple integration and administrative improvements, including:

1. Key management can be centrally administered and made invisible to IT operations.
2. The systems support password recovery, including remote recovery and one-time unlock codes.
3. Backups are performed by credentialed user accounts, working seamlessly with backup routines by gathering an unencrypted copy of the data.
4. System management can be performed in a number of ways, including key management hierarchies and integration with access control systems, providing a gateway for configuration and patch management.

The goal of media encryption is to safeguard data in the event it is lost or stolen or because a disk drive is missing, a tape falls off the back of a truck, a server gets sold on eBay, a smartphone is left on the bus, or a laptop is left at the airport. While a nuisance, it does not mean these incidences will conflict with your ability to manage these devices.

Claim No. 4: "Database encryption is hard to implement and too slow to use."

We hear this claim from many security practitioners in the field. There is a degree of truth to the statement because database encryption can be difficult to implement, and depending on how it is deployed, requires both application code changes and a database redesign. When diligently applied, however, database encryption protects data that resides on media as well as misuse of sensitive data by credentialed users, with only a marginal performance impact. Careful deployment will sidestep these issues, so we classify this statement as fiction.

Relational database vendors provide 'transparent' database encryption; it's called transparent because it is invisible to database queries and operations, encrypting all database content by altering nothing more than a few configuration settings. Other options, such as products that intercept and encrypt data prior to being written to the file system or use of encrypted disk drives, act 'transparently' as well. While each of these variations have security advantages and detractors, they perform seamlessly and are incredibly simple to implement.

While we are categorizing this one under 'fiction,' performance can be an issue depending on your environment. How many transactions are processed per day? What type of transactions? The age of the hardware and how encryption is used all impact throughput and performance. Simple transactions consisting of single row insertions and updates offer reasonable performance. Heavy analytics or processing on encrypted tables is not suitable for encryption. It is better to remove or obfuscate sensitive information from these databases, or utilize other technologies to protect the data.

Claim No. 5: "Before I can start my encryption project, I need centralized key management and key management standards."

The most common complaint we hear as companies deploy encryption systems is the difficulties surrounding key management. Encrypting data used across multiple systems or by large numbers of users creates key management challenges that require automated support. But that does not account for the majority of data encryption systems which are self-reliant, and where centralized key management is neither necessary nor appropriate. In reality, most encryption solutions build in key management, obviating the need for some kind of "uber" centralized key management service. Since central key management needs to be considered on a case-by-case basis, this statement is false.

Support for a large numbers of users, remote sites that poorly implemented key management in an existing solution, or sharing data across applications are suitable candidates for centralized key management. The complexity of key security, key sharing, access controls and backup/recovery are best performed by specially designed, automated systems. There are many use cases for encryption that do not fall into those categories, such as closed systems or cryptographic systems that support a small number of users, and are not candidates for supporting management services. Examples include:

- Intra-application encryption, such as transparent database encryption, is used to safeguard data within the system from exposure. It does not need to share keys with other applications, and autonomously provides key creation, data encryption and key backup.

- Most backup and file/folder encryption solutions build key management in, and no external management is needed.
- All modern full-disk encryption solutions include centralized key management.
- Public-key systems that use external key authorities and key generation do not require additional central-key management services, unless they do a bad job of managing their keys.

Key management can be difficult and complex, but it's built in to most encryption solutions today. There's no reason to combine your database, endpoint, backup and application keys into a single repository as long as you can manage them effectively individually. You'll waste more time trying to centralize management than it takes to use what's built in.

Claim No. 6: 'Free' encryption is bad encryption."

This is a lie. It is often claimed that free encryption is bad because the code cannot be trusted, when in fact, some of the finest encryption algorithms are available license-free and un-copyrighted. The Twofish Block Cipher [http://www.schneier.com/twofish.html] was one of the finalists for adoption as the AES standard and is just such an example.

To get an idea of why people claim free cryptography is bad, we really need to differentiate between the quality of the theoretical cipher and the quality of the implementation of that cipher. This myth is often propagated because there is the occasional person/company who will try to recreate a well-known cipher without any understanding of the subtleties that go in coding cryptography, resulting in a very bad implementation of a very good cipher. It does not take long to locate high-quality encryption products. Trustworthy cryptographic libraries, with downloadable copies on the Internet, are freely available. You will know the quality ones as they are based upon open and public standards, their code has been reviewed and accredited by experts in the fields of cryptography and cryptanalysis, and they are widely used in the industry.

Keep in mind there are benefits to buying from an accredited vendor, namely the products provide a level of manageability, integration and support that are not found with the free versions.

Keep in mind there are benefits to buying from an accredited vendor, namely the products provide a level of manageability, integration and support that are not found with the free versions. Free-for-use encryption is usually a toolkit or library that requires some customization or integration to work, and is therefore accessible to fewer audiences. Most enterprise IT organizations do not have expertise or time to justify building atop these libraries, and it make sense to purchase a comprehensive solution from a vendor who specializes in off-the-shelf software. But make no mistake, some of the best encryption products in the world are available for free.

In summary, encryption is an incredibly effective and powerful tool, yet it's also shrouded by misunderstanding and consistently used improperly. Focus on using it for the right problems, and you'll find yourself spending less, while being more secure.

Adrian Lane is a senior security strategist with Securosis LLC, an independent security consulting practice. He has 22 years of industry experience, specializing in database architecture and data security. Prior to joining Securosis, Lane was the CTO at the database security firm IPLocks, and he has also served as the vice president of engineering at Touchpoint, three years as the CIO of the brokerage CPMi, and two years as the CTO of the security and digital rights management firm Transactor/Brodi.

Rich Mogull has over 17 years experience in information security, physical security, and risk management. Prior to founding Securosis, Rich spent 7 years as one of the leading security analysts with Gartner, where he advised thousands of clients, authored dozens of reports and was consistently rated as one of Gartner's top international speakers. He is one of the world's premier authorities on data security technologies and has covered issues ranging from vulnerabilities and threats, to risk management frameworks, to major application security. Rich frequently contributes to publications ranging from Information Security *to* Macworld.

Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

READERS' CHOICE AWARDS

ENCRYPTION

SPONSOR RESOURCES

ADVERTISING INDEX

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

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

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

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

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

SR. VICE PRESIDENT AND GROUP PUBLISHER
Andrew Briney

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

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

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Neil Dhanowa ndhanowa@techtarget.com

Patrick Eichmann peichmann@techtarget.com

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 Eric Sockol

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

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

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

TechTarget
The Technology Media ROI Experts

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