INFORMATION SECURITY®

JULY/AUGUST 2011

On the Lookout

Countering modern threats requires hunting down intruders

also

SECURITY INTELLIGENCE

INDUSTRY CONSOLIDATION

TechTarget

INFOSECURITYMAG.COM

FROM OUR SPONSORS

Securing Your Journey
to the Cloud

contents

JULY/AUGUST 2011
VOLUME 13 NUMBER 6

FEATURES

Become a Hunter

19 **TARGETED ATTACKS** Fend off modern computer attacks by turning your incident response team into counter-threat operations.
BY RICHARD BEJTLICH

Turning Insight into Action

28 **INTELLIGENCE** Security teams strive to gain visibility from a deluge of information and put that data to work. **BY SCOTT CRAWFORD**

In the Land of Giants

39 **MARKET TRENDS** Big tech companies are scooping up security vendors with mixed results.
BY MARCIA SAVAGE AND MICHAEL S. MIMOSO

DEPARTMENTS

End of the Line?

5 **EDITOR'S DESK** Large IT companies are buying up security vendors, but that doesn't mean there won't be plenty of room for innovative startups. **BY MARCIA SAVAGE**

PCI Group Urges Caution with Virtualization

11 **SCAN** Online challenges in achieving compliance with payment data on virtualized systems. **BY ROBERT WESTERVELT**

Token Trouble

13 **SNAPSHOT**

How's the Security Job Market? It's Up to You

15 **CAREER ADVICE** Be aware of changing technology and industry trends, and your job prospects will fall in line.
BY LEE KUSHNER AND MIKE MURRAY

ALSO

The Web 2.0 Fallacy

8 **PERSPECTIVES** The idea that social media and other Web 2.0 technologies have vastly altered the threat landscape is plain wrong.
BY RAVILA HELEN WHITE

55 **SPONSOR RESOURCES**

What's Your Acceptable Level of Risk?

(It's Lower than You Think)

Because malware is pervasive and advanced, visiting even popular websites can be risky. But to be relevant and efficient, businesses rely on Web 2.0 sites such as Facebook and Twitter. How can you get the access you need without raising your level of risk? With the most accurate malware detection available, the M86 Secure Web Gateway protects from threats that elude other security solutions, so you can use the Web with confidence.

To learn more about the M86 Secure Web Gateway, visit **www.m86security.com/swg** today. Or call **888.786.7999** for a free product evaluation.

M86™ SECURITY
Real Time Security for the Borderless Network

End of the Line?

Large IT companies are buying up security vendors, but that doesn't mean there won't be plenty of room for innovative startups. BY MARCIA SAVAGE

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

I'VE COVERED THE information security industry for more than a decade and seen plenty of security companies come and go. Remember Entercept? How about Riptech, Neoteris or Teros? All were energetic startups that made a splash before being swallowed up by larger vendors.

In fact, if there's been any constant in the industry over the past 10 years, its consolidation. Symantec's been one of the biggest buyers, acquiring 23 companies between May 2005 and last August. Its purchases include some big security players, such as Verisign's security business and PGP, as well as some outside of security like Veritas. McAfee (which has been through several incarnations, including being part of the old Network Associates) has gone on its own shopping sprees, snagging Foundstone, Reconnex and Secure Computing, among others, before being acquired by Intel last August.

McAfee getting bought by chip giant Intel surprised many in the industry, but the deal was part of an ongoing shift in information security market consolidation. In addition to security vendors snapping up other pure-play security vendors, increasingly we've seen large tech companies outside of the traditional security space like EMC, HP and IBM buying security players. (We examine this trend in depth on p. 39). These industry heavyweights say customers are fed up with managing so many point security products and contend that their integration will drive a more holistic approach that provides better insight into a company's security posture.

In addition to security vendors snapping up other pure-play security vendors, increasingly we've seen large tech companies outside of the traditional security space like EMC, HP and IBM buying security players.

But is this truly the wave of the future for security? Will best-of-breed protection disappear and the market left with a few big players? I don't think so, at least not anytime soon.

Certainly, if vendors follow through on their promise of better integration of security technologies, it could provide a measure of relief for enterprise security managers.

According to a survey of 2,456 IT practitioners in the U.S., UK, France, Japan and Germany by the Ponemon Institute, managing the complexity of security is the top information security challenge facing companies in all of the countries in the study. The survey, which was sponsored by Check Point Software Technologies and released earlier this year, showed that on average, respondents in the U.S. and Germany count seven security vendors in their environments.

That's a lot to juggle. At the same time, though, many enterprises tend to favor best-of-breed technologies. And few security managers are eager to put all their eggs in one basket when it comes to protecting their company's sensitive data. Plus, from what some IT managers and industry say, the large IT vendors have a ways to go on following through on the promises of integrated technologies.

Moreover, there are always going to be new security problems to solve, leaving plenty of room for innovation by small companies that are enthusiastic and nimble. For example, new companies have sprung up with technologies for combating the growing problems of botnets and online banking fraud. And cloud computing has already spawned a handful of new security vendors looking to solve the problems of encryption, identity management and server security in cloud environments.

Most likely, these startups eventually will be acquired, continuing the consolidation cycle. But today, security is too vast of a problem to be solved by a handful of technology providers. ›

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

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

OBSESSIVE COMPULSIVE NETWORK SECURITY PARANOIA.

SOLVED.

We're paranoid as well. We just call it prudence. Backed by every major security certification, we can help design and install the right security solutions for you.

Trust no one except us at CDW.com/security

CDW PEOPLE WHO GET IT™

©2011 CDW LLC. CDW®, CDW·G® and PEOPLE WHO GET IT™ are trademarks of CDW LLC.

The Web 2.0 Fallacy

The idea that social media and other Web 2.0 technologies have vastly altered the threat landscape is plain wrong.

BY RAVILA HELEN WHITE

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

THERE'S BEEN A lot of talk lately about Web. 2.0—Web applications that facilitate sharing, collaboration and user-managed design, such as social media, blogs and wikis—greatly expanding the threat landscape. The first time I heard this, I didn't take it seriously because it was made by someone outside of information security. However, as of late, fellow information security professionals have begun to make the same or similar assertions. Frankly, the threat landscape has not expanded because of Web 2.0.

Threat Considerations

Web 2.0 may represent another attack vector, but the same old threat landscape exists. Even without Web 2.0, technology still is highly vulnerable to threats and attack. Humans make technology. As much as we want to be perfect, we are not. Sure, companies can embed quality checks into technology; however, the dynamic life of technology makes it hard to match quality 100 percent of the time.

Case in point, the non-profit Open Web Application Security Project (OWASP) is doing a fantastic job of evangelizing secure coding. It's working to a degree for those organizations willing to invest in training their developers, but such organizations are rare. Secure coding as a core competency is absent in the developer community. If developers are in a hot industry such as banking, working in an organization that must meet PCI requirements or that's suffered a security breach and privacy sanctions, then secure coding may be a part of the software development lifecycle. But even if the developers code securely, consider the upstream chance that someone will not patch a server the application is hosted on or has added the dreaded "any any" rule to your firewall. The weakest link has always been humans.

Consider the fact that attackers typically take the surest path of exploit. If Web 2.0 did not exist, attackers would target the vector offering the greatest critical mass. For example, appliance-based technology (e.g. SSL VPNs or application delivery controllers) is ripe for exploitation when we consider it is built on open source technology and freely available to anyone who wants to use it. However, it takes a bit more effort and expertise to abuse

the access gained once an exploit has succeeded. There will always be new attack vectors; information security professionals should expect it.

Technology Considerations

Looking at the threat landscape from a service-oriented architecture (SOA) perspective, attackers build on the existing threat landscape by reusing Web 2.0 as an additional attack vector. Attacks over port 25, 80 and 443 are commonplace in Web 1.0 technologies. Attackers reap the benefits of attacking traditional Web services and have taken that knowledge to use against Web 2.0: iFrame, code injection and cross-site scripting (XSS) attacks. The black hat community draws from lessons learned in writing exploits against Web 2.0 technology. One of the biggest lessons is exploitation is possible when defense in depth is rote as opposed to rational. Rational defense in depth will consider layering defenses from at least two perspectives, thereby creating a mesh of defenses that are difficult to defeat. Rote defense in depth is a checklist you can show your auditors; a look beneath the hood will reveal the absence of technology tuning and in some cases, disabling of features that are integral to a strong defense posture.

An example of rote defense in depth is the now infamous Google hack where criminals launched whaling attacks to gain access. The attack is labeled "sophisticated" because it used encrypted channels to hide its presence. Since at least 1999, firewall technology has provided protocol inspection to defeat tunneling of protocols, but some networking and information security professionals have been led to believe protocol inspection either breaks applications or slows down network traffic. Networks that have been sized correctly with data flow analysis will rarely run into problems leveraging protocol inspection.

Ultimately, Web 2.0 is here to stay, but it hasn't radically changed the threat landscape. We're still dealing with the same fundamental threats—fallible humans and old flawed technologies. Rational analysis is best to determine the right defenses.

Ravila Helen White is the director of enterprise security and architecture at a company in the Pacific Northwest. Prior to that, she was the head of information security at The Bill & Melinda Gates Foundation and drugstore.com. Send comments on this column to feedback@infosecuritymag.com.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

THE ULTIMATE
ENTERPRISE THREAT AND RISK MANAGEMENT PLATFORM.

The **ArcSight ETRM Platform** is the world's most advanced system for safeguarding your company against data theft, complying with policies and minimizing internal and external risks. Finely tuned to combat cybertheft and cyberfraud, the ArcSight ETRM Platform gives you better visibility of real-time events and better context for risk assessment, resulting in reduced response time and costs.

Learn more at www.arcsight.com/etrm

ArcSight™
An HP Company

ArcSight Headquarters: 1-888-415-ARST | © 2011 ArcSight. All rights reserved.

ANALYSIS | PCI

PCI Group Urges Caution with Virtualization

Outlines challenges in achieving compliance with payment data on virtualized systems. BY ROBERT WESTERVELT

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

THE PCI Security Standards Council is warning merchants about the complexities of protecting credit card data running in virtualized systems and cautioning that some configurations may make it nearly impossible for organizations to achieve compliance.

The PCI DSS Virtualization Guidelines Information Supplement (.pdf), issued in June, has long been awaited by merchants, qualified security assessors (QSAs) and other security experts. In addition to providing information on virtualized systems located within the network, the document addresses merchants using cloud computing services for payment transactions.

While the PCI virtualization document could help reduce the ambiguity in how QSAs assess virtualized environments, the report may be too broad, says Diana Kelley, a partner with Amherst, N.H.-based consulting firm SecurityCurve.

"There's a lot of useful information here and it's a step towards better information on how to protect cardholder data in a virtualized environment," Kelley says. "Given the scope of this document being both virtualization and cloud, it may raise as many questions as it answers."

The report is grounded in four basic principles: PCI DSS requirements apply to virtualization technologies if cardholder data is present; the technology introduces new risks that must be assessed; the virtual environment must be thoroughly documented to include all interactions with cardholder data; and controls and procedures will vary because there's no one-size-fits-all configuration.

The same basic approach to physical cardholder environments is being applied to virtual environments. Merchants deploying virtualized systems can limit the scope of a PCI assessment if they segment in-scope components from out-of-scope components.

According to the PCI SSC, the hypervisor will always be in scope for PCI DSS if it connects to a system containing credit card data. Access to the hypervisor should be restricted and activity monitoring conducted. In addition, the entire VM is in scope, including the underlying operating system if it contains cardholder data or if it connects to an entry point into the card data environment. Virtual IDS/IPS, firewalls and other security appliances, as well as virtual routers and switches, will be considered in scope if they connect to in-scope system components.

"Weaknesses in hypervisor isolation technology, access controls, security hardening and patching could be identified and exploited, allowing attackers to gain access to individual VMs," according to the PCI virtualization report.

The council also warned organizations against mixing VMs of different security levels and advised that isolating systems containing cardholder data may be impossible if the in-scope and out-of-scope components are hosted on the same hypervisor. The guidance reflects the PCI DSS, which states that organizations must implement one primary function per virtualized server to prevent functions that require different security levels from co-existing on the same server.

"As a general rule, any VM or virtual component that is hosted on the same hardware or hypervisor as an in-scope component would also be in scope for PCI DSS," according to the council's guidance.

Virtual applications and desktops should also be considered in scope if they are involved in the processing, storage or transmission of credit card data or provide access to the card data environment.

For organizations using public cloud service providers, the PCI council warns that in multitenant environments the "physical isolation between tenants is not practical," because all resources are shared. The document warns merchants to thoroughly understand the details of the services being offered by cloud service providers. The service provider must clearly define and document the responsibilities assigned to each party for maintaining PCI DSS requirements.

For organizations using public cloud service providers, the PCI council warns that in multitenant environments the "physical isolation between tenants is not practical," because all resources are shared.

Security Curve's Kelley says Visa provides merchants with a list of cloud service providers that have been validated for PCI. She says despite the validation, the onus is on merchants to isolate systems containing cardholder data and put effective controls in place to maintain PCI compliance.

"Your cloud provider can be validated, but what is done in the provider's cloud is the merchant's responsibility," Kelley says.

The PCI virtualization report was developed by the PCI Council's Virtualization Special Interest group, chaired by Kurt Roemer, Citrix chief security strategist, and representatives from companies that include Bank of America, L.L. Bean, AT&T, HP, Savvis, Southwest Airlines, VMware and Verizon Business.

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

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Token Trouble

by *Information Security* staff

RSA SecurID, the industry's ubiquitous two-factor authentication token, hangs from the key chains of more than 40 million end users worldwide. It was a trusted ally of security professionals and end users until that trust was threatened by an attack announced March 17. Since the persistent attack was announced by RSA president Art Coviello, other attacks on defense contractors and large enterprises have been linked to the attack on SecurID. Here's a Snapshot of the SecurID breach by the numbers:

45,000: The number of SecurID tokens being replaced at Lockheed Martin

2'S ARE WILD: Two phishing attacks used against RSA, over a two-day period to two small groups of low-level RSA employees, featuring two separate attack vectors—a Microsoft Excel file and a Adobe Flash zero-day attack.

2011 RECRUITMENT PLAN: The subject line of the phishing email used against RSA.

MITIGATION; RSA OFFERS TO:

- Replace SecurID tokens for customers with concentrated user bases typically focused on protecting intellectual property and corporate networks.
- Implement risk-based authentication strategies for consumer-focused customers with a large, dispersed user base, typically focused on protecting Web-based financial transactions.

61%: SecurID market share (Frost and Sullivan)

overheard

"Certain characteristics of the attack on RSA indicated that the perpetrator's most likely motive was to obtain an element of security information that could be used to target defense secrets and related IP, rather than financial gain, PII, or public embarrassment."

–ART COVIELLO, president, RSA, The Security Division of EMC

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Demonstrate your value without saying a word.

Résumés/CVs may *list* your experience and knowledge, but an ISACA® certification designation after your name *proves* it.

www.isaca.org/certification-infosecmagazine

CISA® Certified Information Systems Auditor® — An ISACA® Certification

CISM® Certified Information Security Manager® — An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT® — An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™ — An ISACA® Certification

December Exam Date: 10 December 2011
Registration Deadline: 5 October 2011

ISACA®
Trust in, and value from, information systems

How's the Security Job Market? It's Up to You

Be aware of changing technology and industry trends, and your job prospects will fall in line. BY LEE KUSHNER AND MIKE MURRAY

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

WORKING AS AN INFORMATION security recruiter and career advisor, many of my conversations begin with the question, "How is the market?" While the question at face value appears to be simple, the answer is complex, and greatly dependent on variables uniquely associated with the individual.

Information security professionals possess many different skill combinations. Some refer to themselves as generalists, having broad knowledge that includes technical, organizational and management skills. Others categorize themselves as specialists or subject matter experts who have deep expertise in a discipline such as penetration testing, network security, application security or forensics. Just as there are a variety of skills profiles, there are a variety of markets for these individuals and their information security career. These markets are driven by two external factors: broader-based technology trends, and locally based corporate and industry trends. Broader market trends for information security professionals often involve the emergence of new technology trends that drive demand for specific talent. Technical trends enhance the market for subject matter experts and have little effect on generalists.

The emergence and importance of Web-based applications is an example of a recent business trend driving the market for Web application penetration testers. The emergence of this broader market force drove up the value and demand for information security professionals with these specific Web application testing skills and technical foundations, and, conversely, drove down the demand and compensation for traditional network penetration testers. (Understand that a global trend will rarely affect industry-leading talent.) Traditional network penetration testers who recognized this and were capable of learning Web application testing skills were able to make the adjustment and create additional value because of their skill

Lee Kushner's and Mike Murray's blog can be found at www.infosecleaders.com where they answer your career questions every Tuesday, or you can contact them via email.

Lee Kushner is the president of LJ Kushner and Associates, an information security recruitment firm, and co-founder of InfoSecLeaders.com, an information security career content website.

Mike Murray has spent his entire career in information security and currently leads the delivery arm of MAD Security. He is co-founder of InfoSecLeaders.com, where he writes and talks about the skills and strategies for building a long-term career in information security.

blend. In turn, they created a secondary market, based on their skill combination. On the other hand, traditional network penetration testers who decided not to adapt or were not capable, have seen the market for their skills shrink dramatically.

Currently, some of the emerging global information security technology trends include the implementation of security information and event management tools, data loss prevention tools, cloud computing, software security and protecting companies against advanced persistent threats. In all of these skill disciplines, there are more ongoing projects than there are competent security professionals to execute upon them. Information security professionals who have documented successful experience with these technologies currently have the luxury of a strong employment market.

Another prime market driver for information security professionals are industry trends. Over the last few years, companies have become more exposed to the consequences of not protecting their data and their customer information. Through breach notification legislation, regulations (primarily PCI DSS), hacktivism and the media, information security concerns have moved to the forefront of many businesses that have never properly invested in the development of an information security program.

When companies begin to formally commit to the construction of an information security program, or make the decision to upgrade their existing programs, professionals with broader information security skills generally stand to benefit. In these types of scenarios, companies are most concerned about securing their businesses and managing risk, and are prone to hire information security leaders who can help ingrain information security into the fabric of the business. Information security professionals who have specific industry knowledge, and excellent communication skills, generally can benefit from these situations.

Broader forces influence the market at large for information security professionals, but the individual determines his or her career market.

Broader forces influence the market at large for information security professionals, but the individual determines his or her career market. Although skills are the most important component to the equation, it is the personal factors that ultimately play an equal role in determining the market for your skills. Many times, in order to advance your information security career and maximize your skills, you need to be willing to make some sacrifices that include travel, additional commuting and relocation. Many information security professionals find there is a market for their skill, but the required personal sacrifices prohibit them from recognizing the market opportunity.

If I had to answer the initial question, I would say the overall market for information security professionals is quite healthy. The combination of the pent-up demand created by the economic slowdown and the continued emergence of information security as a business enabler and differentiator, has provided a rebirth of opportunity for highly

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

skilled information security professionals. However, many of these newly created positions come with increased personal demands, including long work hours, extensive travel and a high level of scrutiny.

As in the past, you are the determining factor for the market for your skills. Competition, both in the present and the future, will continue to increase, and the proactive management of your information security career, through continued skill development and by making strategic career investment, is the only way to ensure the market for your skills remains strong. ›

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Get recognized— our members do.

In a sea of IT professionals, ISACA members get noticed.

Many IT and information systems professionals worldwide consider membership in ISACA® essential to their career advancement. As a nonprofit, global association, ISACA connects exceptional people with exceptional knowledge to provide members with a robust offering of professional resources.

ISACA®

Trust in, and value from, information systems

www.isaca.org/benefits-infosecmagazine

Become a Hunter

Fend off modern computer attacks by turning your incident response team into counter-threat operations.

BY RICHARD BEJTLICH

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

IT'S NATURAL FOR members of a technology-centric industry to see technology as the solution to security problems. In a field dominated by engineers, one can often perceive engineering methods as the answer to threats that try to steal, manipulate, or degrade information resources. Unfortunately, threats do not behave like forces of nature. No equation can govern a threat's behavior, and threats routinely innovate in order to evade and disrupt defensive measures.

Security and IT managers are slowly realizing that technology-centric defense is too easily defeated by threats of all types. Some modern defensive tools and techniques are effective against a subset of threats, but security pros in the trenches consider the "self-defending network" concept to be marketing at best and counter-productive at worst. If technology and engineering aren't the answer to security's woes, then what is?

To best counter targeted attacks, one must conduct counter-threat operations (CTOps). In other words, defenders must actively hunt intruders in their enterprise. These intruders can take the form of external threats who maintain persistence or internal threats who abuse their privileges. Rather than hoping defenses will repel invaders, or that breaches will be caught by passive alerting mechanisms, CTOps practitioners recognize that defeating intruders requires actively detecting and responding to them. CTOps experts then feed the lessons learned from finding and removing attackers into the software development lifecycle (SDL) and configuration and IT management processes to reduce the likelihood of future incidents.

People who know how to detect and respond to intrusions are the key to fighting modern threats.

CTOps certainly requires application of engineering and technology, but the focus remains on people. People who know how to detect and respond to intrusions are the key to fighting modern threats. We will define what those people should do, as well as how you can ensure your security staff is meeting the challenge posed by modern threats.

An emphasis on CTOps should not come at the expense of measures that try to remove vulnerabilities from the enterprise. Efforts to improve software security through better coding, improved configuration, and sound business logic are the preferred way to build a sound foundation for enterprise computing. CTOps practitioners are usually very supportive of efforts to rid the enterprise of weak applications, because being a hard target frustrates intruders and reduces the overall number of intrusions that defenders must detect and handle. Therefore, CTOps encourages software security efforts that build security into applications.

JUSTIFYING COUNTER-THREAT OPERATIONS

What does it mean to conduct CTOps? I recommend either building or repositioning the enterprise computer incident response team (CIRT) as the home for CTOps. If the organization lacks a CIRT, or the CIRT doesn't currently conduct CTOps, the first requirement is convincing management that CTOps is necessary.

No single argument for conducting CTOps or building a CIRT will likely resonate with management. Rather than relying on a single argument, CIRT builders may find one or more of the following "13 C's" to be helpful. Incorporating these justifications into a discussion may help convince those who have budgetary and organizational authority to facilitate construction of a CTOps-capable CIRT.

1. **Crisis.** When the enterprise suffers a devastating security incident, managers are usually ready to take action. Although this is the worst way to justify a program because it comes *after* an incident, it is often very effective.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

2. Compliance. Compliance requirements may contain the language necessary to construct a team. Beware applying resources in such a manner that the original CTOps mission is lost. For example, creating a team that does nothing more than monitor for configuration changes will not result in finding advanced or even moderately skilled intruders.

3. Competitiveness. My blog post "Forget ROI and Risk. Consider Competitive Advantage" explains that preserving or enhancing competitive advantage often resonates with business people. Few people responsible for a profit and loss operation in an organization want to "lose the game." If these decision makers can frame perception of security in terms of competition, they may understand the importance of CTOps and CIRTs.

4. Comparison. If your security team is 10 percent the size of the average peer organization, it's not going to look good when you have a breach and have to justify your decisions. The blame for under-resourcing the CIRT will likely rest with the manager to whom the CIRT reports, so convince him or her to fund the operation to deflect possible future criticism.

If your company security team is 10 percent the size of the average peer organization, it's not going to look good when you have a breach and have to justify your decisions.

5. Cost. It's likely that breaches are more expensive than defensive measures, but this can be difficult to capture empirically. In regulated industries one may be able to estimate the fines that could be levied against a breach victim, and the costs of funding credit monitoring services and associated legal and human resource expenses. For example, the U.S. Department of Defense recovered $1.3 million of a $5.4 million Pentagon contract from Apptis Inc. Investigators claimed Apptis "provided inadequate computer security" due to a breach in a subcontractor's system. (Contractor Returns Money to Pentagon, *Washington Times*, July 25, 2009.)

6. Customers. It seems rare to find customers abandoning a company after a breach; people still shop at TJX brands. Still, you may find traction here. Compliance is supposed to protect customers, but it often is insufficient.

7. Constituents. I use this term to apply to internal parties served by a central CIRT. Large companies often provide services to other business units, so a cross-company constituency may ask for help fighting intruders.

8. Controllership. A well-governed organization can often point to a centralized counter-threat center of excellence, such as a CTOps-practicing CIRT.

9. Conservation. This is a play on "green IT." What has a lower carbon footprint: 1) flying consultants all over the world to handle incidents, or 2) handling them remotely by moving data, not people? A properly resourced and equipped CIRT can rely on instrumen-

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

SECURING YOUR JOURNEY TO THE CLOUD

TREND MICRO™ IS #1 IN VIRTUALIZATION SECURITY*
VMWARE® IS #1 IN VIRTUALIZATION**

Trend Micro and VMware allow you to fully capitalize on the operational benefits of virtualization and cloud computing with innovative, complementary solutions for security and compliance. These include the first and only agentless antivirus, intrusion prevention and integrity monitoring solutions for virtualized datacenters and desktops. Additionally, our encryption and key management solution for public, private and hybrid clouds allows you to better manage and secure your data wherever it resides. The result is a true business advantage. **»TRENDMICRO.COM/VMWORLD**

SCAN ME!

vmware®

VISIT US AT VMWORLD® 2011 IN LAS VEGAS

TREND MICRO™

*2011 Technavio, *Global Virtualization Security Management Solutions* **IDC, *Worldwide Quarterly Server Virtualization Tracker*
© 2011 Trend Micro, Inc. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Inc.
© 2011 VMware, Inc. All rights reserved. VMware and VMworld are registered trademarks of VMware, Inc.

tation that accesses data needed to analyze intrusions, rather than sending people into the field to fight fires. See my blog post "Green IT" for more details.

10. Consolidation or Centralization. These themes are likely to enable specialization, more effective internal resource allocation, and improve defenses.

11. Confidence. Confidence applies to all parties involved. Can you trust your data?

12. Counting. Developing metrics is crucial for justifying a CIRT's role. Managers often want to know how regularly the enterprise suffers compromises, and how quickly the CIRT can detect and respond to intrusions.

13. [Securities and Exchange] Commission. A growing number of public security voices (for example, Melissa Hathaway) advocate disclosing significant security breaches in the 10-K forms required of publicly traded companies by the SEC. Many companies already report serious intrusions, as noted in my blog post *"Publicly Traded Companies Read This Blog"*.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Five Reasons CIRTs Should Join FIRST

FIRST is the Forum of Incident Response and Security Teams, an international organization with more than 200 members. Here's why your organization's CIRT should join:

1] Professional incident responders tend to be FIRST members. FIRST membership is similar to certification, but it's not the result of passing a test. Rather, FIRST membership is an ongoing, dynamic relationship that demonstrates a certain level of maturity for each organization.

2] The FIRST membership application process may help justify some CIRT initiatives. For example, FIRST membership may help make the case for a separate, isolated malware analysis network and environment.

3] Applying for FIRST membership compels CIRTs to document a variety of processes. For example, FIRST requires applications to document how they handle sensitive information from third parties. Following the application process brings a certain degree of rigor and clarity to CTOps work.

4] FIRST membership is sometimes a differentiating factor when recruiting talent.

5] FIRST members share operational practices and information through mailing lists and conferences.

5 reasons

—RICHARD BEJTLICH

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

SIZING AND ORGANIZING THE CIRT

Once management believes a CIRT is necessary to conduct CTOps, the next questions involve the size of the CIRT and its structure. In order to help answer this question, I polled 12 organizations with employee counts in the low thousands to the mid hundreds of thousands. I asked each organization to count the number of people they employed to detect and respond to intrusions. Based on this survey, I determined that the average number of detection and response roles for these 12 organizations was five per 10,000 employees. In other words, if your company consists of 60,000 employees, you would likely have a CIRT with 30 people.

This 5 per 10,000 standard may sound fanciful to many readers, but consider the sorts of roles one must fulfill to be able to truly combat threats to the modern enterprise. The last CIRT that I built consisted of the following three teams:

- The Incident Response Center (IRC), responsible for the daily incident detection and response mission.
- The Security Assurance Team (SAT), responsible for Threat Intelligence and Reporting, Red Team engagements, and Technical Assistance (i.e., internal consulting).
- The Support Group,responsible for designing, building, and running infrastructure used by the IRC and SAT.

Within each CIRT sub-team, I divide responsibilities by skill level. All of these roles and experience levels will likely vary depending on the nature of the organization hosting the CIRT.

The IRC consists of these team members:

- Incident handlers are subject matter experts (8-12 years of technical experience) who use unstructured analysis tools and techniques to detect and respond to the most advanced or complicated threats.
- Incident analysts (4-8 years of

Six Steps to Take Now

1] Create a team logo.

2] Create a team name.

3] Be a leader, not a manager. Read my post Everything I Need to Know About Leadership I Learned as a Patrol Leader.

4] If you are not making progress on executing your vision within a year, or you encounter inordinate resistance, consider another role.

5] Create documents justifying your team and have them ready when management asks.

6] Use time-based metrics to explain workload. For example, if it takes two weeks for your analysts to review indicators, and that figure continues to increase, use that metric to justify additional hires. It's similar to a manufacturing situation, except the output is incident reporting. ›

—RICHARD BEJTLICH

6 steps

technical experience) are developing as subject matter experts; they work with incident handlers to learn how to deal with advanced threats, but they also mentor event analysts.

- Event analysts (2-4 years of technical experience) are beginning their incident detection careers; they use structured analysis tools and techniques to detect and respond to well-understood threats.

The SAT consists of these team members:

- Principal analysts are subject matter experts (8-12 years experience) who understand and conduct advanced counter-intelligence work, fully simulate adversary activity, and/or lead complicated security consulting projects.
- Senior analysts (4-8 years of technical experience) are developing as subject matter experts; they work with principal analysts on larger projects while mentoring analysts.
- Analysts (2-4 years of technical experience) demonstrate aptitude in security assurance, but are learning how to offer these services.

The Support Team consists of these team members:

- Developers write software and tools to help the IRC and SAT detect and respond to intruders.
- Architects design systems and lead major projects in conjunction with engineers who implement tools and techniques.
- Administrators care for the systems used by the IRC and SAT, as well as infrastructure enabling the support team mission

I did not provide estimates of experience for each role in the support team because system administrators could have 20 years of maintaining infrastructure under their belt, whereas a very effective architect might only have 8 or 10 years of experience.

I recommend a person lead each of these three teams, with a single CIRT leader working as director of incident response. The director of IR should name one of the three team leaders as his or her deputy.

SOCs vs CIRTs

At this point, it may sound like we are describing a security operations center (SOC). To a certain extent the work of a SOC is pertinent to CTOps. SOC work tends to imply a more routine workflow whereby security devices generate alerts for generally well known or recognizable security violations. Analysts interpret the alerts, generate reports, and notify their constituencies. All of this work is necessary, but it is not sufficient to combat modern threats. SOC work tends to be somewhat passive, structured, and often not very creative.

In addition to performing SOC work, CTOps requires more active, unstructured, and creative thoughts and approaches. One way to characterize this more vigorous approach to

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

detecting and responding to threats is the term "hunting." In the mid-2000s, the Air Force popularized the term "hunter-killer" for a missions whereby teams of security experts performed "friendly force projection" on their networks. They combed through data from systems and in some cases occupied the systems themselves in order to find advanced threats. The concept of "hunting" (without the slightly more aggressive term "killing") is now gaining ground in the civilian world.

If the SOC is characterized by a group that reviews alerts for signs of intruder action, the CIRT is recognized by the likelihood that senior analysts are taking junior analysts on "hunting trips." A senior investigator who has discovered a novel or clever way to possibly detect intruders guides one or more junior analysts through data and systems looking for signs of the enemy. Upon validating the technique (and responding to any enemy actions), the hunting team should work to incorporate the new detection method into the repeatable processes used by SOC-type analysts. This idea of developing novel methods, testing them into the wild, and operationalizing them is the key to fighting modern adversaries.›

Richard Bejtlich is the former director of incident response for General Electric, and served as principal technologist for GE's Global Infrastructure Services division. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

THREAT DEFENSE

INTELLIGENCE

CONSOLIDATION

SPONSOR RESOURCES

Blue Coat

Find The Dangers That Lie Within Social Networking

Blue Coat web security solutions analyze more than 3 billion web requests per week to provide businesses with a real-time defense against malware and other threats, whether you need appliance-based or cloud-based web security.

ForSaferSocialNetworking.com

© 2011 Blue Coat Systems, Inc. All rights reserved.

Turning Insight into Action

Security teams strive to gain visibility from a deluge of security information and put that data to work. BY SCOTT CRAWFORD

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

GETTING A HANDLE on "big data" has become a priority for every aspect of business, and information security is no exception. The number and variety of threats and vulnerabilities have exploded in recent years. Add in the challenges of managing exposure in complex IT environments, and the burden on security organizations just to stay abreast of it all can be overwhelming.

Yet security's own data deluge also conceals an opportunity, for in this mass of information is the evidence that could help businesses better understand the reality of their security posture and manage risk more effectively. How can security teams turn big data from a threat into an opportunity?

This is the objective of security intelligence, a term that is undergoing a re-definition on

multiple levels. As the number and variety of potentially rich data sources has expanded, security professionals are striving to develop disciplines and expertise that yield more actionable intelligence. Security technologies also are turning to more dynamic data sources to drive their functionality, in the beginnings of a trend that may transform the nature of IT defense. As these initiatives gain momentum, innovations from related domains such as business intelligence and the rise of what Turing Award recipient Jim Gray calls the "fourth paradigm" of data science, may become more visible in the world of IT risk.

The changes being wrought by an abundance of information and the demand for greater insight into the reality of information risk are already well underway. How security teams learn to make the most of both the opportunities and the challenges these changes present may transform what the practice of security becomes tomorrow, as a focus on "data-driven security" shapes the way information turns to insight—and action.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

DRIVING THE NEED FOR CHANGE

The need to tame runaway data is just one issue facing security teams. A far more significant factor, particularly for organizations responsible for high-value information assets, is an increased recognition of the economics of exploit. Those who know their assets are a target also know that dedicated attackers have the means to evade many common defenses. Nick Selby, a Texas police officer and managing director of PoliceLedIntelligence.com, says, "If it costs you 50 million to build intellectual property but only 3 million to steal, [what attackers] can say no to numbers like that?" The need for realistic awareness of the threat landscape—within the enterprise and beyond—has led many businesses to expand their investment in both broader insight outside the organization, and deeper visibility within.

"If it costs you 50 million to build intellectual property but only 3 million to steal, [what attackers] can say no to numbers like that?"

–NICK SELBY, Texas police officer and managing director of PoliceLedIntelligence.com

Large enterprises aren't the only organizations that have become more sensitive to information risks. According to Rick Howard, general manager of Verisign's iDefense security intelligence unit, a growing awareness of more sophisticated techniques for getting at sensitive data or threatening business priorities has heightened the need for security intelligence across a broader spectrum of organizations than in the past. "Cyberwarfare, espionage—large companies and governments have known about these threats for a long time," says Howard. "But when it comes to things like hacktivism, reputation risk or the more dedicated adversary, a much larger swath of businesses worrying about these today than they have been ever have before."

Within the enterprise, businesses need to improve their performance with the information

they already collect. In the 2009 Verizon Data Breach Investigations Report, evidence of a breach was available to the victim organization in 82 percent of cases, but was either not noticed or not acted on. That figure actually increased to 86 percent in Verizon's 2010 report. In its 2011 report, 86 percent of breaches were discovered by a third party. Many companies recognize that their current approaches will not address these failures, and are looking for ways to make better use of the information they collect.

Many businesses also recognize that potentially meaningful data may be locked up in silos of information that, if better used, could reveal the nature of threats more fully. For example, marketing data says much about behavior across entire populations, while within the business, logistical and facilities data can reveal where physical activity corresponds to a digital threat. Executive protection services may correlate suspicious behavior in IT with a specific target, while resources from social media to brand protection services can be used by defenders to identify potential threats before they materialize.

These factors suggest how the drivers of security intelligence may have much in common with those behind the growth of business intelligence (BI) for yielding valuable insights out of large volumes of often disparate data sources. Not surprisingly, more than a few major enterprise technology vendors such as EMC, HP and IBM have increased their investments in both security and BI in recent years. These two lines of business may not have much in common—yet—but the opportunity is there. The converging interests of security and areas such as data analytics suggest where they may intersect tomorrow, as the demand for security intelligence drives the need for better performance in information management, and as linkages grow and expand across data sets that, on the surface, may seem unrelated.

"Intelligence is a discipline. It may be a noun that describes what you get, but ultimately it is a process. The problem is not with getting information disseminated. It's with extracting meaningful, actionable truth."

–NICK SELBY, Texas police officer and managing director of PoliceLedIntelligence.com

A focus on technology, however, can distract security organizations from where investment in intelligence may be needed most. "Intelligence is a discipline. It may be a noun that describes what you get, but ultimately it is a process. The problem is not with getting information disseminated. It's with extracting meaningful, actionable truth," Selby says. This highlights the need for organizations to develop both individual expertise and organizational processes for making the most of security data.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

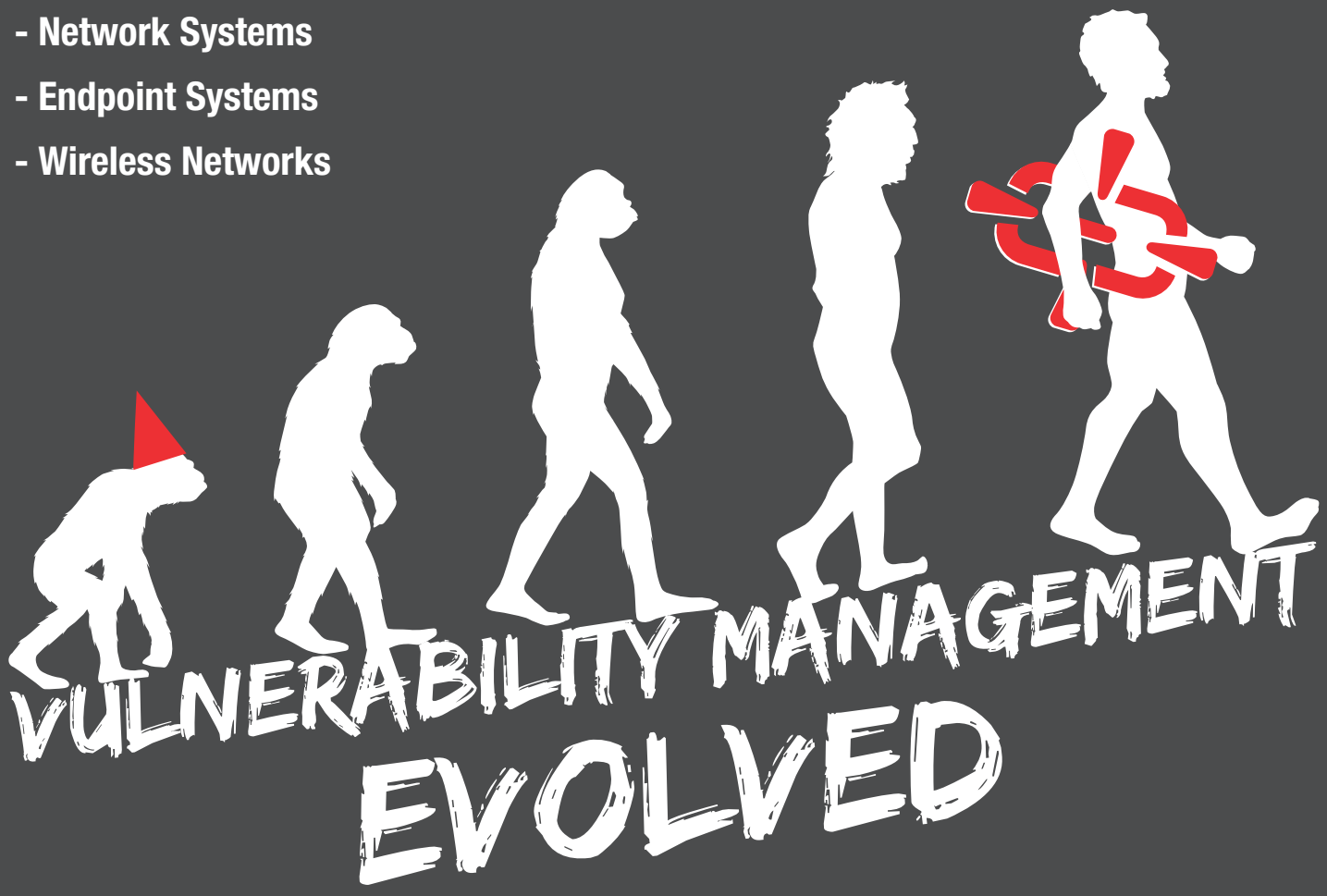
CORE IMPACT PROFESSIONAL

Find the gaps in your vulnerability management program ...

Click here to download a free gap analysis tool.

Penetration Testing Software for:

- Web Applications
- Network Systems
- Endpoint Systems
- Wireless Networks



CORE IMPACT® Pro provides the missing link in your vulnerability management program.

- Identify exploitable vulnerabilities
- Prioritize critical exposures and risks
- Map attack paths across IT layers
- Eliminate false positives
- Assess end users against phishing attacks
- Comply with PCI, FISMA/NIST, HIPAA and other mandates

Learn more:
Visit www.coresecurity.com
or call us at (617) 399-6980

CORE SECURITY TECHNOLOGIES

Copyright ©2010 CORE SDI, Inc. Core Security Technologies and CORE IMPACT are registered trademarks of CORE SDI, Inc.

NEW SOURCES OF INTELLIGENCE DATA

IT security product vendors and intelligence services have long provided current information on vulnerabilities and attacks to their clients. With increased growth and diversity in adversaries and threat tactics, these services have expanded their range. Providers such as Cyveillance, Verisign's iDefense business and Vigilant's recently introduced intelligence services enable organizations to extend their eyes and ears into domains outside their normal reach. Subscribers often benefit from information available only to those with specific expertise, credentials or ability to participate in restricted groups or organizations. Providers may offer access to in-country foreign expertise or specialized insight into brand or reputation risks that may be hard to come by otherwise. Intelligence services may also play to their strengths, as with iDefense insight that supports assurance for critical services such as DNS, thanks to its relationship with parent Verisign.

The ability of intelligence services to connect threats against IT with physical risks has become particularly valuable in industries such as utilities, where these interests often intersect. Lester "Chip" Johnson, a 28-year veteran of South Carolina law enforcement and security for the energy sector who now heads his own security and risk management consulting firm, says, "You could literally have your own staff doing just this alone, full time. No one's budget will allow for that, yet utilities and energy companies can't do without this

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

The Risks of Intelligence

Intelligence gathering has sparked privacy and security concerns.

Today's information explosion can be a potent enabler of security initiatives, but it has its risks. First off, the tools that enable security teams to better understand malicious activity may also be just as available to the adversary. Search, for example, is already recognized as a technology that can reveal more personal and corporate information, including security weaknesses, than many would care to acknowledge.

The explosion of social networks has amplified these concerns. "One of the biggest changes we've seen in the last year or more has been the use of social networks by criminals, not only through malicious URLs, but also to discover more personal information about targets to elicit a specific response," says James Brooks, Cyveillance director of product management. He cites the openness of social networks that leads many to assume a false sense of security. Others point to the difficulty of keeping up with a broad, intricate and often changing scope of privacy settings on sites such as Facebook.

Civil libertarians and those who advocate for greater access to the information collected by governments and other organizations have spoken out, not just about intelligence gathering in the name of security, but also about risks such as the relentless collection of personal information by search and social networks. In a recent interview with Russia Today, Wikileaks founder Julian Assange called Facebook "the most appalling spying machine that has ever been invented."

–SCOTT CRAWFORD

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Security Intelligence and "Big Data"

The techniques of large-scale data analysis could help security.

So far, discussions of "big data" in the realm of security have largely to do with the sheer volume of data that confronts security teams. Outside the field, "Big Data" (note the capitals) may more frequently invoke large-scale data analysis, data warehousing and mining, and tools such as multidimensional databases and the increasingly recognized toolsets such as Hadoop and techniques for optimizing large-scale analysis such as MapReduce. Do these two notions of big data ever intersect? Do the techniques of large-scale data analysis have potential for application to security and intelligence?

Though they still have a ways to go before these intersections become common, the answer is a resounding "yes." Consider, for example, that not only can columnar databases such as Hadoop's HBase and Google's BigTable scale out enormously, they may also free data management from the need for schemas or pre-existing structural definitions. Schemas can be generated when data is retrieved, rather than relying on a schema defined when the database is initially set up. This means that, when new types or formats of data are introduced, they can be added to the database virtually as-is. This is a particular benefit to security and intelligence data, which may include such things as malware variants or a wide variety of digital evidence–some perhaps not previously used in intelligence gathering.

Consider also that techniques of distributed analysis such as MapReduce and highly scalable storage strategies such as the Hadoop Distributed File System (HDFS) not only enable massive scale for data management, they also provide techniques for improving the performance of analysis by assuring that computation is carried out as close to the data as possible. And this, in turn, more closely fits models of cloud computing that make highly responsive, large-scale data analysis for time-sensitive tasks such as intelligence gathering far more accessible to a wider range of organizations than many legacy approaches. ›

–SCOTT CRAWFORD

tools

sort of information in today's world. Intelligence services help meet that need."

As the availability of information increases, so does access to what some regard as "open source" intelligence. Security professionals are always seeking new ways to obtain data. "We're always trying to get as close to the source as humanly possible," says one security analyst for a financial services firm who, though his organization subscribes to intelligence services, relies even more on his relationships with leading researchers, community-based efforts, and information that can be collected directly by his organization.

The ubiquitous information gathering capabilities of search and social networks are also having an impact on security intelligence. Businesses increasingly look to sources such

as Google and Facebook for background on prospects, partners and job candidates—a trend not lost on security intelligence services, which also use these resources in gathering broader information on the risks their clients face. And more than a few security pros rely on Twitter for keeping up with the latest thinking among their peers.

One increasingly visible source of intelligence is behavior observable directly from network and application activity. Fraud data collected in this way helps defend tangible assets against exploit in banking, for example. Within the enterprise, technologies such as those of AccessData's SilentRunner, NetWitness (recently acquired by EMC), Niksun and Solera Networks enable organizations to record complete network traffic content for threat investigation and forensic analysis. At the service provider level, companies such as Narus (acquired by Boeing) can derive intelligence from observation of network content on carrier-class networks, while others, such as Verint, provide analytic capabilities for complex network content such as voice, video and unstructured text.

It's worth noting that vendors such as Narus originated in network usage analysis to help service providers develop more profitable services. This echoes other ways in which network management technology has become valuable in security, as with anomaly detection technologies used in intrusion detection and security event management systems that use NetFlow data originally intended to support network management for applications. This suggests the role other vendors with visibility into network activity may play in delivering intelligence services in the future. Renesys, for example, provides data on how network traffic actually moves throughout the world. Today, this capability helps ISPs—and their customers—keep a closer eye on how network traffic is managed in compliance with service agreements, for example. Tomorrow, this capability may find useful application in providing insight into network traffic movement with direct implications for security.

Many data sources focus on what may be considered "inputs"—potential threat sources, attacks in the wild or exploitable vulnerabilities.

Many data sources focus on what may be considered "inputs"—potential threat sources, attacks in the wild or exploitable vulnerabilities. In the last few years, outcome data has added a dimension of realism to security intelligence that was largely lacking. Few examples highlight this more than information on data breach cases provided by those such as the Open Security Foundation through its DataLossDB the Privacy Rights Clearinghouse, and Verizon's annual Data Breach Investigations Report. These resources reveal how compromise actually succeeds across multiple incidents, highlighting commonalities and calling out trends.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

PUTTING INTELLIGENCE TO WORK

One of security's biggest challenges is turning data not only into understanding (which is, of course, implicit in the very meaning of "intelligence"), but into action.

Intelligence services increasingly focus on tailoring the delivery of information to meet specific customer requirements. Secunia's Vulnerability Intelligence Manager enables organizations to customize vulnerability alerts that target those most directly responsible for handling specific systems or vulnerability remediation processes within an organization. Cyveillance, iDefense and Vigilant support the integration of their feeds directly into centralized platforms for managing security data, such as security information and event management (SIEM) consoles, vulnerability management platforms such as Qualys, and systems for managing IT governance, risk management and compliance (GRC) priorities.

Recent years have also seen the rise of data synthesis platforms such as Maltego and Palantir that give investigators tools for connecting data points and visualizing analysis in ways that make understanding more vivid. Forensic analysis platforms have also expanded their ability to develop data synthesis, combining tactical intelligence gathering from the network with input from multiple data sources and creative approaches to data visualization.

Intelligence is also being put to work more directly in the technologies of defense. Legacy defense technologies may be considered "data-consuming," caching local copies of static data such as threat signatures that are updated intermittently. In contrast, today's emerging defenses may be considered more "data-driven," with more dynamic dependence on data feeds or behavior observed in real (or near-real) time.

Distributed threats such as botnets, for example, can be identified through techniques such as recognizing when compromised systems attempt to communicate with known malicious command-and-control hosts. Team Cymru's BATTLE service for law enforcement and companies such as Damballa, FireEye, Umbra Data and Endgame Systems' recently introduced ipTrust products enable customers to leverage their knowledge of botnet behavior gained across multiple enterprise and service provider networks. Using these tools, businesses can identify—and in some cases, block—specific incidents of compromise based on current insight into fast-changing botnet topologies.

Distributed threats such as botnets, for example, can be identified through techniques such as recognizing when compromised systems attempt to communicate with known malicious command-and-control hosts.

Fraud prevention technologies also leverage insight into observed behavior. Risk-based authentication techniques use this data directly to increase the level of authentication required or deny access altogether when attempts to access sensitive resources appear to be

anomalous, such as access attempts from two distant physical locations within a few minutes of each other. Silver Tail Systems monitors website traffic over time, recognizes attempts to abuse or manipulate application behavior, and enables organizations to mitigate risk by modifying business flows in Web applications. Mykonos can both identify and track malicious parties that seek to exploit Web applications while defending the underlying application itself.

Antivirus and antimalware technologies increasingly look to data sources to improve performance in recognizing new attacks. When suspicious content is not specifically recognized by security software on the endpoint, its characteristics can be referred to centralized resources for more immediate analysis and faster deployment of defense. These approaches leverage insight into the prevalence of software gathered from among their global customers to help differentiate threats and bring the identification of new attacks to all customers more quickly. They help close the "zero-day window of opportunity" and reduce the footprint of security software at the endpoint. Such techniques are already reshaping the nature of antivirus and antimalware, as exemplified by Symantec's Insight, McAfee's Global Threat Intelligence, and Trend Micro's Smart Protection Network.

THE ULTIMATE MEANING

Greater insight poses risks of its own. Intelligence can be an advantage to the adversary as well as to the defender. Concerns about both the scale and the nature of information collected in the name of intelligence have motivated some to take direct action to expose what they see as abuses *(see "The Risks of Intelligence")*.

Regardless whether intelligence is seen as an asset or a threat, there seems little doubt that the growing abundance of data available to security teams will continue to drive the demand for greater insight into risk. In order to make the best—as well as the most conscientious—use of this data, people will need to develop the individual skills and the organizational practices that define the ultimate meaning of intelligence. Police-Led Intelligence's Selby says, "There is an 'aliveness' to intelligence that people often overlook. Intelligence must be iterative, with constant feedback, checks on bias, constantly evaluating and re-evaluating sources and calling conclusions into question."

Those on the cutting edge of security information analysis would likely agree with the human-centric nature of intelligence. In fact, one such professional says, "Technology can clear away a lot of the noise, but you must first make it understand what is noise, and what isn't. Automation can't make any difference until we tell it what to care about, and we may not know what to care about until we've investigated."

This suggests the rise of a new approach to security practice, one where defense becomes a function of visibility, and where automation is more dynamically and responsively defined by investigative expertise. The value of the practice of investigation within security organizations has already been called out by examples such as EMC's acquisition of NetWitness.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Though a technology play, NetWitness primarily serves investigators who know how to use its tools. Its output, however, can be used to refine the automation of security information analysis, not just in correlating security events, but in mining security data to discover concerns that might otherwise go unnoticed.

Ultimately, this trend may lead us in directions foreseen by those who see the rise of data science as a new profession. What security becomes in the future may well depend on the expertise being built today by those directly engaged not only in the work of intelligence, but in the still-emerging discipline of investigation based primarily on data analysis. Together, this fusion of expertise may well define the data-driven security strategies and tactics that will make a difference in what security intelligence becomes tomorrow.›

Scott Crawford is managing research director of security and risk at Enterprise Management Associates, an IT industry analyst firm based in Boulder, Colorado. He is the former CISO of the Comprehensive Nuclear-Test-Ban Treaty Organization's International Data Centre in Vienna, Austria, and has over 20 years' experience as an IT security and operations professional in the private and public sectors, with organizations including the University Corporation for Atmospheric Research and Emerson. Send comments on this article to feedback@infosecuritymag.com.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

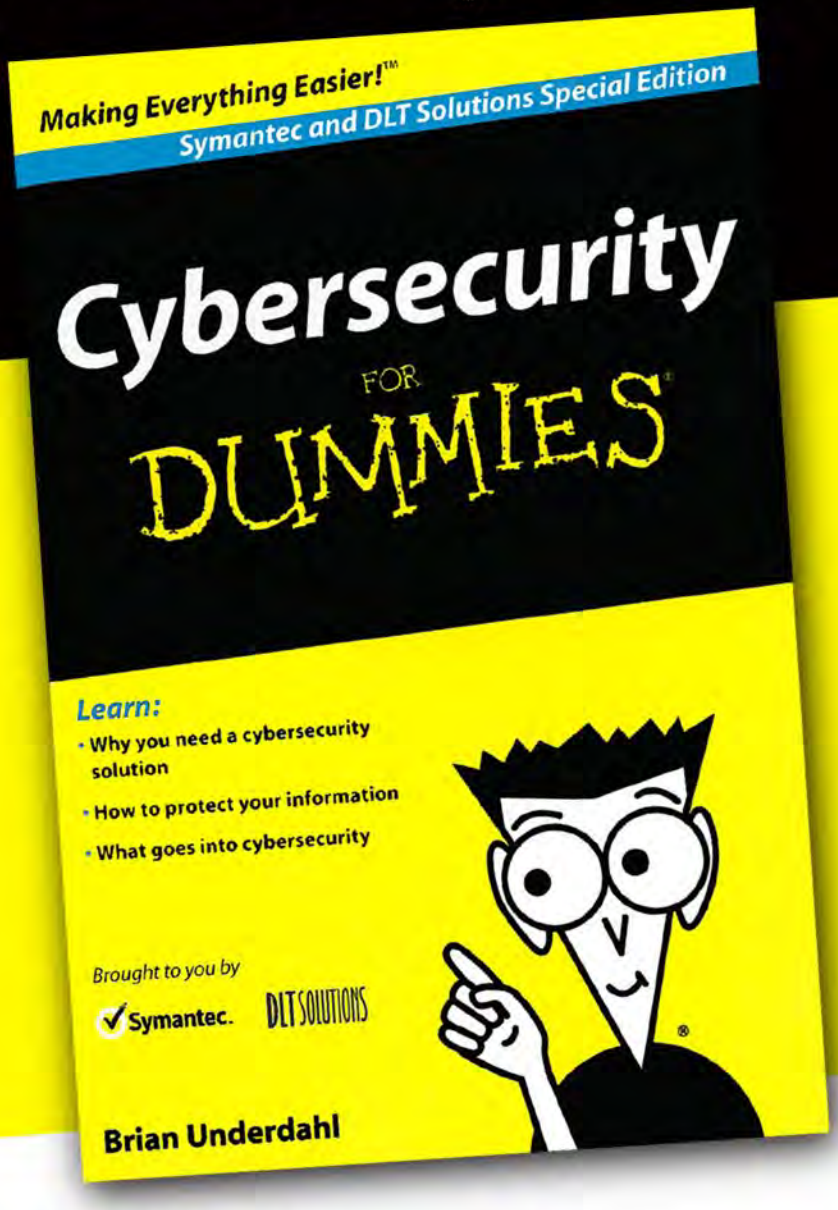
THREAT DEFENSE

INTELLIGENCE

CONSOLIDATION

SPONSOR RESOURCES

Protect Your Agency with Solid Cybersecurity Practices

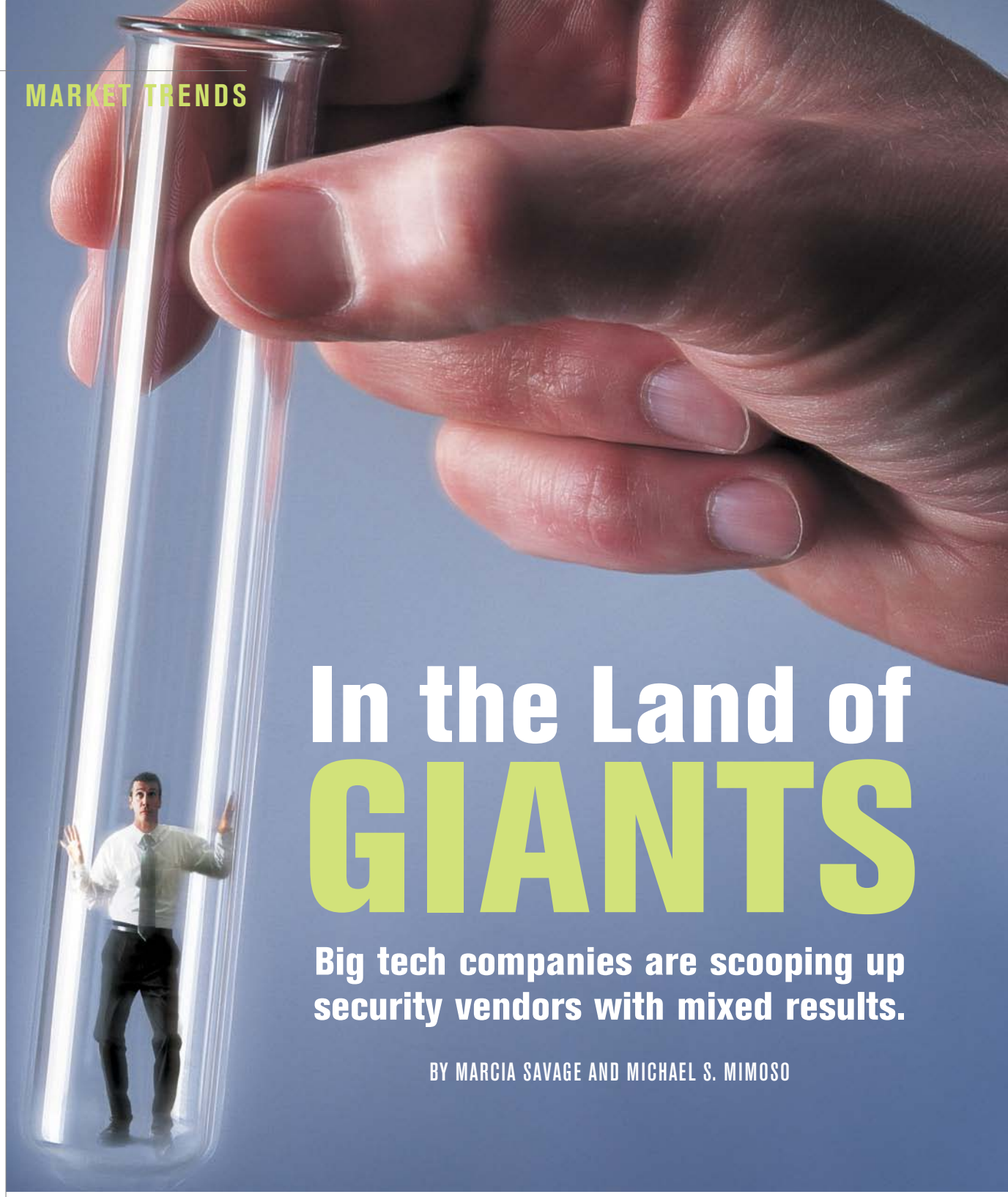


DLT SOLUTIONS

Symantec.™

www.dlt.com/cybersecurity-eDummies

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES



In the Land of GIANTS

Big tech companies are scooping up security vendors with mixed results.

BY MARCIA SAVAGE AND MICHAEL S. MIMOSO

IN THE MIDDLE of the last decade, SPI Dynamics was among the darlings of the security startup world. It had cool technology in a burgeoning segment of the security industry. The company's profile was growing from modest beginnings (16 people, including three co-founders and a handful of engineers in an office behind a strip club near Georgia Tech University) to eventually to more than 150.

Investors loved the little Web app security company that could. Four rounds of funding helped the company's engineers develop products such as Web app pen-testing

tool WebInspect, which were solving real-world security dilemmas. Revenue was doubling, literally, every quarter. The good times were rolling; the company still maintained that informal, startup feel too, and innovation remained the priority despite the increasing focus on business and shareholder satisfaction.

"We were going through growing pains adjusting to being a bigger company and culture; it was crazy during our peak," says Caleb Sima, one of the co-founders. Sima saw the handwriting on the wall; despite solid revenue, they needed more resources to hit their absolute peak and double, maybe quadruple, their business. "We had to decide: Stay small, or explode to a large company?"

"We were going through growing pains adjusting to being a bigger company and culture; it was crazy during our peak."

–CALEB SIMA, co-founder, SPI Dynamics

The "For Sale" sign may never have been formally hung on the door, but acquisition was inevitable. This was the hey-day of consolidation in the security industry. Not only were pure-play security companies scooping up standout security startups, but large tech companies were taking a shine to security. From 2005 to 2006, there were at least 19 security deals. SPI Dynamics, for instance, had Compuware, IBM, Hewlett Packard and numerous others knocking at its door. Google was looking for entry into security; Cisco, EMC and CA too.

Very few startups sell to have their stuff fall off the face of the planet. Developers and execs alike have an emotional attachment to the technology and the culture that helped build it. To have it spiral into the black hole of some corporate abyss was sacrilege. But Sima says that's what happened to SPI Dynamics for a period of time after it was acquired by HP in June 2007 for an undisclosed sum. Same story for Internet Security Systems (ISS) after IBM paid $1.3 billion for it in 2006. In fact, it became IT security's version of a drinking game to ask, "Whatever happened to ISS?"

Today, information security market consolidation continues at a rapid clip, with large infrastructure companies like IBM active players. While some say consolidation hurts innovation and customer service, others—particularly the IT giants—say in the long run, it promises better integration, more insight into an enterprise's security posture and, ultimately, improved risk management. Fewer point products for security managers to deal with, fewer headaches. But is that really the case? What have companies like IBM, HP and EMC done with their security acquisitions?

SPOTTY TRACK RECORD

So far, the record's been mixed, says Khalid Kark, vice president and research director at Forrester Research. A few years ago, Forrester predicted security would become a function of larger IT infrastructure management. "This was almost inevitable," Kark says.

"In terms of the technology, a lot of these capabilities [from the acquired companies] still aren't well integrated into the existing management or infrastructure capabilities that

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

these companies have," he says.

Oftentimes, acquisitions can hurt innovation and also translate to prices that are equal or even higher than before, leaving the end user with just one benefit: technology that has the backing of a big company. "IT buyers who want to play it safe and rely on a well-established, financially secure vendor are able to get that," Kark says.

Amrit Williams, a former Gartner analyst and CTO at configuration and vulnerability management company BigFix before IBM bought it last summer, says large IT vendors historically haven't done a good job at integrating security with their operational technologies, but are improving the way they handle security. In previous years, security at both IBM and HP was run by the brand, he says: "It was hard to find a single voice or strategy for security that spanned the brand and ensured the type of integration that would provide value to customers."

But IBM and HP have made organizational changes so security spans their brands and EMC made RSA its own division, Williams says: "You're seeing the large vendors recognizing the importance of security and not bury it in the brand."

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

BIG BLUE CHARGES INTO SECURITY

At IBM, security has become a big business that's core to the company's overarching "Smarter Planet" strategy of making systems more interconnected and intelligent, says Marc van Zadelhoff, director of strategy for IBM Security Solutions.

To that end, IBM launched its security solutions group in March 2010 to give customers one place to access all of its security products and services and has made 11 acquisitions in security since 2006. Those acquisitions are driven by the IBM security framework, which outlines key risk areas organizations face, van Zadelhoff says. For example, IBM's acquisition of BigFix was driven by the increased risk mobile devices and disparate endpoints pose to enterprises. "That company gets into a core part of our strategy, which is this whole interconnected planet and being able to manage the security on all these devices," he says.

"We're very good at that. We're good at retaining key people and integrating them into the IBM fabric."

–MARC VAN ZADELHOFF, director of strategy, IBM Security Solutions.

Since 2000, IBM has acquired more than 100 companies. "We're very good at that. We're good at retaining key people and integrating them into the IBM fabric," says van Zadelhoff, a former executive at Consul Risk Management, which was bought by IBM in 2007. He previously was on IBM's security M&A team. "I would argue that a bunch of other companies aren't as good at integration or the innovation side," he says.

He defends IBM's handling of its acquisition of ISS, which was initially put in IBM's

Corporate Quagmire

SPI Dynamics co-founder says acquisition by HP was anything but smooth.

SPI Dynamics' suitors began knocking, bearing figurative wheelbarrows filled with cash. Compuware called. IBM did too, and so did HP and a handful of others. Startups in security and other IT segments probably have a dedicated line for merger and acquisition calls, and SPI Dynamics was no different. But they weren't desperate either. They had a number and they were sticking to it. For three years, IBM tried its damndest to bring SPI's Web app security capabililties into the Big Blue family. The pitch, however, was always a lowball offer–as were most of the offers that Sima, CEO Brian Cohen and the rest of the management team fielded.

IBM tired of the chase and came to SPI with a take-it-or-leave-it offer. "They said, 'Here is our final offer, if you don't accept it, we're going to acquire different technology,'" Sima recalls. "We said 'No.' It was not close to what we wanted. We heard rumors after we turned them down that they were acquiring Watchfire, our major competitor."

And that's exactly what happened. And that's exactly the nudge HP needed to get serious about its offer to SPI.

"HP called and asked what it would take for us to acquire you and get it done within two months," Sima says. "HP made its offer, and we put down a minimum number. They came back, and said they would do this and this, and it was a good deal to us."

SPI had leverage in knowing IBM was ready to pluck Watchfire off the shelf and HP wanted to get into the same space before IBM. "They gave us our number, and we said 'fantastic.'" Ironically, IBM beat HP to the punch by one day, announcing its acquisition of Watchfire 24 hours before the SPI deal was made public on June 19, 2007. The horizon was now endless for SPI, which was promised access to HP's massive global sales force, channels and endless development dollars.

"We can literally change the way Web app testing QA is done; this was a big sell," Sima says. "This was very appealing to me. Every entrepreneur wants to change the world. That pitch was given to us as a nice goal for us."

What happened, however, was opposite. SPI was in a Bizarro mega-corporate world, cash flush sure, but suddenly without that startup feel. HP's Mercury Interactive group, acquired in July 2006, along with HP's corporate M&A team, managed the SPI Dynamics purchase. There was a 90-day integration deadline in place and things moved relatively quickly–and in a disturbing direction. Customer support was no longer within SPI's purview, instead it was moved into a call center system with tiered levels of support that were foreign to SPI customers used to the company's intimate relationships with customers. Sales and channel were also moved into corporate, and Sima says there was little motivation internally to sell SPI. HP corporate even bandied about changing product names, and made the team move from its prepaid office near Georgia Tech to an office an hour north in Atlanta.

"We fought to the death for all of this not to happen," Sima says. "But it was like a Prius and a Monster Truck; you're gonna get run over. There's nothing you can do."

Rather than focusing on their product as they had all those years, the SPI team was suddenly in the middle of corporate politics, evangelizing Web application security internally, scratching and clawing for development, sales and channel support. For a year, the little company that could was a cog inside the massive machine that was HP and was a poster child for the integration nightmare small startups can face when they're gobbled up by tech giants.

"It should have been expected, we should have had more experience and foresight because that's what large companies are wont to do," Sima says. ›

–MICHAEL S. MIMOSO

case study

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

WHO DOESN'T LIKE FAST AND EASY?

When it comes to **antivirus protection**, fast and easy is ***exactly*** what you should expect.

Finally, an antivirus solution that delivers the protection, speed, and performance you need. With VIPRE Antivirus Business, protecting against malware is now faster and easier than you ever thought possible.

We make your world simpler and your employees safer through:

- Faster real-time protection
- Unrivaled threat detection
- Easy deployment and management
- High-performance scanning and remediation

Fast and easy antivirus has never been so good. Test drive VIPRE today.

Find out more and download your FREE trial:

www.TestDriveVipre.com

$10 per seat limited time offer*

VIPRE® AntivirusBusiness

tel: 1 (888) 688-8457 | fax: 1 (727) 562-0101 | email: vipresales@gfi.com | **www.gfi.com**

*New licenses are available for $10/seat for VIPRE Business and $12/seat for VIPRE Business Premium, up to 500 seats, minimum 5 seats.
For customers with over 500 seats, please call for special pricing. Available for a limited time and subject to change without notice. Offer is valid in North America and Latin America only.

Copyright © 2011 GFI Software. All products and company names herein may be trademarks of their respective owners.

GFI®

services group—a move that critics say led to the ISS intrusion detection technology falling behind in the market. About a year ago, IBM moved the ISS products into its software group.

"There are phases in any company. We made the right move to keep the company together and allow the teams to collaborate until we had the integrations completed," van Zadelhoff says. IBM's acquisition of ISS opened up career paths for ISS service engineers, and also led to the development of IBM's virtual server security product, he adds. "An acquisition needs to be supported by a strong integration philosophy, then by the acquiring company's innovation that can drive and complement these technologies."

In February, IBM released Tivoli Endpoint Manager, what the company calls its "blue wash" of BigFix technology with new capabilities. van Zadelhoff says IBM is working to extend BigFix to mobile device management and showed off prototypes at the RSA Conference earlier this year. IBM also released a blue wash version of Guardium's database security technology, InfoSphere Guardium 8, about a year after it acquired Guardium.

Analytics is becoming increasingly important in enterprise security in order to detect security threats, he says. "Companies have bought every security product in the world and still don't know if they have an advanced persistent threat." IBM is integrating technology from many of its acquisitions, such as Guardium, Consul and data analytics company Cognos, with its own capabilities and producing prototypes of advanced analytics that can troll through terabytes of data to uncover threats.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

HP'S SECURITY PLAY

Like IBM, HP views security as key to its broader strategy. Last fall, HP unveiled its strategy for providing tools and services, including security, to help companies address the growing use of mobile and cloud computing technologies by enabling an "Instant-On Enterprise." The company's security acquisitions—including intrusion detection vendor TippingPoint, SIM supplier ArcSight and application security company Fortify Software—were intended to build security into the fabric of the network, reduce risks, and help customers detect threats early, says Rick Caccia, vice president of product marketing of HP ArcSight.

"We think if we tie all that together we have a strong ability to understand who's on the network, what applications are there, where vulnerabilities might exist, and monitor to reduce risk in the business."

–RICK CACCIA, vice president of product marketing, HP ArcSight.

HP is developing a security intelligence and risk management framework that integrates its acquired security technologies with some of its traditional capabilities in IT operations and applications management. "We think if we tie all that together we have a strong ability to

understand who's on the network, what applications are there, where vulnerabilities might exist, and monitor to reduce risk in the business," Caccia says.

Core to the framework is the ArcSight technology. Since HP acquired the SIM vendor last fall, it's been working to integrate the ArcSight log management product with its system management technology. That integration gives customers better context for network events, Caccia says.

HP also has been working to integrate the static code analysis capabilities it acquired when it bought Fortify Software last September with the dynamic testing capabilities from its SPI Dynamics deal. In April, the company released a hybrid analysis product, which Subbu Iyer, senior director of products and application lifecycle management at HP Software, describes as an "industry first." Fortify, like ArcSight, is run as a standalone business within HP. It's headed by former Fortify CEO John Jack, and combines the R&D teams of Fortify and SPI Dynamics.

Iyer says the rationale behind Mercury Interactive handling the SPI Dynamics deal was to add security to Mercury's application performance testing, but he adds that HP could have done some things differently with the acquisition.

"We learned a lesson. That's why we've been very intentional in the way we have worked with Fortify and ArcSight," he says. "We've not rushed to functionalize these organizations. We've made sure they run as independently as possible and sell to the core security buyer."

Caccia sees an opportunity to improve on enterprise security, where multiple point products are failing to catch intruders or malware slipping through the cracks.

"There are lots of security products [today]. They work well but are fairly narrowly focused," he says. "We think there's an opportunity to provide unification across those. We don't want to replace them, but we want to provide better insight and intelligence across them because customers demand it."

EMC BANKS AND BUILDS ON RSA

"We knew security was important to EMC. We didn't know what our approach would be."

–TOM HEISER, president, RSA, the security division of EMC

Tom Heiser led the team responsible for M&A at EMC before becoming president of the company's RSA security division. For a year leading up to the RSA acquisition in 2006, EMC embarked on a security strategy. "We knew security was important to EMC. We didn't know what our approach would be," he says. After quickly deciding against building its own security business, it looked to M&A and eventually RSA, which had the "critical mass" and technology strategy that fit with EMC's.

Since then, its layered in more security acquisitions to its RSA business, based on a strategy that looks at market dynamics, growth opportunities, and customer needs, says Ted Kamionek, vice president of business development at RSA who leads security M&A for EMC/RSA. EMC's purchase of GRC software vendor Archer Technologies last year and its

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Lumension®
IT Secured. Success Optimized.™

Gain control. Get the big picture.

Every computer is both a source of productivity & point of risk. Lumension® secures all endpoints against unwanted and malicious applications without affecting efficiency.

To gain control, you first need to see the big picture.
Download our FREE Application Scanner Today

lumension.com/gain-control

info@lumension.com
1.888.725.7828

No Small Feat

Integrating ISS into Big Blue was a complicated process, former ISS strategist says.

Internet Security Systems, like SPI Dynamics, fell off the radar of the security world for some time after it was acquired by IBM in 2006. ISS not only was an intrusion detection and prevention pioneer with its Proventia product line, but its X-Force research team was an all-star team of white hat hackers at the forefront of analysis on worm and malware outbreaks. Unlike SPI Dynamics, ISS was a sizable corporate entity with 1,400 employees and a global workforce at the time IBM plunked down more than $1 billion for it in October '06.

"It started to get to the point where it made a lot of sense," says Dan Ingevaldson, former ISS technology strategist and director of professional services of the acquisition. "We were the biggest independent security company out there aside from McAfee. There was a lot of activity, nothing specific to IBM at first. But it was apparent that something was going to happen."

ISS was the focal point of the corporate security research world for some time and featured some heavy hitters, such as founder Chris Klaus, president Tom Noonan, CTO Chris Rouland and a bevy of talented engineers and hackers who built up the formidable Proventia and RealSecure product lines and helped detect and combat such threats as the SQL Slammer worm. IBM certainly had the assets to scoop up a shiny target such as ISS. The opportunity was there to bolster its fledgling security services offerings with the ISS portfolio. IBM was sorely lacking intrusion prevention and vulnerability assessment technology, and ISS being a leader was a natural fit. IBM filled gaping holes with the ISS buy, and had close to a complete security story to tell alongside its Tivoli identity management play.

Integrating the company inside IBM, however, was a significant undertaking. IBM serviced thousands of accounts, and had a shiny new security bobble to offer its customers. IBM also serviced companies globally, from enterprises to the midmarket, something that would expand ISS' almost exclusive enterprise foothold.

"Promises were made, but it's always harder than advertised," Ingevaldson says. "But I think they were largely successful in integrating ISS. When IBM acquired us, they had 300,000 employees. The natural thing to assume is that you won't have access to (resources) like before, and be buried and hard to find. It's a logical concern. But IBM is better at buying companies than anyone else."

Ingevaldson says IBM worked hard to identify potential organizational issues that might arise as employees left and were replaced. "They managed our existing business and kept our account teams together," he says. "IBM was not interested in reeling us in."

IBM continues to invest and offer the Proventia product lines, including its Network Scanner, SiteProtector and endpoint threat mitigation offerings. These were the backbones of a company on the front lines of security research not so long ago.

"At the time, we were just focused on creating cool technology customers wanted," Ingevaldson says. "We were seen as the new guard in dealing with the threats of the day. We really were positioned in the trenches with customers, on the phone 24/7. Our teams were in the offices on weekends, nights, whenever, reverse-engineering systems and putting capabilities into our products. Our account managers were constantly relying on the X-Force to position themselves as a knowledgeable partner, a trusted advisor for the industry. We had a good technical relationship with customers. Our customers had an intellectual interest in the problems of the day; it wasn't about checking boxes for PCI that's driving buying decisions today." ›

–MICHAEL S. MIMOSO

case study

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

Each day the news reveals another **hacked company**. Working and engaging online exposes enterprises and individuals to successive waves of hacks, cracks, spam, scams, and other digital exploits. Learn how to **stop the hacks** and protect your company and users in TeleSign's white paper:

The Fraud Epidemic

Fight fraud with phone-based authentication and verification

Download the White Paper Now:
"The Fraud Epidemic: Fighting fraud with phone-based authentication and verification"

TeleSign

April acquisition of network monitoring company NetWitness are deals that allow EMC to grow while providing integrated technologies that give customers better visibility into their infrastructure, he says.

Startups have a hard time scaling and reaching a lot of customers, Heiser says. "Companies don't want to buy point products, they want to buy solutions. …When we acquire companies, customer expectations go up substantially in terms of customer responsiveness, service, product quality and functions down the road," he says. "Many customers rely on us to buy these smaller companies to make sure they're hardened for mission-critical applications."

In the case of Archer, EMC/RSA capitalized on the company's loyal user community. Archer gave its customers the ability to design and prioritize features and functions through online forums and an annual user conference, and RSA has invested heavily in sustaining that Archer user community, Kamionek says.

"Now we're taking that community and rolling it across other products to leverage that powerful input. …That's an example of how we've taken what worked for a small company and brought that into RSA to help accelerate and prioritize innovation here," he says.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

FALLOUT ON THE FRONTLINES

That rosy picture is at odds with the more common scenario in the wake of an acquisition, in which the customer experience changes and not usually in a good way. "The simplest way to think about it is products disappearing without a good migration strategy. Post sales degradation. All the usual things when you have a company that's too big and distracted," says Andrew Braunberg, research director at Current Analysis.

Shopping for Security

Some of the security acquisitions made by big tech companies in the past few years.

2006 IBM acquires Internet Security Systems. EMC acquires RSA and SIM vendor Network Intelligence.

2007 HP buys SPI Dynamics. IBM acquires compliance and security audit software vendor Consul Risk Management and Watchfire, a Web application vulnerability assessment company. Google buys email security vendor Postini and antimalware and browser security supplier Green Border.

2009 IBM buys database security vendor Guardium and Ounce Labs, a provider of source code testing tools.

2010 HP acquires Fortify Software and ArcSight. EMC buys Archer Technologies. IBM buys BigFix.

2011 EMC buys NetWitness.

m&a

While Williams says acquisitions—when handled strategically rather than just filling a portfolio gap—can sustain innovation, René Bonvanie, vice president of worldwide marketing at Palo Alto Networks, an independent provider of enterprise firewalls, says innovation is always hampered in large companies. "The challenge for large companies is to stay focused on something as specific as security," he says.

Innovative or not, though, it's easier to sell security to executive management when it comes from a large company rather than a niche player, says Brian Engle, director of information security at Temple-Inland, a manufacturing firm based in Austin, Texas. If a company is already a customer of a large IT provider, it's easier to approach the C-suite with a security component from that provider. "It's like adding a line item rather than formulating something from scratch," he says. "It doesn't mean what you'll get will be the best thing there is, but sometimes you have to make that sacrifice."

If the promised technology integration from consolidation actually happened, security would improve by no longer being bolted on after the fact, Engle says. "As long as we have this separate security industry, we're going to have difficulties in providing top-to-bottom security," he says. "If consolidation was truly working, we'd be better for it, but we aren't getting everything we need from the integration."

However, Chris Ipsen, CISO for the state of Nevada, is wary of the consolidation trend leading to what he calls a monoculture. "As soon as we become overly reliant on one way of thinking, we become less secure," he says.

Going forward, a layered approach to security that mixes new ideas and established technologies will be critical for resilience, he says. "It requires us to go back to basics in terms of rigorous controls, separation of duties, layers of defense and enforceable policies. All those things that represent good hygiene in a network become more important with consolidation."

"What gets people into trouble is when it's difficult to switch, especially if the technology has a lot of integration including customization specific for your organization."

–AMRIT WILLIAMS, former Gartner analyst and BigFix CTO

Every vendor can be acquired and companies should be prepared, Williams says. He advises getting contractual commitments to roadmap items that are critical to your company, especially during license renegotiations. Security managers also should look at the vendor's competition for potential alternatives.

"What gets people into trouble is when it's difficult to switch, especially if the technology has a lot of integration including customization specific for your organization," Williams says. "That's a situation where you want to be candid with the acquiring company and say, 'I need to make sure commitments that were made to me by the company you acquired are kept.'"

Forrester's Kark cautions against getting locked into long-term commitments as a vendor gets acquired. "It might sound easy to lock into three years and get a great deal, but there's a reasonable amount of uncertainty with this transition, so you want to make sure you're not in a situation where you signed a three-year contract and after a year, 40 percent of the people

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

you dealt with are gone," he says.

For Sima and SPI, the experience of being swallowed by a big company was rough, but he sees improvement. Since then, HP has continued to invest in security and has had integration success stories folding in Fortify and ArcSight, he says.

"Looking back, it was unfortunate we were the example. We fought hard inside of HP when they were doing the acquisition of Fortify to make sure the same things didn't happen to them that happened to SPI," Sima says. "They learned a lot of lessons. Things are much better. SPI has a foothold working inside HP now. It took a long time and a huge amount of mistakes." ›

Marcia Savage is editor of Information Security. *Michael S. Mimoso is editorial director of the Security Media Group at TechTarget. Send comments on this article to feedback@infosecuritymag.com.*

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREERS

THREAT DEFENSE

INTELLIGENCE

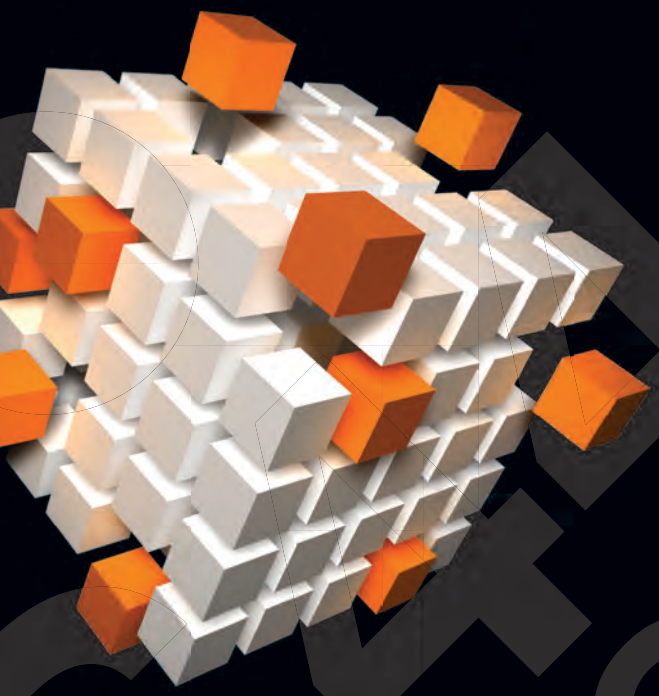
CONSOLIDATION

SPONSOR RESOURCES

Source 44 Consulting

www.source44.net

Network and Data Security Services



Threat Mitigation

Network & Security Technologies

Security Assessments

Network Audit / Security Architecture Review
Vulnerability Assessments
Penetration Tests
Incident Response
Forensic Readiness Assessments

Support Services

Professional Services & Full Support
Security Infrastructure Management

Digital Forensics

Investigations
Data Recovery
e-Discovery
Litigation Support

IT Security Training

Training Courses

PROTECTING YOUR MOST VALUABLE ASSETS

Contact us for a **FREE**

1-hour consultation

info@source44.net

905.237.4576

For your SPECIAL OFFER please scan the QR Code

www.source44.net

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
CAREERS
THREAT DEFENSE
INTELLIGENCE
CONSOLIDATION
SPONSOR RESOURCES

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Michael S. Mimoso

SENIOR SITE EDITOR Eric Parizo

EDITOR Marcia Savage

MANAGING EDITOR Kara Gattine

NEWS DIRECTOR Robert Westervelt

SITE EDITOR Jane Wright

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Maggie Sullivan

ASSISTANT EDITOR Greg Smith

UK BUREAU CHIEF Ron Condon

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum,
Lee Kushner, Mike Murray

CONTRIBUTING EDITORS
Michael Cobb, Philip Cox,
Scott Crawford, Peter Giannoulis,
Ernest N. "Ernie" Hayden,
Robbie Higgins, Jennifer Jabbusch,
David Jacobs, Diana Kelley, Nick Lewis,
Richard E. Mackey Jr., Kevin McDonald,
Sandra Kay Miller, Ed Moyle, Lisa Phifer,
Ashley Podhradsky, Ben Rothke,
Anand Sastry, Dave Shackleford,
Joel Snyder, Lenny Zeltser

USER ADVISORY BOARD
Phil Agcaoili, Cox Communications
Richard Bejtlich, GE
Seth Bromberger,
Energy Sector Consortium
Chris Ipsen, State of Nevada
Diana Kelley, Security Curve
Nick Lewis, Saint Louis University
Rich Mogull, Securosis
Craig Shumard, CIGNA CISO Retired
Marc Sokol, Guardian Life
Gene Spafford, Purdue University
Tony Spinelli, Equifax

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS
Amy Cleary

VICE PRESIDENT/GROUP PUBLISHER Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT Susan Shaver

DIRECTOR OF MARKETING Kathleen Quinn

SALES DIRECTOR Tom Click

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER Elizabeth Lareau

PRODUCT MANAGEMENT & MARKETING
Kim Dugdale, Andrew McHugh,
Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com
Patrick Eichmann
peichmann@techtarget.com
Sean Flynn seflynn@techtarget.com
Jennifer Gebbie
jgebbie@techtarget.com
Jaime Glynn jglynn@techtarget.com
Leah Paikin lpaikin@techtarget.com
Jeff Tonello jtonello@techtarget.com
Vanessa Tonello
vtonello@techtarget.com
George Whetstone
gwhetstone@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

COMING IN SEPTEMBER

Readers' Choice Awards

Information Security and SearchSecurity.com have surveyed our readers to determine the best products for protecting data and networks. Readers only vote on products they've deployed, including authentication devices, intrusion prevention and vulnerability management systems. They rate them in a number of areas such as ease of installation and vendor support. Our survey findings can help you plan and simplify your information security product buying decisions.

Vulnerability Management

With targeted attacks and zero-day vulnerabilities shrinking the window of time between vulnerability disclosure and exploit availability, it's becoming more incumbent on security managers to understand the assets in their IT environment and the patch levels of those machines. In this feature, you'll gain insight on how to improve your asset discovery processes, as well as how to determine the patch level of the machines in your environment. You'll learn how to determine what the best patch management option is for you; whether Microsoft's update tools and services are sufficient, or when it's time for a third-party solution.

Don't miss our monthly columns and commentary.

TechTarget
Where Serious Technology Buyers Decide

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.

All rights reserved. Entire contents, Copyright © 2011 TechTarget. No part of this publication may be transmitted or reproduced in any form, or by any means without permission in writing from the publisher, TechTarget or INFORMATION SECURITY.

what drives *your* approach to IT security?

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

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

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

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

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

See ad page 10

- Implementing the 20 Critical Controls with Security Information and Event Management (SIEM) Systems
- Continuous, Proactive FISMA Compliance

See ad page 27

- Blue Coat Mid-Year Security Report 2011
- Corporate Web Security - Market Quadrant 2011
- Magic Quadrant for Secure Web Gateway

See ad page 7

- Network Protection and the Influx of Threats
- Network Vulnerability Management

See ad page 31

- Optimizing Vulnerability Management

See ad page 38

- Cybersecurity for Dummies: eBook Download
- Symantec Endpoint Protection 12.1 Webcast

See ad page 43

- Small Business Endpoint Protection Performance Benchmarks
- 5 Security Mistakes SMBs Make and How to Correct Them

See ad pages 14, 18

- **Enhance Your Credibility and Influence - Attain an ISACA Certification**

See ad page 46

- **Think Your Anti-Virus Software Is Working? Think Again**
- **Unruly USB: Devices Expose Networks to Malware**

See ad page 4

- **First Half 2011 Security Labs Report**
- **Simplifying Email Compliance, Policy, and Management**

See ad page 48

- **The Fraud Epidemic: Fight fraud with phone-based authentication and verification**
- **Stop spammers, scammers, frasters and phishers with phone-based authentication and verification**