INFORMATION SECURITY®

OCTOBER 2012 • VOLUME 14 • NO. 8

READERS' CHOICE AWARDS 2012

YOUR PICKS FOR CREAM OF THE CROP

PLUS:

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

FROM OUR SPONSORS

SOPHOS

Q1 Labs®
Total Security Intelligence | An IBM Company

CDW

Symantec.

McAfee®

CORE SECURITY

WEBROOT
SecureAnywhere

Copper River
Information Technology

Ping
Identity®

Java Trouble

Attackers are zeroing in on Java but disabling the popular programming language is problematic in the enterprise. BY MARCIA SAVAGE

VULNERABILITY MANAGEMENT is a time consuming, complex process and the recent onslaught of attacks on Java hasn't made it any easier. To recap: In August, security researchers reported that attackers were actively exploiting zero-day vulnerabilities in Java. Oracle—not always the quickest on the draw when it comes to fixing flaws—actually released a patch pretty fast only to have security researchers uncover holes in it.

All the Java security problems—and a growing track record of security snafus with the popular programming language—led to calls from a number of security experts to disable Java. Tod Beardsley, Metasploit engineering manager at Rapid7, says that's simply sound advice.

"For the Java browser plug-ins, users should disable Java. Unlike Flash, HTML5 or even PDF, it's not ubiquitous technology on the Web...Disabling unnecessary functionality is always good advice—doing so reduces your attack surface," he says.

In the enterprise, however, shutting off Java is easier said than done. A number of common business applications such as conferencing and collaboration rely on the Java runtime, and some data center applications run on Java, says Scott Crawford, managing research director at industry analyst firm Enterprise Management Associates.

"Pulling the plug on Java in a business is not going to be a slam dunk by any means," he says.

With Java interfaces developed for a wide array of enterprise systems, the popular platform-independent programming language "tends to be used everywhere," says Paul Hill, senior consultant at SystemExperts.

And its pervasive nature is what's making Java attractive to attackers. That wasn't the case a few years ago. Wolfgang Kandek, CTO of Qualys, says Web browsers used to be a prime target for attackers until browser makers developed better security defenses. Attackers shifted their attention to other software such as Flash and PDF, but now Adobe has put a lot of resources into hardening its products. Now it appears Java is in the crosshairs.

So what's a company to do? While organizations can apply extensive protections in the data center, it's more problematic on the endpoints, Crawford says. Kandek acknowledges that controlling use of Java in the enterprise is complicated. Organizations need to take stock of applications they use that require Java and find workarounds or use whitelisting, he says.

Microsoft Internet Explorer provides the ability for companies to whitelist by implementing the security zone mechanism, Kandek says. He recommends banning Java in the Internet Zone and only allowing websites where it's needed in the Trusted Sites Zone. Beardsley says Firefox's NoScript plug-in is a fairly easy solution that IT can either train users on or deploy for them.

Kandek says a workaround for some applications that use Java might be a native client. For example, if a user has the WebEx client, then the conferencing program won't need Java on the user's machine to run.

SystemsExperts' Hill recommends that organizations take a defense-in-depth approach by keeping Java patched, maintaining updated antivirus, and using network security devices such as IDS/IPS and SIEM. Beardsley says proxy and egress IPS devices could help a network manager who can't control all desktops directly by blocking Java applets over HTTP. "With a combination of desktop configuration and network management, I don't think it's unreasonable to pursue a block-and-whitelist strategy," he says.

However, companies are finding other ways to avoid Java. Hill sees many organizations that are phasing out dependencies on Java applets. "Now people are developing rich Web applications using Ajax techniques so Java is on the server and not executing on the client," he says.

And of course, Oracle could do a better job of correcting Java vulnerabilities. ■

MARCIA SAVAGE *is editor of* Information Security *magazine. Send comments on this column to feedback@infosecuritymaga.com.*

Big Benefits, Big Risks

Big data offers business benefits and improved security but also comes with risks. BY STEVE DURBIN

THE VOLUME OF DATA that businesses collect is exploding exponentially. This includes financial transactions, location-based data, customer interactions, the supply chain, as well as data produced by employees, contractors, partners and suppliers using social networking sites, intranets, extranets, and corporate wikis. In fact, sources such as mobile and online transactions, social media traffic and GPS coordinates now generate more than 2.5 quintillion bytes of "big data" every day, according to IBM.

The commercial impacts of big data analytics—the practice of performing increasingly sophisticated analysis on massive amounts of data, predominantly unstructured—have the potential to generate significant productivity growth for a number of vertical industry sectors. In short, big data analytics presents an opportunity to create unprecedented business advantage and better service delivery. At the same time, it promises benefits for information security while also presenting increased risks.

Senior executives and boards the world over are now faced with extremely large amounts of data, and this can be viewed as both a burden and an opportunity for their business. Research suggests that companies capturing and using big data and business analytics to guide their decision-making are more productive and have higher returns on equity than competitors that do not.

Research conducted by the McKinsey Global Institute points to big data having the capability to create substantial value and commercial impact. McKinsey found the potential of a 60 percent increase in retailers' operating margins, 0.7

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

percent increase in productivity in U.S. health care, all translating into a $300 billion value per year. In addition, there's the potential increase in demand for deep analytical talent positions, estimated between 140,000 and 190,000.

Pressure is mounting on businesses to embrace big data because of the enormous insights and competitive advantage it can provide. Computers are increasingly crunching numbers to find answers previously thought indecipherable. This is introducing new problems. For example, poor quality information or untested models can send businesses off course.

As big data changes the game for businesses, the security risks have become much greater. From an information security standpoint, the key issues surrounding big data—both pro and con—tend to fall into the following five buckets:

Data breaches: With more transactions, conversations, interactions and data now online, the incentives for cybercriminals have never been better. Companies have more to worry about than the one-off data breaches or hacker attack stories that make headlines; breaches involving big data could have far-reaching consequences and mean reputational damage, legal liability and even financial ruin. Cyber resilience and preparedness strategies are crucial for big data. However, using big data security analytics could also help identify cybercriminals or zero day attacks.

Data in the cloud: The pressure for businesses to quickly adopt and implement new technologies such as cloud services, often to support big data's challenging storage and processing needs, comes with unforeseen risks and consequences. Big data in the cloud is a highly attractive target for harvesting data and places more demand on businesses to get their secure cloud sourcing strategy right. Furthermore, importing data into a big data store in the cloud can result in the removal of permissions or confidentiality restrictions on the original data.

Consumerization: Together with the growth of big data is the proliferation of new mobile devices used to gather, store, access and transfer data. The challenge for businesses is in managing and securing personal devices brought into the workplace by employees and balancing the need for security with productivity. Businesses should enforce employee acceptable usage policies and continue to manage mobile devices in line with their established security policy.

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

Businesses should also consider how they might use big data analytics tools to identify any misuse or unusual access to systems through remote login, mobile or other personal devices.

Interconnected supply chains: Organizations are part of often complex, global and interdependent supply chains, which can be their weakest link. There is a key role for information security in coordinating the contracting and provisioning of business relationships, including outsourcers, offshorers and supply chain and cloud providers. Big data analytics has the potential to create an overarching view of an organization's supply chain security by analyzing high-risk suppliers' data and comparing suppliers across different dimensions of information security risk.

Privacy: As huge amounts of data are generated, stored and analyzed, privacy concerns are becoming an even larger issue. Businesses need to start planning for new data protection requirements as soon as possible while monitoring for further legislative and regulatory developments in other jurisdictions where your customers are based. Also, they should consider using big data analytics tools to identify where private personal information is being stored and how it is protected.

Big data analytics have the potential to reduce the growing number of cyber security risks and increase business agility. Businesses eager to adopt these new technologies for business benefit will be well advised to set out clear good practice guidelines for big data. They need to understand the legal and other restrictions that may apply to data they collect, store and use across multiple jurisdictions. Companies should also implement privacy best practices, designing them into the analytics programs they are using for big data, and build in transparency and accountability, all the while considering the impact of big data usage on people, processes and technology. ■

STEVE DURBIN *is global vice president of the Information Security Forum, an independent, nonprofit association. His main areas of focus include the emerging security threat landscape, cybersecurity, consumerization, outsourced cloud security, third-party management and social media across both the corporate and personal environments. He was senior vice president at Gartner, where he was the global head of Gartner's consultancy business. Send comments on this column to* feedback@infosecuritymag.com.

The Rise of Cross-Platform Malware

Security researchers are finding more malware that attacks multiple operating systems. BY MORIAH SARGENT

C**ONVENTIONAL WISDOM** about malware targets is evolving with the emergence of cross-platform malware into the cybercriminal's arsenal.

Over the last year, cross-platform malware, sometimes referred to as multi-platform, has grabbed attention in the industry. This particular type of malware can infect different versions of operating systems and machines and is becoming more popular in the world of cybercrime. Microsoft's Windows platform has been the biggest target for malware creators, but experts say rising market shares of other operating systems has made the cross-platform approach more attractive and logical. Experts say enterprise security teams must address this malware trend on all platforms they use, whether they are desktop computers or mobile devices.

In April, the Flashback Trojan targeted computers running Mac and Windows by exploiting a security vulnerability in Java. Microsoft published a blog post in July about how it has become beneficial for cybercriminals to attack multiple operating systems through one Trojan. Also in July, security companies detected the Crisis Trojan, which targets Mac OS X systems. Symantec researchers then discovered that the Windows version of Crisis is able to spread to VMware virtual machines and Windows Mobile devices. There have been other cross-platform malware attacks, and experts say there will be more. Now that cybercriminals have figured out a way to infect multiple operating systems, Chester Wisniewski, senior security advisor at Sophos, says they will recycle cross-platform malware, as they have done with other attack templates.

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

Experts said the cross-platform approach is dangerous partly because of attitudes toward security. Wisniewski says that because most Windows users have experienced a large volume of potential threats, they know they need to protect their systems. This is not true for users of other operating systems.

“People have been lulled into thinking they don’t need protection for Macs” and other systems, he says.

“It doesn’t matter what brand you’re on,” Wisniewski says. He recalled an instance when a customer received a suspicious link and didn’t click on it on the computer; instead, the customer used an iPad to check the link. Experts, including Wisniewski, say this type of thinking is dangerous.

"People have been lulled into thinking they don't need protection for Macs."

—Chester Wisniewski, senior security advisor, Sophos

The division of IT teams is another concern. Enterprises often have two teams, a network group and an endpoint group. Wisniewski says these groups need to coordinate and share information so security breaches don’t slip through unnoticed. An issue observed on the network may be brushed aside, he says, but when connected to issues on the machines could reveal a more serious problem.

The same security mechanisms and fixes may not work across all platforms, Cameron Camp, security researcher at ESET says and an official strategy would need to reflect this. Wisniewski believes operating systems should be monitored similarly.

“As much as possible, the operating systems should be treated the same,” he said. “Make sure Mac and Linux are being monitored in the same ways as Windows.” ■

MORIAH SARGENT *is an editorial assistant for SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.*

End the Bolt-on Era

Unless security is viewed as a core function instead of an add-on, we're bound to repeat the mistakes of the past.

BY DOUG JACOBSON AND JULIE A. RURSCH

A**REN'T YOU TIRED** of seeing the same headlines recycled in newsprint and magazines and blasting over the airwaves, cable news channels, and Internet? Headlines like "The U.S. is Losing the Information War," "Cyber Space is the Next Battleground" and "Money Motivates Today's Hacks"? Articles with these kinds of headlines lay out the plight of the American public, business and government when encountering new vulnerabilities, exploits, credit card frauds, and/or viruses. But are the threats and vulnerabilities truly new? Or are we seeing an ongoing recurrence of the same type of problems because we are not properly addressing security and incorporating long-term solutions into the fabric of our country? Are we, in fact, doomed to repeat history because we do not recognize the pattern and work to avoid the mistakes of the past by continuing to follow the same information security trend?

2013 will mark the 25th anniversary of the Morris worm being released into the Internet and some would argue we are no more secure today than we were then. If we think of the Morris worm signaling the dawn of the cybersecurity industry, then we must depict ourselves at high noon in the O.K. Corral of the cybersecurity shootout. We continue to see advances in technology solutions and escalations of technological exploits of these solutions. As IT professionals implement the newest piece of hardware or software to protect us from the latest threat, cybercriminals are already working to find shortcomings in these new systems that will allow access to our personal data, credit cards, bank accounts, critical infrastructure, and/or disrupt our daily lives. While advances in technology have plugged holes or slowed the bleeding, they also have caused the criminals to become ever more savvy in their approach and execution.

So, why do we continue to struggle with problems that are similar to the ones we observed nearly a quarter of a century ago? In the simplest of terms, we treat security as a bolt-on feature rather than a core product or function. Because cybersecurity is a top priority, we have appointed committees, added meetings to our days, required cybersecurity certification standards, and sent people to training. Yet security is still often viewed as a separate issue to be addressed. Rarely do we approach a design or system problem with the intent to include security from the start.

It has also become obvious that technology alone will not fix security; people are the real way to make inroads in protecting cyberspace. Consequently, over the past 20 years there has been an increased focus on security education. But have we really educated anyone in cybersecurity and are we making any reduction in cybersecurity attacks on our nation? In government and business we have mandatory security training sessions or put up posters around the office talking about how to be more secure. Some organizations go as far to offer advanced security training for their staff. In academia, where we train young computer engineers and computer scientists, we treat security as a separate topic, offering separate majors in information assurance and network security. When security is covered as part of a course on operating systems or programming it's treated as an add-on topic. It's covered at the end of the semester, if time permits.

> It has become obvious that technology alone will not fix security; people are the real way to make inroads into protecting cyberspace.

In general, we don't educate our computer engineers and computer scientists to take a holistic approach to security and when these individuals enter the workforce, security is treated with the same separatist approach. Worse yet, computer engineers and computer scientists aren't the only ones who either ignore or segment security into its own little world. All disciplines suffer from not including security as a core product, but instead bolt it on at the end of the course or product.

This leaves those at management decision-making levels just as ignorant of security concerns as those who work for them. So, when we will finally see security as central to all disciplines and avoid the pitfalls of repeating history?

In the coming months, this column will be devoted to examining the difficulties in cybersecurity education at all levels, from formal university education and specialized training and certificates to security literacy for the masses. We hope to spur a national dialogue among the stakeholders in cybersecurity, including universities, training organizations, corporations, and government, and encourage an evolution so security is no longer an afterthought. ■

DOUG JACOBSON *is a professor in the department of electrical and computer engineering at Iowa State University and director of the Information Assurance Center, which was one of the original seven National Security Agency-certified centers of academic excellence in information assurance education.*

JULIE A. RURSCH *is a lecturer in the department of electrical and computer engineering at Iowa State University and director of the Iowa State University Information Systems Security Laboratory, which provides security training, testing, and outreach to support business and industry. Send comments on this column to feedback@infosecuritymag.com*

secureworld expo

NATIONAL SECURITY LEADERSHIP, LOCAL ISSUES, NETWORKING WITH RESULTS, ACCESSIBLE EDUCATION

ST. LOUIS – September 11-12, 2012
BAY AREA – September 19-20, 2012
DETROIT – October 3-4, 2012
DALLAS – October 10-11, 2012
SEATTLE – October 30-31, 2012
BOSTON – March 27-28, 2013
ATLANTA – April 2-3, 2013
HOUSTON – May 1-2, 2013
PHILADELPHIA – May 22-23, 2013
CHARLOTTE – May 29-30, 2013

To receive $50 off the $265 Two-Day Conference Pass or $100 off the $695 SecureWorld Plus. Enter code **SWCTT12.**

Register now for a conference near you!
WWW.SECUREWORLDPOST.COM

SecureWorld Features Nationally Recognized Security Leaders Including:

2012 SECUREWORLD EXPO THEME:

DECRYPTING the MAYAN CODE

Join SecureWorld as we take you on an adventure four hundred years in the making: "Decrypting of the Mayan Code".

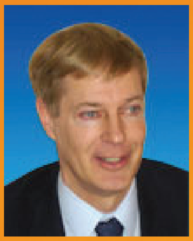
secureworld post

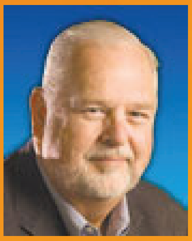
Stay informed on the latest IT security news.

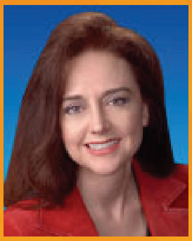
WEB CONFERENCES

Timely Topics, Leading Experts

Visit **WWW.SECUREWORLDPOST.COM!** Register for an event, learn more about the theme, web conferences, or SecureWorld Post.


Scott Borg
Director and Chief Economist,
U.S. Cyber Consequences Unit


Dave Cullinane
Former, Chief Information
Security Officer, eBay


Rebecca Herold
Privacy Professor, CEO,
Rebecca Herold & Associates

Gene Kim
Founder: Tripwire, Author

Bob Russo
General Manager,
PCI SSC

Jason Witty
Chief Information Security Officer
US Bank

"In the eight years that I've participated, what amazes me is that SecureWorld Expo is that local event that I get to see and catch up with almost every regional security team once a year. It is an affordable conference for the whole team and provides quality content."

–Phil Agcaoli, CISO, Cox Communications

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

2012 READERS' CHOICE AWARDS

For the seventh consecutive year, *Information Security* readers voted to determine the best security products. More than 2,100 readers participated this year, rating products in 14 different categories.

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

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

APPLICATION SECURITY AWARD

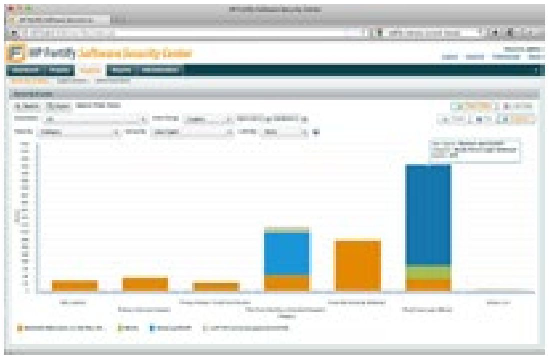
Static and dynamic vulnerability scanners, and other source code analysis products and services used during development.

GOLD

HP Fortify Real-Time Analyzer

Readers awarded the gold medal to HP Fortify Real-Time Analyzer. The tool received high scores across all criteria, making it the clear winner in the application security category. Readers particularly liked the product's ease of installation, configuration and administration.

They also liked the analyzer's effectiveness in preventing known attacks and/or vulnerabilities as well as the frequency of updates to detect new exploits and/or vulnerabilities. HP Fortify Real-Time Analyzer also ranked higher than any of its competitors for integration with other security reporting and remediation tools.



HP Fortify Real-Time Analyzer is intended to protect applications from vulnerabilities that were not fixed during development or QA testing. The software is designed to reduce risks in deployed Java and .NET applications by automatically blocking attacks for common vulnerabilities from inside the application. The user can configure the software to respond with various risk mitigation techniques when an attack is detected; for example, by blocking the user or alerting an administrator. The analyzer can also automatically monitor applications and collect data on attacks.

According to HP, the software requires no customization, training, coding or modeling.

SILVER	eEye Digital Security Retina Web Security Scanner
BRONZE	HP Fortify Static Code Analyzer

EXPERT'S MARKET REFLECTION

> *"The application security market has a lot of growth ahead. End users still struggle with implementing security measures across the software lifecycle, and there is still ample room for innovation. We should continue to see healthy growth in the foreseeable future."*
>
> —CHENXI WANG, VICE PRESIDENT AND PRINCIPAL ANALYST, FORRESTER

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

AUTHENTICATION AWARD

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

GOLD

RSA SecurID

For the third year in a row, SecurID, the two-factor authentication product from RSA, the Security Division of EMC, has dominated the authentication category of our annual Readers' Choice Awards. Despite a breach of RSA's systems in March 2011, SecurID has not only held its customers' loyalty, but also steadily remains the choice two-factor authentication solution among readers.

Readers gave SecurID high scores across the board. the product ranked especially high in the areas of ease of use, vendor service and support, and security of credentials against cracking and discovery. Customers had overall positive feedback for the product, calling it reliable and powerful, with most championing its trustworthy security and longevity as the features they appreciate the most.

RSA offers SecurID hardware authenticators as well as software-based two-factor authentication tokens for smartphones, tablets, and PCs. With more and more employees going mobile and bringing in their own devices to work, it's becoming increasingly important to implement a reliable two-factor authentication solution to ensure the security of sensitive company data. For many readers, SecurID has proven to be that secure solution.

SILVER	Symantec VeriSign Authentication Services
BRONZE	Entrust IdentityGuard

EXPERT'S MARKET REFLECTION

> *"Extended-enterprise imperatives are strongly shaping enterprises' authentication strategies. They need to enable strong authentication for cloud- and mobile-based transactions, and use risk-based authentication as a fraud detection booster shot."*
>
> —EVE MALER, PRINCIPAL ANALYST, FORRESTER

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

EMAIL SECURITY AWARD

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

GOLD

Cisco Systems IronPort Email Security Appliances

A regular contender in our Readers' Choice awards, Cisco Systems IronPort Email Security Appliances are the recipient of the gold medal in email security. Promoted from last year's bronze, readers recognized the email security appliances for their ability to detect and block spam, phishing attempts, viruses and spyware in messaging traffic.

The appliances scored well across the board, but readers particularly liked their ease of use, integration with existing messaging applications, and the quality of vendor service and support.

The email security appliances also received rave reviews by readers who provided write-in commentary. The appliances were described as "good," "easy to use," and "works exactly as described."

Cisco Systems IronPort Email Security Appliances are designed to protect organizations of all sizes against messaging threats. The appliances feature spam protection, digital rights management, archiving, virus defense and email encryption, and tracking and reporting tools. Cisco IronPort also offers DomainKeys signing, directory harvest attack prevention and protection against bounced-message attacks. Different filtering policies can be set for different groups within the organization and real-time reporting allows administrators to modify policies if the network is under attack. Cisco offers its IronPort Email Security technology on cloud-based, hybrid or managed models.

SILVER	Google Message Security
BRONZE	Barracuda Spam and Virus Firewall

EXPERT'S MARKET REFLECTION

"Spam and virus filtering is at an acceptable rate across most solutions. More advanced solutions are focused on filtering irritating bulk marketing emails, dangerous targeted spear phishing threats, advanced data loss prevention and encryption capabilities."

—PETER FIRSTBROOK, VICE PRESIDENT, GARTNER

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

ENDPOINT SECURITY AWARD

Business-grade desktop and server antimalware and endpoint protection suites that include antivirus and antispyware, using signature-, behavior- and anomaly-based detection, whitelisting, host-based intrusion prevention and client firewalls.

GOLD

ESET NOD32 Antivirus 4 Business Edition

It was a close race for gold in the endpoint security category, but ESET NOD32 Antivirus 4 Business Edition pulled ahead with notably higher scores for frequency and speed of signature updates, ability to detect and block unknown malware and zero-day exploits, and return on investment. This is the second year in a row that ESET has received gold in our Readers' Choice awards, proving that the Slovakian firm is a serious endpoint/antimalware contender.

ESET NOD32 Antivirus 4 Business Edition offers protection from malware, email and Internet traffic scanning, and proactive threat detection. ESET differentiates itself with software that runs fast while consuming fewer system resources than other antimalware/endpoint products. Readers backed this up with comments such as "bloat free and easy on system resources," "small footprint," and "runs invisibly."

Readers also pointed out that the software runs well on Macs. According to ESET, the Mac OS X edition of ESET NOD32 is the only anti-malware solution ICSA Labs certified for both Mac and Windows. The software provides protection for cross-platform threats to help prevent Macs from carrying malware that could be passed to other OSes.

SILVER	Kaspersky Lab Kaspersky Open Space Security
BRONZE	Sophos Endpoint Protection

EXPERT'S MARKET REFLECTION

"The endpoint protection market is in transition. Signature-based protection mechanisms alone no longer offer sufficient protection. Organizations want converged platforms that offer multiple styles of protection within a single policy management framework, including firewalls, antimalware and encryption as well as application control and device control."

—NEIL MACDONALD, VICE PRESIDENT AND DISTINGUISHED ANALYST, GARTNER

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

ENTERPRISE FIREWALLS AWARD

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

GOLD

Cisco Systems Adaptive Security Appliances

The more things change, the more they stay the same. Multifunction network security appliances like next-generation firewalls and intrusion prevention systems have dramatically altered the face of the enterprise network firewall product landscape, but one of the biggest vendors in the market keeps winning the hearts and minds of enterprise customers.

Using phrases like "a best-of-breed product," "easily configurable," and "rock solid," respondents to *Information Security* magazine and SearchSecurity.com's 2012 Readers' Choice survey voted Cisco Systems Adaptive Security Appliances 5500 Series as this year's gold winner in the enterprise firewalls category.

The ASA series is a broad line of multifunction network security devices, providing not only comprehensive firewall and IPS capabilities, but also VPN/remote access, unified communications security, content filtering, antimalware, URL filtering and more. Cisco offers models like the ASA 5505 for SMB customers, while the new 40 Gbps top-of-the-line 5585-X is designed for data centers and large enterprises.

Readers' Choice survey respondents gave the ASA series its best marks for its ability to block intrusions, attacks and other unauthorized network traffic, as well as vendor service and support.

SILVER	Barracuda NG Firewall
BRONZE	Juniper ISG Series

EXPERT'S MARKET REFLECTION

"Rumors about the death of the firewall are greatly exaggerated, despite debates to the contrary. Interest in next-generation firewall technology has revived the market and helped to propel startup Palo Alto Networks' successful IPO."

—PAULA MUSICH, PRINCIPAL ANALYST FOR ENTERPRISE SECURITY, CURRENT ANALYSIS.

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

IDENTITY AND ACCESS MANAGEMENT

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

GOLD

IBM Security Identity Manager

Earning high marks across the board, IBM Security Identity Manager was the clear gold medal winner in the identity and access management category. Readers particularly liked its scalability, end-user transparency/ease of use, and vendor service and support. IBM Security Identity Manager also received high scores for integration and compatibility with associated products, directories and other information stores. Readers described the product as "robust," "dependable," "trust worthy," and "well worth the investment."

IBM Security Identity Manager helps automate the creation, modification and termination of user privileges throughout the user lifecycle. It offers request-based provisioning of requesting and approving user access to roles, accounts or fine-grained access entitlements like shared folders. The product's customizable user interface is tailored to specific types of users, such as auditors, managers and administrators. And self-service interfaces allow users to reset passwords, perform password synchronization and modify personal information without having to call the help desk.

Access recertification capabilities check whether user access is still valid and allows for automated access remediation. Managers can recertify a user's roles, accounts and groups in bulk. The software also provides auditing and reporting mechanisms.

SILVER	Microsoft Forefront Identity Manager
BRONZE	Oracle Identity Management Suite

EXPERT'S MARKET REFLECTION

> *"The IAM market is shifting to a service-based orientation (i.e. cloud), addressing scale and user experience concerns, and preparing for wider mobile client use (i.e. tablets, mobile phones."*
>
> —EARL PERKINS, RESEARCH VICE PRESIDENT, GARTNER

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

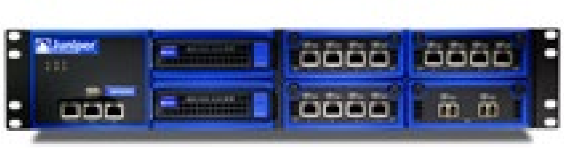
INTRUSION DETECTION/PREVENTION AWARD

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

GOLD

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances

After a two-year absence, Juniper Networks reappears in the intrusion detection/prevention category with a gold medal for its IDP Series Intrusion Detection and Prevention Appliances. The networking vendor previously earned a gold medal for the same product in 2009. This time around, readers gave the IDP Series high ratings for its ability to effectively and accurately detect, prevent and/or block attacks and suspicious activity, the frequency of signature updates and response to new threats, its reporting and alerting functionality, and vendor service and support.



The IDP Series uses stateful signature detection as well as protocol and traffic anomaly detection to help protect networks against both known and unknown threats. According to the vendor, the appliance's application-layer intelligence helps reduce false positives and increase throughput. The appliance examines traffic in the context of an application, enabling it to identify the signature pattern at the location where an attack can occur.

The product also provides application awareness/identification, application policy enforcement and application volume tracking, which allows administrators to observe how much bandwidth an application is using.

SILVER	Sourcefire IPS
BRONZE	McAfee Network Security Platform

EXPERT'S MARKET REFLECTION

"Application visibility and control has blurred the lines between the IPS and firewall appliance markets. While large enterprises will likely continue to use both next generation firewalls and IPSes, medium-sized enterprises are more likely to select one or the other."

—PAULA MUSICH, PRINCIPAL ANALYST, CURRENT ANALYSIS

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

NETWORK ACCESS CONTROL AWARD

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

GOLD

Symantec Network Access Control

Symantec Network Access Control garnered the gold, scoring high in a number of categories but most notably in logging and reporting. Readers also liked Symantec Network Access Control's enforcement options, and vendor service and support.

Symantec Network Access Control is designed to control access to corporate networks through integration with existing network infrastructures. The product can discover and evaluate endpoint compliance status, provision the appropriate network access, provide remediation and monitor endpoints for changes. Endpoints can connect to the network using a Symantec Network Access Control Enforcer that integrates directly into the network, a host-only option requiring no network integration or an agent that is integrated into the Web application environment.

The product's architecture consists of three core components: policy management, endpoint evaluation and network enforcement. According to Symantec, these work together as a single product to provide end-to-end network access control. However, Symantec Network Access Control also integrates with other NAC technologies, including those from and Microsoft.

Readers praised Symantec Network Access Control in general, commenting that it's easy to use and scalable.

SILVER	Cisco NAC Appliance
BRONZE	Juniper Networks Unified Access Control

EXPERT'S MARKET REFLECTION

> *"Many organizations are still thinking about NAC, but vendors are making it easy by offering a wide variety of products and strategies to make integration as simple as possible—for a complex technology."*
>
> —JOEL SNYDER, SENIOR PARTNER, OPUS ONE

REMOTE ACCESS AWARD

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

GOLD

Juniper Networks SA Series SSL VPN Appliances

Readers awarded Juniper Networks SA Series SSL VPN Appliances with the gold medal for remote access, praising the products' capabilities in the areas of authentication support, ease of installation and configuration, and breadth of applications and devices covered. Readers also highlighted the support they received from the vendor, as well as their return on investment.

The series includes the SA2500 for small to medium-size businesses, SA4500 for midsize to large organizations, and SA6500 for large enterprises and service providers. A single SA6500 device can support up to 10,000 concurrent users with the ability to scale much higher with two- and four-unit clusters. The virtual appliance in the SA series runs on VMware software. Designed primarily for service providers, it can scale to an unlimited number of customers.

The SA Series SSL VPN Appliances provide secure remote access without requiring client software and feature cross-platform support to allow users to access corporate resources from any type of device.   Host Checker capabilities scan endpoint to verify compliance with security policies, and single sign-on capabilities reduce the need for end users to maintain multiple sets of credentials.

SILVER	Citrix Access Gateway
BRONZE	Check Point Remote Access VPN Software Blade

EXPERT'S MARKET REFLECTION

> *"As business computing shifts from notebook to tablet, so must secure remote access. Increasingly, solutions protect data between consumer-grade devices and public/private cloud applications, independent of location, ownership, or connectivity."*
>
> —LISA PHIFER, PRESIDENT, CORE COMPETENCE

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

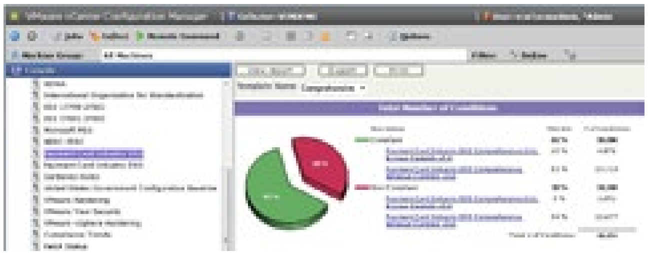
POLICY AND RISK MANGEMENT AWARD

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

GOLD

VMWare VCenter Compliance and Configuration Manager

Readers resoundingly awarded VMWare VCenter Compliance and Configuration Manager with the gold in the policy and risk management category. While the product scored highest in vendor service and support, it also earned noteworthy scores for ease of installation, configuration and administration, and granular and flexible policy management definition capabilities.



VMWare VCenter Compliance and Configuration Manager is designed to automate configuration management across virtual and physical servers, workstations and desktops. It automates tasks such as configuration data collection, compliance assessment, patch management and OS provisioning. It can also be used to continuously audit the configurations of VMware infrastructure as well as Windows, Linux and Unix OSes. Compliance templates can be used to assess configuration compliance with industry and regulatory mandates such as SOX, HIPAA and PCI-DSS. The product is also designed to manage clouds built on VMware technology, as it features integration with vSphere and hardening capabilities for VMware infrastructure.

Readers were very complimentary of VMWare VCenter Compliance and Configuration Manager, frequently describing the product as good, excellent and solid.

SILVER	RSA Archer eGRC
BRONZE	Fortinet FortiManager

EXPERT'S MARKET REFLECTION

> *"Vendors offering policy and risk management capabilities are incredibly diverse, with some focusing on documentation, others focusing on automating processes. Most organizations see value in getting a better handle on their compliance and risk posture, but with so many choices they have to carefully discern what exactly these vendors have to offer."*
>
> —CHRISTOPHER MCCLEAN, SENIOR ANALYST, FORRESTER RESEARCH

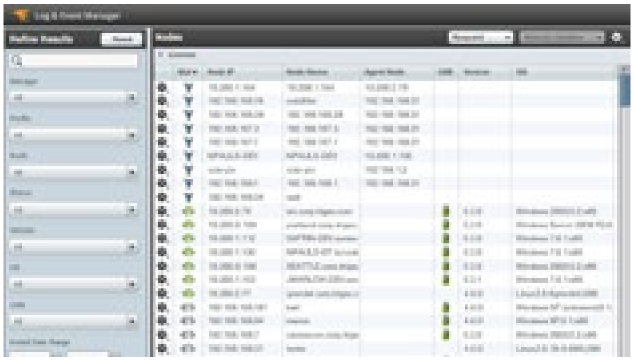
SIEM AWARD

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

GOLD

SolarWinds Log & Event Manager

The acquisition of TriGeo in 2011 added an award-winning security management tool to SolarWinds' product portfolio. The Austin-based technology vendor makes its gold-winning debut in the Readers' Choice awards with accolades for Log and Event Manager. SolarWinds Log and Event Manager offers log collection, analysis and real-time correlation in a virtual appliance.



According to SolarWinds, Log and Event Manager offers advanced search capabilities over other SIEMs. Users can search a range of data using visual search tools, including word clouds, tree maps, bubble charts and histograms. By searching a range of data, from high-level events to detailed log data, users can quickly perform forensic analysis. The security software also features USB Defender Technology, which is designed to eliminate endpoint data loss and protect sensitive data.

Readers particularly liked Log and Event Manager's integration and compatibility with existing systems, devices and applications. The software also received high scores for ease of installation, configuration and administration, vendor service and support, and return on investment.

SILVER	McAfee Security and Information Event Management
BRONZE	HP ArcSight Enterprise Security Manager (ESM)

EXPERT'S MARKET REFLECTION

"Early log management products evolved into SIEM as their scope was extended to include a broader range of events across a wide range of IT devices from the data center, across the network to the desktop. More recently some of the vendors have souped up their products to enable them to act on data in real time."

—BOB TARZEY, ANALYST AND DIRECTOR, QUOCIRCA

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

VULNERABILITY MANAGEMENT AWARD

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

GOLD

XQualysGuard Vulnerability Management

QualysGuard Vulnerability Management (VM) took home the gold this year, winning high marks from readers for effectively and accurately identifying vulnerabilities in a timely manner. The cloud-based service also scored high marks for its scalability and vendor service and support. Readers also liked its comprehensive and flexible reports and reported that it was easy to install, configure and administer.

QualysGuard VM provides automated network auditing and vulnerability management, including network discovery and mapping, asset prioritization, vulnerability assessment reporting and remediation tracking. Since it is a Security as a Service, the product doesn't require deployment or management of infrastructure. It's no surprise then that readers reported that QualysGuard VM was easy to set up and manage.

The service features full remediation workflow capabilities with trouble tickets. QualysGuard VM's vulnerability reports that readers praised include data on severity levels, estimates on remediation times, impact on business and trend analysis. The service aims to reduce the time that security managers have to spend tracking down and fixing network vulnerabilities, giving them more time to work on other projects.

SILVER	Tenable Nessus
BRONZE	Symantec Altiris Client Management Suite

EXPERT'S MARKET REFLECTION

> *"Vulnerability management has evolved, but at the same time, the playing field has shifted. Assessment and remediation have improved, but attackers have also turned to potentially richer opportunities such as Web and Java applications"*
>
> —SCOTT CRAWFORD, MANAGING RESEARCH DIRECTOR, ENTERPRISE MANAGEMENT ASSOCIATES

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

WEB APPLICATION FIREWALLS AWARD

Standalone Web application firewalls and WAFs that are part of application acceleration/delivery systems.

GOLD

FortiWeb-400C

Fortinet's FortiWeb-400C won the gold in the Web Application firewall category, scoring especially high marks for its ability to block intrusions, attacks and unauthorized network traffic. Readers also rated the product highly in a number of other areas, including its application-layer controls, central management capabilities and logging, monitoring and reporting features. Overall, they feel they're getting their money's worth.

FortiWeb-400C offers flexible deployment options and is well suited for midsized organizations. It secures Web applications and protects corporate assets by blocking threats such as XSS, SQL injection, buffer overflows and DoS attacks. The product includes active/passive high availability support to ensure critical applications remain available. A Web vulnerability scanner complements the WAF capability by providing analysis of existing application vulnerabilities. User activity is automatically profiled to create a baseline of permissible activity.

FortiWeb-400C is part of Fortinet FortiWeb WAF product line, which includes appliances for large enterprises and service providers as well as virtual appliances for implementing Web security within a virtual environment.

SILVER	F5 Networks BIG-IP Application Security Manager
BRONZE	Barracuda Web Application Firewall

EXPERT'S MARKET REFLECTION

"Enterprises are leveraging Web application firewalls investments as a cost effective means to secure Web applications. Many security experts still say 'WAFs are useless,' but we find that—when properly deployed—they raise the bar for security."

—ADRIAN LANE, CTO AND SECURITY STRATEGIST, SECUROSIS

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

WEB SECURITY AWARD

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

GOLD

Check Point Web Security Software Blade

Check Point Web Security Software Blade earned the gold medal among readers this year. Check Point says its software blades are designed to be treated like a building block, enabling companies to quickly configure security controls on any gateway or management system. *Information Security* magazine readers gave the Web Security Software Blade high marks for detecting and blocking malware and for its customizable reporting and alerting features.

The software blade is designed to pre-empt the execution of malicious code and protect against buffer overflow attacks. Check Point says its Malicious Code Protector detects malicious executable code within Web communications by identifying not only its existence within a data stream but its potential for malicious behavior. It operates at the kernel level providing protection that does not compromise performance, and can be configured to provide different levels of control for various Web applications and servers.

The software blade also contains Advanced Streaming Inspection, a Check Point kernel-based technology that processes the overall context of communication. This technology can make real-time security decisions based on session and application information and protects Web communication even when it spans multiple TCP segments.

SILVER	Symantec MessageLabs Web URL Filtering Service
BRONZE	Websense Web Security Gateway

EXPERT'S MARKET REFLECTION

> *"Web security products provide lots of opportunities for protection. The market itself is fairly robust. Clients are under attack so there's some obvious need for security given the ambiguity going on at the client level with BYOD, performance issues and so on."*

—PETE LINDSTROM, RESEARCH DIRECTOR AT SPIRE SECURITY.

THE CRUCIAL COMBINATION

A successful threat management program requires effective processes, layered technology and user education.

By Diana Kelley

STAYING SAFE ON THE ROAD involves a number of controls, rules and responses. The car itself is equipped with safety features like anti-lock brakes, blind-spot warnings, seatbelts and airbags. Rules of the road include speed limits and seatbelt laws and drivers themselves must pass tests to prove they are able to operate their cars properly. No one would dream of suggesting that just because a car has airbags that it could be operated safely by a driver with no license going at 100 mph.

But what appears ludicrous in the realm of safe driving can be tempting in the hectic world of IT. Can't a company just buy a single unified threat management (UTM) product with the best, most advanced threat detection technology and guarantee the organization is protected? Unfortunately, the answer is "no." Just like driving a car requires multiple parts working together, "driving" a corporate IT network safely requires a blend of the traditional triumvirate: people, process and technology.

So what goes into creating a successful threat management program? Read on to hear what security professionals have to say about best practices for enterprise threat prevention.

ENTERPRISE THREAT PREVENTION: BUILDING A FOUNDATION

In 2012, threat prevention has evolved into an integral part of the corporate IT risk and security management program. Most companies have moved beyond stand-alone monthly malware updates and quarterly device scans to an integrated set of technologies that are fully incorporated with the security or network operations center.

Security pros have various ways of defining threat management at their organizations. Waqas Akkawi, director of information security at global moving and relocation services provider SIRVA, defines threat management at a high level as the "real-time monitoring and reporting of user activities—and having the ability to effectively query the environment, report on capabilities and send timely alerts" when someone or something accesses protected data. Leo Walsh, IT risk compliance subject matter expert for Memphis, Tenn.-based bank holding company First Horizon National Corporation, notes that a formal definition is less important to threat prevention and management than having an IT risk operations team of people who are entirely focused on IT risk operations and strict change control processes. However, he and other security pros agree on this: The core purpose of threat management is to protect business data and assets from internal and external attacks.

Though the specific answers to what a threat is and how to manage it will vary from organization to organization, there are some high-level definitions that apply to all (or almost all) threat management programs. Taking a moment to review these is worthwhile because it helps a company to level set the business needs for the threat management program and ensure the right systems are selected. Since threats can come from multiple sources and at many points

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

in the IT architecture, understanding where and how the attacks originate will enable a company to create a more robust plan for mitigating and preventing those attacks.

Threat management begins with threat identification. In SP800-30, NIST defines a threat as "the potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." A threat source can be human, such as a hacker or disgruntled internal employee; natural, such as tsunamis or tornadoes; or environmental, such as a power outage or water damage from leaky pipes. So a comprehensive threat management program must take into account all the sources. NIST also recommends defining the threat motivations of each threat source and the potential actions of these sources. For example:

- **Threat source**: Disgruntled employee
- **Motivation**: Damage company reputation
- **Action**: Logic bomb that defaces website in publicly embarrassing manner

NIST also recommends defining the threat motivations of each threat source and the potential actions of these sources.

But formal threat definitions aren't for everyone. The First Horizon IT Risk Operations Team focuses on trying to keep the company safe, Walsh says, "There are so many ways unauthorized access can happen—an effective approach is to look at what needs to be protected, assess whether or not it has been protected and then monitor the asset continuously to see whether or not it has been accessed," he adds.

As Philip Keibler, director of information security at athletic shoe and apparel retailer The Finish Line, puts it, successful threat management starts with a "need to understand the infrastructure and data, the ability to be proactive and to leverage protection components before the attacker does." Components of a robust threat management and prevention program are not restricted to technical controls like anti-malware, firewalls and IDSes, he added. While these technologies play an important and active role in threat management, they need to be part of a traditional process-technology-people triumvirate, and part of the bigger enterprise risk management picture.

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

THREAT MANAGEMENT PROCESS

How formal the threat prevention and management process is will vary by enterprise. Some companies have adopted formal standards like ISO 27001 and ISO 27005 guidelines that call for certain activities and artifacts to be completed as part of the security management process, and extend this approach into the threat management program. Keep in mind that although there are many excellent guidelines for risk management frameworks and processes, including OCTAVE, NIST Risk Management Framework, the FFIEC Examiner's Handbook on information security risk assessment, and ISO 27005, none of these are specific to threat management. And for smaller organizations, a process-heavy approach may not be feasible.

However, even in very informal environments, it's important to create and maintain at least high-level written policy and procedure documents because these will be required during most audit cycles. Without proper documentation, even the best threat management program on the planet could fail an audit simply because the written proof of the process wasn't available. "Any good security program will have policies as a foundation" and the ability to monitor conformance to those policies with proper tools and reporting, The Finish Line's Keibler says.

Without proper documentation, even the best threat management program on the planet could fail an audit.

Keeping the process proactive or "pre-attack" focused keeps a company ahead of the attacker. Keibler doesn't like playing catch-up and stays prepared using a process that includes scanning so vulnerabilities can be remediated before they're exploited. The Finish Line process also leverages data classification and network segmentation for "before-the-fact" protection and continuous deep-packet inspection monitoring is performed on all traffic going into and out of the segments. Policies and rules are set according to the sensitivity and classification of the asset or data, so data that requires tighter controls is placed in a higher trust zone than data at a lower sensitivity level.

At SIRVA, Akkawi says he's integrated threat management into the company's risk management program so IT security can "decrease the risk while ensuring the company continues to operate in a profitable manner." Akkawi's team uses data maps to follow where the data is going; threat and risk management questions are addressed during pre-deployment assessments of new applications. In collaboration with the business, IT answers questions such as, "What kind of data will the application handle?" "How will that data be protected?" and "Who will have access to that data?" IT then uses the answers to put proper controls in place and build alert and remediation procedures in the event of unauthorized access and to train technicians on response plans.

Weaving threat prevention management into change management is part of the process at First Horizon. Scans and penetration tests can be conducted before implementing a change in production. If a vulnerability in a particular device is discovered, the IT risk operations team contacts the business owner about it and is able to block the change until the vulnerability is fixed, Walsh says.

Though integration with other processes and systems, including change management, helps to ensure the threat management program runs in concert with the business, there is one area where it makes sense to have separation of duties: audit and compliance. Some change requests may come in as highly time sensitive for the business without giving the operations team enough time to evaluate the threat impacts. Having a separate team review and validate changes can prevent or limit unintended threat exposures because the separate audit or compliance team has more time to spend on threat impact analysis. If the compliance, audit or risk team determines the business need can be met with a more restrictive granular rule, then updates are implemented accordingly.

Remediation is an essential part of a successful threat management process, but one that organizations can neglect, according to Sadik Al-Abdulla, CDW security practice senior manager. "Many organizations have a blind spot, and until a serious breach occurs, the necessity of a response plan is rarely recognized," he says.

Key components of a remediation plan should include executive ownership, a communications plan, an escalation strategy and a law-enforcement contact strategy. "You don't want people that are under severe stress making decisions about what and how to communicate to customers," he says. The communication plan is often overlooked in IT, but as breaches and exposure scenarios continue to increase, there will be increasing pressure for companies to go on record when attacks occur. Having media-trained technologists who can convey

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

difficult technical concepts in a calm and understandable manner will go a long way towards preventing compounding data breach damage with a major PR gaffe.

A LAYERED APPROACH

Finding the right threat management technology fit is not as simple as buying a high-powered UTM and putting it between the organization's internal network and the Internet. There are no one-size-fits-all answers, or as SIRVA's Akkawi puts it, "there is no magic solution." The most effective threat management solutions use layered technology approaches, both architecturally and technically to detect, alert and respond. "Bluntly, it's 'defense in depth.' This is the same drum that the security industry has been banging since inception, but the evolution of more and more sophisticated threats is reproving that it is absolutely essential," says CDW's Al-Abdulla.

Technologies in use at companies as part of their threat management program include (but are not limited to):

- Firewalls/next-generation firewalls;
- Intrusion prevention/detection systems (IPS/IDS);
- UTMs (firewall, IPS, anti-malware, Web filtering, etc.);
- Endpoint protection suites (anti-malware, host firewalling, filtering);
- Message hygiene filters;
- Web hygiene filters;
- Network access control (NAC);
- Data loss prevention;
- Security information and event management (SIEM)/log aggregation;
- Network vulnerability scanners/Web app scanners;
- Policy and configuration management;
- Patching and software delivery;
- Web application firewalls/database monitors;
- Penetration testing tools; and
- Strong authentication.

Every threat management program doesn't need all of the above listed technologies and some use other technologies. The goal isn't to check off the most

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

"product" boxes, it is to reduce the threat surface and prevent attacks. So assess each technology for how well it will accomplish the business goal of threat detection and prevention.

For example, at SIRVA Akkawi has found the IPS component of the company's NAC system from ForeScout to be extremely helpful with threat management. The NAC product allows them to see who is connected, what their patch level is, and passes all the information into the LogRhythm SIEM so it can be reviewed and correlated, he says. SIRVA is also using the endpoint protection to detect issues like patch levels that are not up to data and devices that do not have antivirus installed. When the NAC detects non-compliant devices, it triggers alarms and the devices are taken off the network and put into a quarantined network segment until they can be remediated.

Assess each technology for how well it will accomplish the business goal of threat detection and prevention.

Finish Line, meanwhile, is exploring handling Web application threats using a combination of load balancing from F5 Networks and Web application scanning from WhiteHat. If the Web application scanner detects a vulnerability in an application, a virtual patch can be applied to the Web application firewall to mitigate exposure. Finish Line also uses endpoint security from Sophos as part of its threat management program.

Keibler notes the importance of bringing alerting and reporting information from tools like an endpoint suite to a single console like a SIEM (his company uses Envision's) so administrators can have visibility into potential threat activity across the network. Some of the things to look for in the SIEM that may indicate threat activity include number of failed logins, multiple login attempts from the same ID but different IP addresses, and creation of new, privileged accounts on servers or databases.

First Horizon's Walsh says a high noise ratio of "false positive correlations may be as much of a problem as no correlation at all." To keep focus on activities with a strong signal, the bank runs a variety of reports from its log aggregation tool that show the number of hits on a specific rule (e.g. access of DMZ via HTTPS) and uses a firewall policy management tool in order to find and assess issues. An anomaly like a huge spike in traffic is "relevant and throws an alert that really stands out" and is of high value to the security operations team, he says.

Another threat prevention technique in use at the bank is segmentation with VLANS. Rather than having to re-provision a switch, blades that are attached to the switches are tagged with the VLAN ID and separated from other servers on

Cloud and Managed Services

COMPANIES ARE INCORPORATING SOME CLOUD OR MANAGED SERVICES INTO THEIR THREAT MANAGEMENT PROGRAMS

A lot of threat management activity is still happening on-premise for larger companies with a few notable exceptions where they're comfortable using cloud services, such as message hygiene and vulnerability scanning.

"Today, most customers have a combination of on-premise and cloud," says Sadik Al-Abdulla, CDW security practice senior manager, explaining how customers are adopting cloud services for threat management. "Email security, for example, has been a highly effective cloud offering for many years and holds a disproportionate amount of the market compared to on-premise solutions. Web security, on the other hand, is almost exclusively on-premise."

He says the most common managed security service provider (MSSP) offering is usually a combination of firewalling and intrusion prevention, but that still has minimal market penetration, and even where used, there are other unmanaged threat prevention solutions in play. According to Al-Abdulla, the most frequently observed threat management architectures today are, in order of occurrence:

1. Mostly on-premise with cloud email security;
2. Fully on-premises;
3. MSSP firewall, other on-premise, and cloud email security; and
4. MSSP firewall, other on-premise. ■

—DIANA KELLEY

the VM switch. Inter-policy zone checks are completed by the firewalls when data crosses from one VLAN to another, providing a way to block unauthorized access and to prevent leaks of sensitive data out of protected zones.

THE HUMAN ELEMENT

As is almost always the case, the effectiveness of a technology tool is, in large part, directly related to the capability of the human interacting with that tool. For threat management, people skills come into play in a few main areas: The people running the threat management tools (admins and engineers), the people interacting with the systems that are under attack (users) and the customer service reps interacting with the users. Don't underestimate the importance of educating each one of these groups. Although it may be tempting to look for a tool that's so easy a child could use it, or to write off users as too "non techie" to help prevent attacks, resist the urge. People really are a full one third of the overall solution.

> As is almost always the case, the effectiveness of a technology tool is, in large part, directly related to the capability of the human interacting with the tool.

"If you are relying on the endpoint to stop all the malware, then it's too late. If the malware gets in, then something failed along the way," says Finish Line's Keibler. "A more effective approach is to start with employee awareness, partner with employees and help them to be another arm of the security program."

"Because there are some social engineering components in 70 to 80% of attacks, every employee has to be part of the program," he adds. At Finish Line, this extends to the help desk, where reps are trained to identify hallmarks of suspicious activity, like a substantial slowdown in device performance that may indicate presence of a bot, and flag this for investigation by the security team.

At First Horizon, data protection is a key driver for all of the IT risk staff. Walsh says he has a seasoned IT risk operations team that's "internally driven and knows the value to the business of keeping out of the Verizon DBIR." He adds, "If your employees are not motivated to keep corporate data safe, no framework or formula will do the trick."

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

The bank also engages people on the business side through regular communication with executives about risk, especially when there are real-world examples in the news with direct impact to the financial services industry. The bank also has a change advisory board that engages business owners in the threat management discussions when new services are brought on and changes are made, Walsh says. It also provides a corporate-wide information security awareness program that includes an annual test that all users must take.

Good user education can go a long way in helping your threat management program succeed. At SIRVA, employees are educated on data security and threat prevention—work that certainly paid off when an employee received a well-crafted spear phishing email that pretended to be a $1000 reward gift card from corporate HR. Rather than clicking on the gift link to collect the reward, the employee immediately reported the email to IT and Akkawi's team proceeded to investigate. A review of the log files and interviews with the employee showed that the spear phish had used social network data from outside the company and had not breached internal systems.

Though successful threat management programs have a number of moving parts and layers, they do not need to be overly complex or process-heavy. Advice from the trenches is to focus on what needs to be protected for the business. Know where the data and assets are and who (or what) has approved access to them. Use network segmentation to cordon off sensitive assets and prevent "panic" moments and audit documentation failures by setting down policy and procedures in writing.

Most companies find success using a layered set of solutions to identify and prevent attacks and maintain visibility into reporting from all of those solutions by rolling them up into a central stem console like a SIEM. And most importantly, don't forget about the people part of the program. Train engineers on data maps and flows and train users to know what's fishy or suspect and how to report suspicious activity to the correct parties. ■

DIANA KELLEY *is a partner with Amherst, N.H.-based consulting firm SecurityCurve. She has served as vice president and service director with research firm Burton Group. She has extensive experience creating secure network architectures and business solutions for large corporations and delivering strategic, competitive knowledge to security software vendors. Send comments on this article to feedback@infosecuritymag.com.*

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

INTENT TO SMEAR

With their goal of damaging corporate reputations, hacktivists aren't your average cybercriminals.

By Robert Westervelt

ASK ADAM O'DONNELL the difference between hacktivists today and those 15 years ago or more, and you won't get a simple answer. Technology has changed, social norms are different and political motivations are diverse.

"Back then there was less interest in the techniques of breaking into people's systems and exposing data that you see today," says O'Donnell, a noted antimalware expert and early hacker before he founded Immunet, which was acquired by security vendor Sourcefire. "Today it's like a decentralized religion; there's an ethos and anyone can label themselves of being part of it … and some groups are more bent in one direction or another, but they're all under

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

the same value system: sticking a finger in the eye of the man."

Indeed, today's hacktivists—notably those affiliated with Anonymous—are slightly different than the original hacktivists groups, such as Cult of the Dead Cow (cDc). Experts say the cDc was more centralized, granting membership to individuals based on their skills. The cDc's aim was mainly to defend human rights and freedom of expression and later to get organizations to find and repair serious vulnerabilities. Members of cDc created a number of hacking tools beginning in the early 1990s from Back Orifice, a rootkit program designed for the purpose of exposing Windows flaws. A later creation called Goolag automated hacking queries via Google to make it easier to find serious website vulnerabilities. Now, hacktivists use a variety of automated tools, many shared by financially motivated cybercriminals, to detect website vulnerabilities and carry out distributed denial-of-service (DDoS) attacks. Unlike a cybercriminal whose intent is solely on making money, the ultimate goal of the modern hacktivist is to sully the reputation of a company for one cause or another, O'Donnell said.

> "Some groups are more bent in one direction or another but they're all under the same value system: sticking a finger in the eye of the man."
>
> *—Adam O'Donnell, antimalware expert*

"It's trying to show up someone up in the face of public opinion," O'Donnell says. "You may lose some data but then you will also have to deal with the seven-day news cycle. Therefore the impact is going to involve public relations more than if a breach was done by a cybercriminal that didn't say anything publicly about it."

Clearly, today's hacktivists with their assorted political and social purposes pose a different breed of attacker than the average cybercriminal. Security experts say hacktivists have caused widespread damage to the infrastructure and reputation of organizations they target, making it critical that companies have a well-organized response plan in place.

MAJOR BREACH FACTOR

Hacktivists had a tremendous impact on data breaches in 2011, according to

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

the 2012 Verizon Data Breach Investigations Report, accounting for two-thirds of all the stolen records documented by the Verizon team. Most of the victims of the attacks were large businesses, says Bryan Sartin, vice president of the Verizon RISK Team and co-author of the report. The relative impact is far less if you remove the largest companies from the DBIR, Sartin says. About 96 percent of organizations analyzed by Verizon were attacked by cybercriminals motivated by financial and personal gain.

Verizon has identified two basic hacktivist types: Individuals who attempt to bring down or deface a website and individuals who pull off far more complex attacks using sophisticated tools. "It is surprising to see how far we've seen some hacktivists go to cover their tracks, sometimes successfully penetrating a network again and again," Sartin says.

Fifty-eight percent of all breached organizations knew in advance that they were going to be attacked, Verizon found. Often hacktivists leave broadly worded warning messages in a forum, on a website or a social network, such as Twitter, Sartin says. In almost every one of the cases, a DDoS attack was used as a diversionary tactic.

Anonymous and its associated group Lulzsec have gotten the most notoriety for recent hacktivism. The group doesn't have a known leader. Anyone with a computer can affiliate him or herself as an Anonymous hacktivist, says Toralv Dirro, McAfee Labs' EMEA security strategist.

Anonymous had its roots in the Antisec movement in the early 2000s. Some experts claim that Anonymous began on the Internet forum 4chan where a group of anonymous posters decided to use their power to protest the lack of black characters on Habbo Hotel, a virtual social network. Although its goals have been vague – the group has targeted pedophiles and railed against Scientology – it also has branched out into libertarian ideals, Dirro says. Its primary activity seems to be to respond to any attempt to regulate the Internet, he says.

The group's actions have caused widespread damage. Members of LulzSec are responsible for hacking into Sony Pictures in 2011, compromising user accounts and forcing Sony to halt its gaming platform until it could contain the breach. The group's members also gained access into the network of HBGary Federal, stealing research and email, including those of its co-founder and noted malware expert, Greg Hoglund. At least 65,000 email messages were posted The Pirate Bay file sharing service.

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

DDOS: THE WEAPON OF CHOICE

Verizon's Sartin and other security experts agree that hacktivists typically carry out DDoS attacks to either disrupt a website's operation or to obscure a far more nefarious attack. While the IT security team deals with the flood of malicious traffic, other hacktivists are busy trying to gain access to another part of the network in an attempt to steal data. Jeff Lyon, president of Los Angeles-based DDoS mitigation firm Black Lotus, says hacktivists typically use fairly standard DDoS attacks using the popular open source Low Orbit Ion Cannon tool. Lyon says the power of social networks has helped groups with similar political views to use their power collectively to bring down websites.

"If you are making a statement against a company or an organization, you can use a medium like Twitter or other social media to generate opinions and attack a target as a collective," Lyon says. "Anyone can launch a low-orbit ion cannon attack and it's difficult for law enforcement to track down individuals."

Verizon's Sartin and other security experts agree that hacktivists typically carry out DDoS attacks to either disrupt a website's operation or to obscure a far more nefarious attack.

In 2009, hacktivists are believed to be responsible for disrupting some U.S. and South Korean government websites, taking them offline for hours. The attackers also brought down the websites associated with the Federal Trade Commission and the U.S. Department of Transportation (DOT) as well as some South Korean government sites. Other high-profile websites were targeted, including the New York Stock Exchange (NYSE), the Nasdaq and the Washington Post. While the attacks took out the websites, the impact was more of a nuisance, according to Lyon and other DDoS experts.

Hacktivists associated with Anonymous claimed responsibility for temporarily disrupting MasterCard's corporate website in retaliation for blocking payments to WikiLeaks and its founder Julian Assange. Paypal and other credit card providers were also targeted. The low-level, easy-to-contain attacks typically involve groups of individuals, but other, more sophisticated denial of service attacks exist, Lyon says. An individual hacktivist can launch a more complex DDoS attack by renting a botnet to control 100,000 systems or more and launch an attack against an individual website.

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

Organizations have several means of mitigating the risk of a denial of service attack, including buying an appliance to address the issue or contracting with a service provider that specializes in DoS prevention.

The market for DDoS appliances and services has matured, giving both large and small and midsize businesses the ability to mitigate the threat. Still, most attacks cause an initial disruption until the service can weed out the bad traffic, Lyon says.

LAW ENFORCEMENT CRACKDOWN

Law enforcement is beginning to make headway in jailing a number of high profile hacktivists and other individuals who align themselves with major hacktivst groups.

In March, federal authorities charged six members of Anonymous and its offshoot hacking groups in connection to the attacks on Sony and HBGary Federal. Also in March, police arrested members of the CabinCr3w, a group that affiliates itself with Anonymous. The individuals are suspected of hacking law enforcement related websites. Members of a number of groups in the UK and Russia were arrested for their role in denial-of-service attacks against the UK's foreign intelligence organization, MI6. Individuals suspected of having ties to attacks carried out by Anonymous were arrested in June in France, Belgium, and Québec, according to McAfee, which is one of a number of security firms tracking the hacktivist movement. The security firm tried to paint a picture of the impact hacktivists are having in a report, "Hacktivism: Cyberspace has become the new medium for political voices" (.pdf).

Sartin says recent arrests have resulted in fewer organized hacktivist attacks. However, the threat is still serious.

"Hacktivism is something that is here to stay," Sartin says. "These are individuals who are mainly unaffiliated with any one group, taking advantage of the fact that law enforcement doesn't have the bandwidth to go after them."

Hacktivist attacks gain widespread media attention, which has fueled interest in security technology and services to address it, he says.

"Activists are just using cyber as a way to express an opinion and I think they have had quite an impact," McAfee's Dirro says. "It's interesting to see that every day companies are getting hacked from nation-state sponsored actors, but what finally makes them take action are the hacktivism attacks in the news."

EDITOR'S DESK

PERSPECTIVES

SCAN

EDUCATION

PRODUCTS: READERS' CHOICE

THREAT MANAGEMENT: THE CRUCIAL COMBINATION

HACKTIVISM: INTENT TO SMEAR

BUILDING A DEFENSE

So how do you defend against a threat actor that isn't clearly identifiable, has an unknown number of members and a loosely defined set of principles?

Experts say the high-profile nature of hacktivist attacks makes planning for a hacktivist related breach essential. Many security vendors offer threat feeds, which can alert security teams when a new threat is detected and provide guidance on defense mechanisms. Security best practices—from keeping software updated to maintaining an intrusion prevention system and proactive log monitoring–prevail in defending against any security threat.

Experts say the high-profile nature of hacktivist attacks makes planning for a hacktivist related breach essential.

But post-breach response, which includes communicating with authorities and customers should be done carefully, says Ellen Giblin, an attorney that specializes in privacy and data protection at the Washington DC-based consulting firm, Ashcroft Group. Hacktivists have raised the stakes, making breach response and disclosure a messy process.

"It has delivered up a whole other avenue and reason for why folks make you a target," Giblin said. "It's getting more and more interesting trying to figure out how to capture the threat, understand it, monitor it and how to defend against it."

Organizations retooling their incident response plans should involve its legal team, a best practice that is sometimes a missed opportunity, she says. The company's legal team can help navigate through breach disclosure rules and other regulatory compliance mandates. Targeted organizations also need a way to counter the negative publicity following a hacktivist attack, she says.

Overall, incident response is immature in most organizations, says Rick Holland, a senior analyst at Forrester Research. Holland, who is developing an incident response security model as part of his research, says organizations need to provide a way for responders to quickly communicate issues to decision makers. Larger organizations with business units distributed around the world need to do a better job empowering incident responders, so they can shut down servers and isolate problems.

"There's a fine line of having all the processes in place, but you also need to make sure the people on the ground and in the trenches can do what they need to do to put out the fires," Holland says.

Mature organizations have most incident response processes documented and everyone on the incident response team knows their role if a problem is detected, he says. Those organizations conduct incident response simulations annually with information security teams getting drilled more often.

Knowledge of the threat landscape and the threat actors that are most likely to target the company is extremely important in incident response planning, according to Holland. Organizations in the financial and government sectors are the most proactive about hacktivism, he adds.

"I have clients who create fake Twitter and IRC personas to do human intelligence collection or are downloading and parsing through things so they know if an attack is imminent," Holland says. "In the financial services world, hacktivsts might be one of their top threat actors." ■

ROBERT WESTERVELT *is news director of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com*

TechTarget

EDITOR
Marcia Savage

SENIOR MANAGING EDITOR
Kara Gattine

SENIOR SITE EDITOR
Eric Parizo

NEWS DIRECTOR
Robert Westervelt

ASSISTANT SITE EDITOR
Brandan Blevins

DIRECTOR OF ONLINE DESIGN
Linda Koury

COLUMNIST
Marcus Ranum

CONTRIBUTING EDITORS
Michael Cobb, Scott Crawford,
Peter Giannoulis, Ernest N. Hayden,
Jennifer Jabbusch Minella, David Jacobs,
Diana Kelley, Nick Lewis,
Kevin McDonald, Sandra Kay Miller,
Ed Moyle, Lisa Phifer, Ben Rothke,
Anand Sastry, Dave Shackleford,
Joel Snyder, Lenny Zeltser

USER ADVISORY BOARD
Phil Agcaoili, Cox Communications
Richard Bejtlich, Mandiant
Seth Bromberger, Energy Sector Consortium
Mike Chapple, Notre Dame
Brian Engle, Health and Human Services Commission, Texas
Mike Hamilton, City of Seattle
Chris Ipsen, State of Nevada
Diana Kelley, Security Curve
Nick Lewis, Saint Louis University
Rich Mogull, Securosis
Tony Spinelli, Equifax
Matthew Todd, Financial Engines

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender
dolender@techtarget.com

ASSOCIATE PUBLISHER
Peter Larkin
plarkin@techtarget.com

TECHTARGET
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget:

TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

Cover and Awards feature: Istock