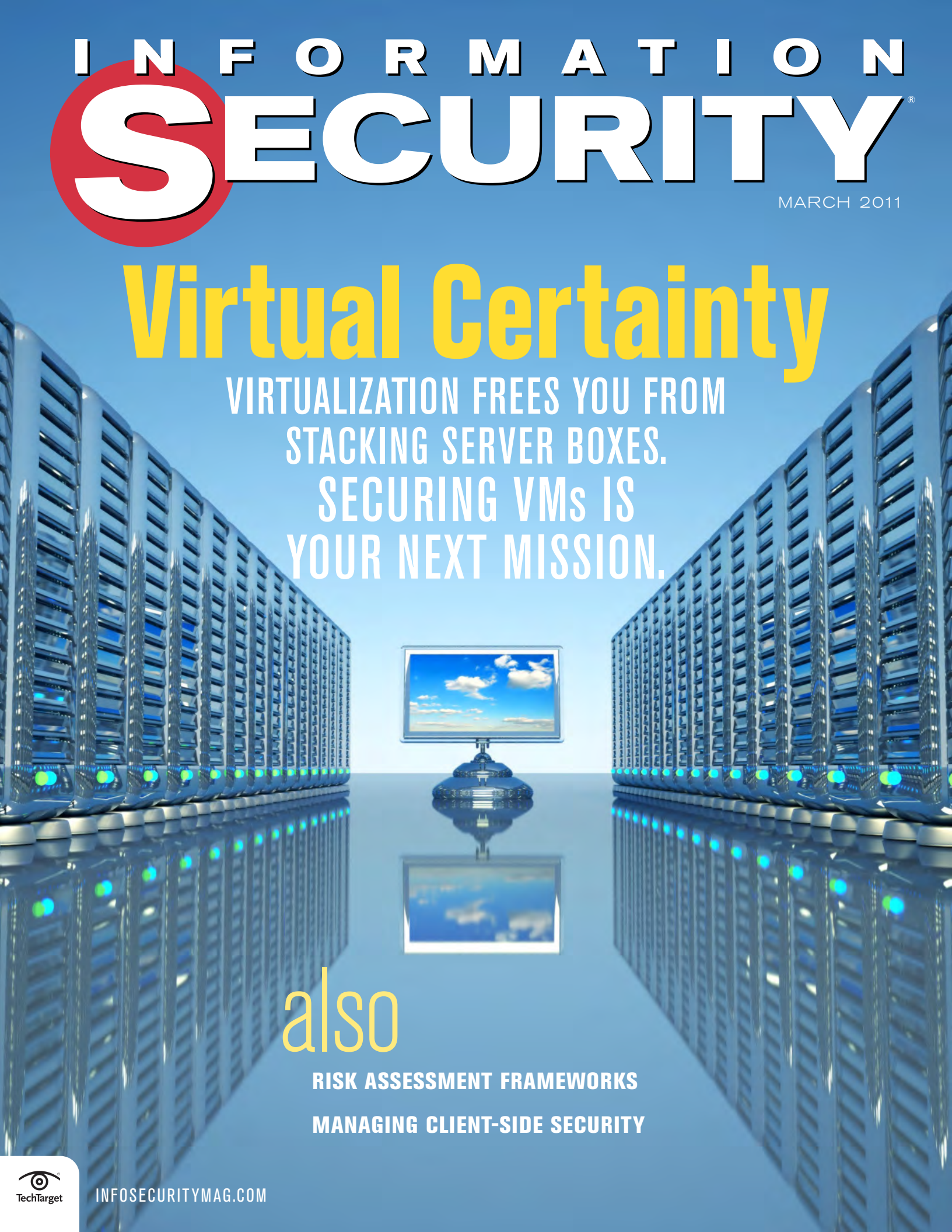
INFORMATION SECURITY®
MARCH 2011

Virtual Certainty

VIRTUALIZATION FREES YOU FROM STACKING SERVER BOXES. SECURING VMs IS YOUR NEXT MISSION.



also

RISK ASSESSMENT FRAMEWORKS

MANAGING CLIENT-SIDE SECURITY

TechTarget
INFOSECURITYMAG.COM

FROM OUR SPONSORS

contents

MARCH 2011
VOLUME 13 NUMBER 2

FEATURES

Virtual Certainty

Sizing Up Risk

The Client Side

DEPARTMENTS

Transformation Time

Help Wanted

Cybercrime Trends

A Framework for Security Career Success

ALSO

Recipe for Reinvention

Unleash your virtual desktop infrastructure

Maximize security AND performance
with the new OfficeScan

Virtually Unlimited Protection for Virtual Desktops

Don't let conventional security stand between you and cost savings. Unleash the security and performance of Trend Micro™ OfficeScan™ 10.5, the industry's first VDI-aware endpoint security. Only Trend Micro, the recognized leader in protecting virtual environments, delivers the accelerated performance of this ground-breaking new security for physical and virtual endpoints.

Unleash virtual desktops

There's only one way to maximize both security and performance.

View Flash Video

Industry-first optimization for virtual desktop infrastructure:

- Maximizes your consolidation ratio with no security tradeoff
- Conserves desktop performance with optimized resource usage
- Improves end user experience by minimizing duplicate scanning
- Integrates seamlessly with leaders such as VMware and Citrix

Contact Us Today to Schedule
a Free Demo. 1-877-21-TREND

TREND MICRO™

877-252-2065 • facebook.com/fearlessweb • twitter.com/trendmicro

Transformation Time

Cloud computing is forcing an evolution of information security practices and technology. BY MARCIA SAVAGE

IF YOU NEEDED any more confirmation of how big cloud computing has become (not that you really did), you didn't have to look any further than last month's RSA Conference 2011. This year's conference featured an entire track devoted to cloud security issues. Plus, the Cloud Security Alliance had a half-day summit at the conference, which attracted about four times as many people as last year.

There's no doubt that cloud computing is far from a passing fancy. Jim Reavis, CSA co-founder and executive director, says he's hearing about a lot of successful pilot cloud computing projects and roadmaps that include cloud adoption within the next year. M&A activity is helping drive cloud adoption, he says. IT leaders at large enterprises tell him they're looking to the cloud to satisfy the new IT needs that come with an acquisition or when a division is spun out into a separate company.

Sixty-eight percent said they're concerned about data protection/encryption in the cloud and 45 percent are worried about identity management/access control.

Security professionals, however, remain deeply concerned—and rightly so—about the compliance and security challenges cloud computing brings. According to the TechTarget Security Media Group Cloud Security Survey, 61 percent of 1,091 respondents cited regulatory compliance/audit as a top security concern with cloud computing. Sixty-eight percent said they're concerned about data protection/encryption in the cloud and 45 percent are worried about identity management/access control.

Transparency continues to be a big problem with cloud service providers. One survey participant—a technologist at a large insurance company—said providers balk at requests by customers to review their security controls. And encryption in the cloud is a complicated issue.

Groups like CSA are working to address the security issues with cloud computing, but Reavis acknowledges CSA's research isn't yet as technically detailed as it will need to be. CSA is making progress, he says, but rapid cloud adoption driven by the global economy makes it a challenge to keep up.

Vendors, of course, also are weighing in. They're seizing the opportunity to exploit the

cloud trend and falling over each other to pitch their products as "cloud" solutions. The hype is tremendous, muddying the real issues. However, some interesting new technologies are making their way through all the noise.

CloudPassage, for instance, touts its server vulnerability management and firewall services as the first purpose-built for elastic cloud environments. CEO Carson Sweet says the technology tackles the problem of managing server security in a cloud environment, where servers are rapidly created through cloning and bursting. CloudPassage's platform, which consists of the Halo Daemon, a small software component on each cloud server and the Halo grid, an elastic compute grid that analyzes data collected by the Daemon, works to automatically secure cloud servers when they're burst or cloned.

Another new company, CipherCloud, offers a Web proxy that provides encryption and tokenization for enterprise data as it's sent to a cloud service provider. Encryption keys remain with the customer, data formats and functions are preserved, and latency is less than two percent, executives say. The technology supports Salesforce.com; support for Google Apps is in development. It's offered as a hosted service or virtual on-premise appliance.

CSA's Reavis says cloud computing is reinventing every part of IT, and he expects it will do will do the same with the information security industry. CSA is researching how cloud computing can be used to secure everything—not just cloud but other forms of IT.

Interesting times, indeed. We'll be tracking developments in the cloud security space on our new sister site, SearchCloudSecurity.com. Check it out.›

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

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™

Recipe for Reinvention

Enterprise use of consumer-oriented technologies requires a new security model.

BY CHENXI WANG

AMYLIN, a diabetes specialist pharmaceutical company, is busy developing e-detailing applications—applications that provide physicians with information about its products—for iPads. Sales reps who often have to squeeze their visits into a doctor's busy schedule love the capability to walk and talk with the doctor, all the while showing a flashy presentation on the iPad. The new world of mobile tablets, like the iPad, hold much appeal over the old ways of bulky flipcharts and heavy laptops. Amylin would see a positive ROI just by eliminating the need to print detailing materials every year.

Amylin is not alone. Almost every Fortune 500 company has a strategy to utilize social, mobile, video and cloud technologies, either to optimize operations or improve customer reach. This is what Forrester Research refers to as the "Empowered movement," where companies are empowering their employees with modern, consumer-oriented technologies to better serve their customers. According to a recent Forrester online survey, nearly 40 percent of information workers today use some form of self-provisioned technologies. This trend is expected to only accelerate in 2011. But is IT security ready for it?

Almost every Fortune 500 company has a strategy to utilize social, mobile, video and cloud technologies, either to optimize operations or improve customer reach.

IT security simply doesn't have a choice: empowerment will happen regardless of security. Just as a few clever individuals will find a way to read corporate emails on their iPhones without IT support, consumer technologies will invade your enterprise independent of any adoption barriers. On the other hand, corporate IT is the only place where business can expect consistent, long-term support for the otherwise fragmented, self-provisioned initiatives. In addition, the organization can benefit from the central oversight and coordination IT brings, as siloed technology efforts can result in inefficiency and missed opportunities to leverage others' experiences.

This movement in fact provides a rare opportunity for IT to reinvent itself. Think

about it: Corporate data is going into the cloud, mobile devices are edging out traditional PCs, and social technologies are enabling ad hoc collaborations anytime, from anywhere. The status quo approaches simply won't cut it anymore. If there ever was a time to rethink existing security models, now is it.

So, how do you do it? How do you protect your company's most prized assets in such a rapidly changing business and technology environment? You need a new modus operandi:

- **Engage the business.** Meet with major business functions proactively to understand their approach to social, cloud, and mobile technologies. Offer the risk perspective and become involved in their strategy decisions. Recruit representatives as your eyes and ears and educate managers and employees about the risks of these groundswell technologies.
- **Run at the threat and shape the outcome.** Tackle the security fundamentals; do not chase the symptom du jour. This allows you to focus on your goals vs. changing strategies every time a new threat or technology enters the enterprise.
- **Influence and incite security-aware human behavior.** Your employees are now your perimeter of defense. It is imperative that they have a basic level of understanding of the risks with these new technologies. IT security can play an education and awareness training role. In fact, you should insist that a baseline for education is that managerial staff understand the risk tolerance level of the enterprise and master the skills for risk assessment so they can make intelligent risk-vs.-reward decisions on their own.

With the Empowered movement, IT security is being thrust into a crucial business function. With your support, the business can more effectively utilize innovative technologies to optimize, innovate, and compete. You can emerge from this process, transforming from the role of a utility provider to a partner, an advocate, and ultimately a trusted advisor.›

Chenxi Wang is a vice president and principal analyst at Forrester Research, where she serves security and risk professionals. Send comments on this column to feedback@infosecuritymag.com.

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

Recognition • Success • Growth

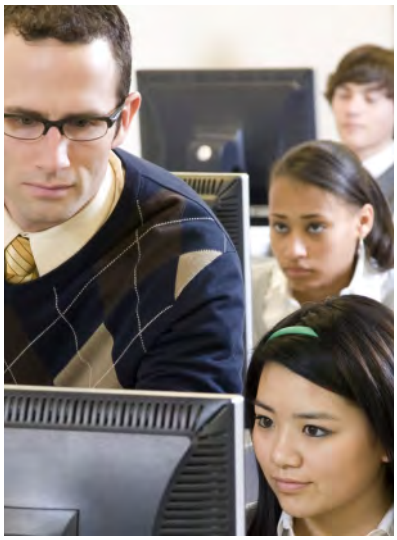
June Exam Date: 11 June 2011
Registration Deadline: 6 April 2011

ISACA®
Trust in, and value from, information systems

ANALYSIS | SECURITY CAREERS

Help Wanted

A new competition tries to foster interest in cybersecurity as early as high school. BY ROBERT WESTERVELT



WHEN KEVIN QUINLAN took a position a decade ago at Bertucci's Corp., he started as a network administrator, ensuring that restaurant chain's critical systems were available at all times. Today, Quinlan is senior director of information technologies at Bertucci's, and a major part of his time is devoted to data security and compliance initiatives, a role he says has evolved over the years.

"I was a general network technician, but it became clear that security was going to be more important every day on the job," he says. "People started losing files and I had to start putting the pieces of the puzzle together."

Like Quinlan, most people who become cybersecurity professionals are drawn into the profession while on the job, says Alan Paller, director of research at the SANS Institute, a Bethesda, Md.-based security training and certification organization. With few people emerging from colleges and universities trained in cybersecurity, Paller believes more work needs to be done to get better skilled security professionals in the government and in the private sector.

"Our very future depends on it," Paller says. "If we want to remain competitive and have strong cybersecurity defenses, we need a larger talent pool. So, our goal is to make cyberskilled people as cool as sports skilled people by giving them visibility."

"If we want to remain competitive and have strong cybersecurity defenses, we need a larger talent pool."

–ALAN PALLER, director of research, SANS Institute

That's why the U.S. Cyber Challenge, a division of the non-profit thinktank, Center for Internet Security, in late January kicked off its Cyber Foundations, an online competition attempting to foster an interest in cybersecurity at the high school level. The com-

petition, partially funded with a federal grant, was launched last year in public schools in Rhode Island, California and Maryland. This year the competition is being rolled out nationally with school systems in Texas, Delaware, and Minnesota conducting formal campaigns to encourage schools and students to participate. The program also receives funding from Lockheed Martin and Microsoft.

While there are some good cybersecurity programs at the college level, their numbers are few and far between. Universities and colleges develop many of their programs based on demand, making the focus on the high school level an important part of developing future talent, says Karen Evans, the national director of the U.S. Cyber Challenge.

"What you have to do is have a group of individuals interested in developing a specific career path," says Evans, an IT veteran who held the title of U.S. chief information officer in the George W. Bush administration. "Students don't know that these opportunities exist, and if you can try to pique their interest, you'll see a greater demand for programs at colleges."

"Students don't know that these opportunities exist, and if you can try to pique their interest, you'll see a greater demand for programs at colleges."

–KAREN EVANS, national director of the U.S. Cyber Challenge

The SANS Institute is providing the training material for the program. Students who register take a series of tutorials followed by several timed quizzes in March and April that test their knowledge in networking, operating systems and system administration. Statewide winners will get cash prizes of up to $100; winners will be announced at the end of April.

Rhode Island was among the first states to pilot the program last fall in three high schools. Officials there say the competition was successful in at least exposing the career path to young students. Now that the program is being implemented more broadly, those behind it hope it could find 10,000 Americans interested in pursuing cybersecurity.

"We don't have an efficient robust cybersecurity workforce at the ready," said Congressman James Langevin (D-Rhode Island) in a press conference kicking off the program. "We're finally challenging our young people in the area of cyber capabilities and networks."

Bertucci's Quinlan says he thinks programs aimed at high schoolers could broaden the talent pool of IT professionals, but cybersecurity may be a skill better learned on the job. Various factors make the career path a hard-sell, he says, but those who pursue it find it very rewarding.

"Security is something that you fall into after a real-world experience," says Quinlan. "You can theorize and think you know what you need to do to secure data, but when you get into the real world you find there are different departments and people that you have to address. It's not a clear-cut career path."

Robert Westervelt is news director of the Security Media Group at TechTarget. Send comments on this article to feedback@infosecuritymag.com.

Be Prepared.

Meet the rising tides of security & compliance demands with identity governance.

With on-demand visibility into "who has access to what," you can address compliance mandates across the most complex IT environment. SailPoint IdentityIQ™ automates access certifications, policy enforcement, and drives the end-to-end access request and fulfillment process. Its Identity Governance platform helps you to centralize identity data and capture business policy, model roles, and proactively manage risk. This unique approach alleviates the cost and complexity of managing user lifecycles and meeting auditor requirements—all while still helping you to meet the highest standards of corporate governance.

Visit **www.sailpoint.com** to learn how we can help you stay afloat.

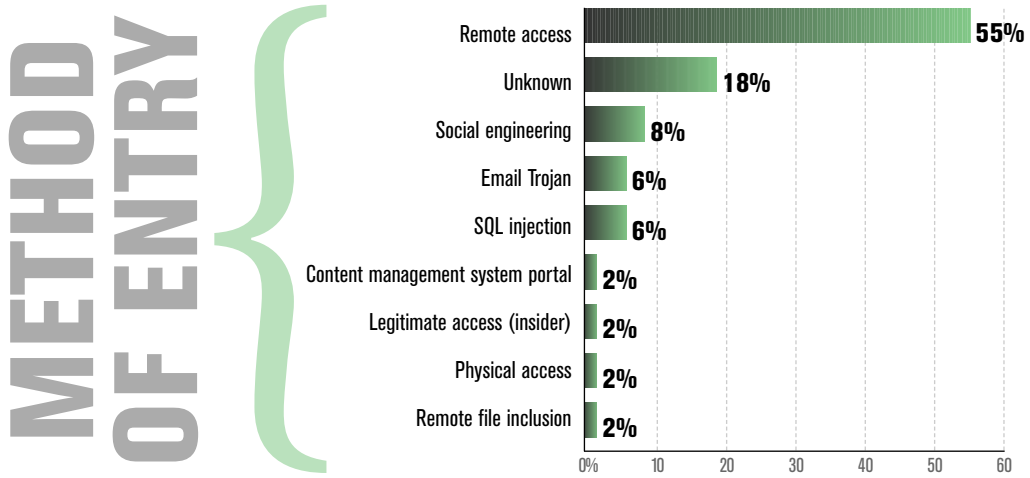
SailPoint™
MANAGING THE BUSINESS OF IDENTITY

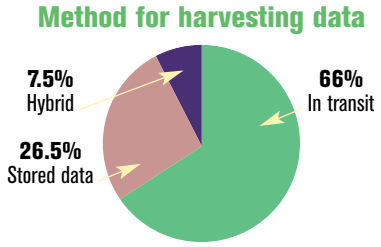
www.sailpoint.com

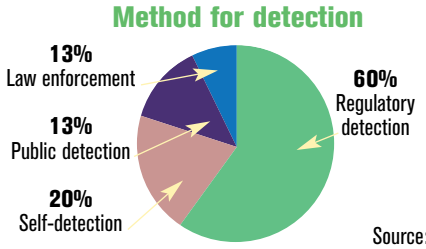
Cybercrime Trends

by *Information Security* staff

Cybercriminals are targeting endpoint devices, stealing data in transit, and exploiting unsecure remote access applications, according to report from Trustwave. Based on 220 investigations conducted by the company's SpiderLabs research team last year, the report showed that use of vendor-supplied default credentials coupled with unsecure remote access apps are making things easy even for novice attackers. Here are some noteworthy findings from the report:







Source: Trustwave

overheard

"If we are to be successful in protecting our critical infrastructure systems from cyber threats–whether intentional attacks or unintentional compromises–we must address our nation's shortage of skilled cybersecurity professionals."

–JAMES A. LEWIS, director and senior fellow, technology and public policy program at the Center for Strategic and International Studies, on the U.S. Cyber Challenge's launch of a high school cybersecurity competition.

Did I just *send* that **file** to the ***wrong person?***

Check Point **DLP** prevents data breaches before they occur

Have you ever accidentally sent an email to the wrong person or attached a document that wasn't meant to be shared?

Check Point makes DLP work by combining technology and processes to move businesses from passive detection to prevention, before data breaches occur.

PREVENT data loss

EDUCATE users

ENFORCE data policies

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

A Framework for Security Career Success

Here are four things you need to do in order to execute on your long-term career plan. BY LEE KUSHNER AND MIKE MURRAY

AS IMPORTANT as it may be for information security professionals to develop a written career plan, executing on your plan is essential to accomplishing your career goal. Now is an opportune time to reflect and determine what you need to do to continue your progression as an information security leader.

Each individual's professional development will vary based on their level of experience, baseline of skills, and stage of their careers. However, the framework for implementing and demonstrating these qualities is consistent for all and consists of the following actions: lead, impact, learn, and assess.

DEMONSTRATE SECURITY LEADERSHIP

The most important attribute information security professionals need to demonstrate is leadership. Leadership takes many forms, such as leadership over security technologies (i.e. application security, cloud computing, security event management), projects or organizational initiatives (i.e. PCI compliance, data loss prevention, identity management), people (including information security professionals and other staff), or an entire security function.

Wherever you are in your career, demonstrate your leadership and take ownership of a specific information security task where you can succeed. Grab the spotlight and showcase your skills to people who may be able to influence your career.

Successful execution of DLP, cloud or identity management projects, for example, will enhance your personal brand inside the company. This should earn you additional chances to demonstrate your talents and provide you with opportunities for advancement and promotion.

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.

IMPACT SECURITY IN MEASURABLE WAYS

Information security leaders must create a measurable impact for the organization, such as cost savings or profitability, efficiency, enhanced security (no breaches), or organizational recognition. It is important for you to understand how your current employer measures contributions, and do your best to align the impact of your achievements to their desired currency.

For example, if your company values cost savings, you should try your best to complete your task under budget. If they value efficiency, you should do your best to complete your project early. And if they value excellence, you should make sure that your project exceeds the accepted baselines.

Exhibiting these results in terms your organization values provides your current manager and employer a view into your personal capabilities. It also gives them the confidence to assign you more advanced tasks that provide you with greater opportunities to demonstrate your leadership abilities to generate more recognizable results.

LEARN SECURITY SKILLS THAT ACCELERATE YOUR CAREER

Opportunities to lead and impact should confirm your skills and strengths, and shed light on your deficiencies and weaknesses. Most importantly, by gaining exposure to newer technologies, more complex business problems, and different business and technology stakeholders, you should be able to gain insight into the current gaps in your skill matrix and make a strategic decision on what you need to learn in order to accelerate your career.

Witnessing your shortcomings in a real-world environment can provide you with better context in the selection of specific career investments that will yield more immediate results.

For example, you may find it to be more efficient to take a targeted course that will directly address your weakness in a short period of time, than to enroll in an executive MBA program that is time consuming and costly. Witnessing your shortcomings in a real-world environment can provide you with better context in the selection of specific career investments that will yield more immediate results.

HONESTLY ASSESS YOUR ANNUAL ACCOMPLISHMENTS

One of the underlying keys to the execution of a successful career plan is the ability and willingness to honestly assess your leadership, impact and learning progress throughout the year.

Keep a written diary of your accomplishments during the course of the year, making it easier to chart your progress and stay on track as you map toward your mid-range and long-term career goals. In addition, if you feel you have nothing to write down and you are not

making any progress, it should serve as a personal wake-up call that others may be surpassing you.

The above framework should be applicable to all information security professionals who aspire to advance their careers. Identify and reach specific short term milestones and goals specific to your career. This will allow you to increase your marketability (to current and future employers) and provide you with a sense of progress and increased job satisfaction.

Demonstrating successful leadership, creating measurable impacts, and making strategic and meaningful career investments are the cornerstones to a successful career as an information security leader. It should be the goal of every information security professional to consistently seek out these opportunities and give yourself the chance to demonstrate your talents.

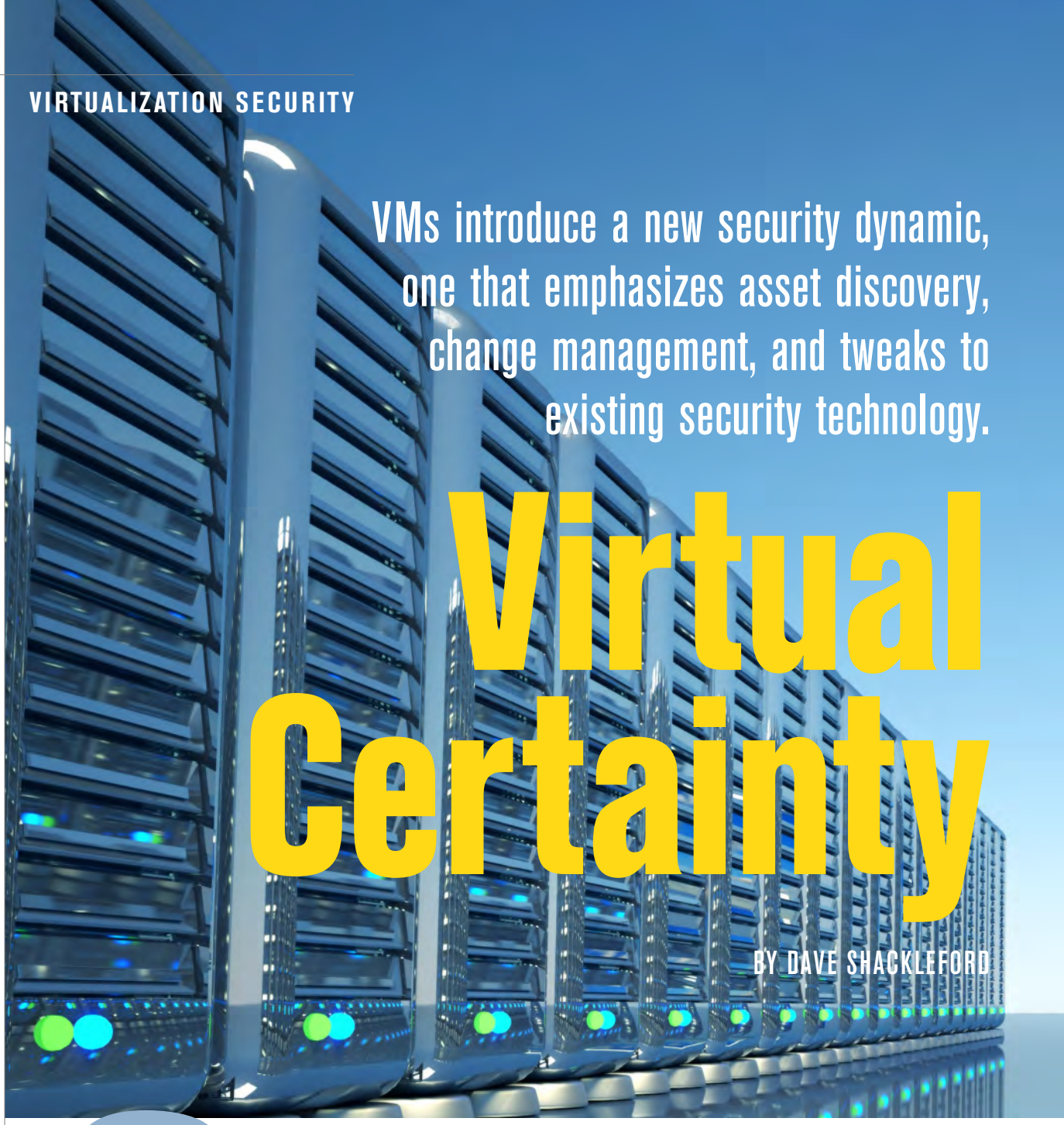
Send comments on this column to feedback@infosecuritymag.com.

Yes, we are those people. **Serious fans of technology.** The engineers **up at 3 am** learning about the latest release. The ones that **answer the customer call** at 10 pm. The people that think CCIEs are **rock stars.** The **fanatics.** The people that **love what we do.** In an industry like ours where change is accelerated, you have to really have a passion to stay ahead. And we honestly believe that helping our clients isn't work, it's **pure fun.**

From virtualization and cloud computing to unified communications and network security, DynTek provides professional technology solutions to architect, secure and support the core areas of your technical environment: Infrastructure/Data Center, Application Platforms and End Point Computing. www.dyntek.com

McAfee®

To schedule a free consultation, call 877-297-3723 or email marketing@dyntek.com.



VMs introduce a new security dynamic, one that emphasizes asset discovery, change management, and tweaks to existing security technology.

Virtual Certainty

BY DAVE SHACKLEFORD

AS VIRTUALIZATION TECHNOLOGY becomes common within the modern IT environment, the need for sound security and risk management for these systems increases. Although the technology and architecture can be complex, there are a number of best practices and straightforward techniques security teams can take to keep track of virtualization components and virtual machines, secure them properly, and maintain a strong, compliant security posture over time.

VIRTUAL MACHINE DISCOVERY AND INVENTORY

A first critical step in properly securing a virtual infrastructure is ascertaining where virtual machines are located and how an accurate inventory can be maintained. In many organziations, system inventories are out of date; in fact, many are kept in spreadsheets with manual input from systems and network administration teams.

Due to the dynamic nature of virtual environments, a common scenario dubbed virtual sprawl can easily occur, where virtual machines are created and used for a period of time, but never noted in a formal systems inventory. Many of these virtual machines may be used for testing or short-term purposes, and remain active long after they've served their initial purpose. Unfortunately, with little lifecycle maintenance, these systems can easily be missed during patching cycles, and may expose your organization unnecessarily.

Due to the dynamic nature of virtual environments, a common scenario dubbed virtual sprawl can easily occur, where virtual machines are created and used for a period of time, but never noted in a formal systems inventory.

There are many ways to maintain an accurate virtual machine inventory via discovery and systems management tools. For many virtualization deployments, inventory can be maintained by using built-in tools within virtualization platforms, such as the inventory category within VMware vSphere's vCenter management console, or Microsoft's virtualization management tools such as Systems Center Virtual Machine Manager. Other tools can be leveraged, as well, such as VMware Lifecycle Manager, which offers more robust system lifecycle management and provisioning, or endpoint security and configuration tools that rely on installed agents within virual machines, such as Symantec Altiris and similar products. Finally, assessing the known inventory on a hypervisor platform such as VMware ESX or ESXi can be accomplished with various scripting tools.

In addition to these tools, several other discovery options should be considered. First, because most virtualization deployments rely heavily on centralized storage, any available storage management tools can be leveraged for VM file inventory maintenance. As most, if not all, virtual machine disk and configuration files will be stored on a storage area network (SAN) or network attached storage (NAS), any inventory tools from storage vendors should be used to the fullest extent possible. Examples of these include EMC Ionix ControlCenter and NetApp OnCommand products. Second, verifying running virtual machines from a network perspective can be done using well-known network scanners such as Nmap and others–all virtualization vendors have a defined set of organizationally unique identifiers (OUIs) in place for the first three hexadecimal values of a virtual system's MAC address. By scanning local subnets, capturing MAC addresses and comparing them to these OUIs, security teams can correlate this data with other inventory information.

VIRTUALIZATION CHANGE AND CONFIGURATION MANAGEMENT

The second major area to consider in properly securing a virtual environment is operations management, namely change and configuration management. At the 2008 Burton Catalyst conference, Alessandro Perilli, founder of virtualization.info, stated that the "weakest part of the security defense we have in our infrastructure is related to the way we manage our operational framework."

Unfortunately, little has changed since 2008. Integrating virtualization platforms, management infrastructure, network components, and virtual machines into existing change and configuration management policies and procedures is critical to ensure long-term stability and security of the entire infrastructure, particularly as the use of virtualization increases.

Configuration management is primarily focused on two elements: security hardening and patching. From a security hardening perspective, numerous sources of guidance exist to help systems and security administrators adequately lock down their virtualization components.

For hypervisor platforms (for example, VMware ESX, Microsoft Hyper-V, and Citrix XenServer), most major vendors have guidance freely available. The latest version of VMware's vSphere Hardening Guide includes guidance on configuring virtual machine configuration files, hypervisor hosts, virtual networks, and management components, with flexible options for different levels of security criticality.

Patching virtualization infrastructure is the second critical configuration task that should be performed regularly.

Microsoft's Hyper-V Security Guide outlines several important configuration practices that should be considered for any Hyper-V implementation, such as running Hyper-V on 2008 Server Core, and selecting specific server roles, implementing Authorization Manager for more granular roles and privileges, and hardening Windows virtual machines. In addition, the Center for Internet Security (CIS) and the Defense Information Systems Agency (DISA) have free configuration guides available for download at their respective sites. These guides should be viewed as a starting point for proper security hardening, since most organizations will have numerous modifications and concessions required for their own operating environments.

Patching virtualization infrastructure is the second critical configuration task that should be performed regularly. The first option for many security and operations teams will be to investigate their existing patch management product(s) to see whether they support virtualization products and platforms. In most cases, the hypervisor hosts will need to be patched with specialized tools, such as VMware Update Manager. The virtual machines can almost always be patched with existing tools, although specific scheduling and testing regimens may be called for. There are two primary differences to consider when patching virtual machine operating systems. First, patching will need to be carefully scheduled so as not to overload the shared pool of physical resources on a single platform, such as RAM, CPU, etc. The second consideration relates to offline, or "dormant" VMs—these will need to powered on in order to patch in most

cases. Be sure that your patch management tools have been tested to work with whatever type of virtual machines you're running (Xen, VMware, etc.).

Change management is another key element of secure and resilient operations for virtualization. Virtual machines can be created and made available within minutes, versus traditional servers and applications that need to be installed on hardware and installed in a data center. For this reason, it's imperative that new change management ticket categories are created for producing, modifying, and deleting virtual infrastructure or virtual machine components, and virtualization teams should be included in all change management review meetings and discussions. Provisioning, patching, updating and decommissioning virtual machines should be done exactly the same way as their physical counterparts from a process and policy standpoint, and this needs to be reinforced from the highest levels of IT management.

Provisioning, patching, updating and decommissioning virtual machines should be done exactly the same way as their physical counterparts from a process and policy standpoint, and this needs to be reinforced from the highest levels of IT management.

SECURITY ARCHITECTURE FOR VIRTUAL NETWORKS

There are many architecture options security and network teams will need to consider for virtual network environments. First, virtual switches are different in many ways from physical switches. Many more switch ports can be provisioned on a single virtual switch than a physical one. Also, default virtual switches from virtualization vendors cannot be cascaded, or connected to each other, inside the virtual environment. For this reason, planning the number and types of virtual switches that need to be connected to physical NICs is critical, because the number of physical NICs in a system is limited.

This also means that virtual switches are isolated from each other by default, and most also support the use of virtual LANs (VLANs) for additional Layer 2 segmentation between specific groups of ports on the virtual switch. Some virtual switches also have built-in security policy settings that can be configured. For example, VMware's default virtual switch can be placed into promiscuous mode for monitoring, and can also have rudimentary MAC address filtering enabled to prevent MAC spoofing attacks.

However, the default virtual switches from platform providers leave much to be desired. True SPAN or mirror ports cannot be created for dedicated traffic mirroring, extensive port-level security is not available (locking down one port to one MAC address, for example), and management capabilities are very limited. Cisco has created a virtual switch, the Nexus 1000v, which can be imported into virtual environments and offers the same features and functionality as a traditional physical Cisco switch, complete with command-line IOS management. For Citrix, KVM, and VirtualBox environments, the Open vSwitch virtual switch is an open-

source alternative that provides similar functionality to Cisco's offering.

Regardless of the virtual switches used, security teams will want to ensure that redundancy and security are built into the virtual network design. Several different traffic segments are typically associated with virtualization platforms. The first is simply the virtual machine production traffic, consisting of virtualized operating systems and applications. This traffic should be on separate virtual switches, with at least two physical NICs for redundancy. The next traffic type is storage traffic and specialized virtualization traffic, often including virtual machine migration that may occur in cleartext. Since this is very sensitive data, this segment should be on distinct virtual switches when possible, with multiple dedicated physical NICs for redundancy, as well. Finally, a third segment should be in place for management traffic, usually consisting of protocols like SSH and SSL-based management console interaction. Like the other two segments, separate virtual switches and redundant physical NICs should be used.

A core tenet of virtualization is the ability to have multiple virtual machines and networks on a single physical platform. By default, virtual machine traffic on different virtual switches is separate, unless both virtual switches connect to the same physical network outside the hypervisor platform. However, all traffic is handled by the hypervisor, and a potential compromise to the hypervisor could allow traffic to be exposed at a single point. For this reason, it is recommended that data of different sensitivity or classification levels be kept on separate physical hypervisor platforms as an added measure of segregation.

HYPERVISOR SECURITY AND MANAGEMENT

One of the most commonly overlooked elements of virtualization security is proper management and administration of hypervisor platforms and related components. In many cases, a single systems administration team is charged with designing and managing all aspects of the virtualization infrastructure, but this violates the security best practices of separation of duties and least privilege.

One of the most commonly overlooked elements of virtualization security is proper management and administration of hypervisor platforms and related components.

To properly maintain these principles, specific roles and groups should be created within the virtualization management console or similar third-party application that allows network teams to manage virtual networks, specific administration teams or development teams to manage particular virtual machines, and a core virtualization team (or other administration team) to manage the general virtualization platform configuration. Additional roles may be needed for auditors and security teams, depending on the scenario. Only the specific privileges needed for these roles should be assigned—in other words, networking teams have no need to manage virtual disk images, auditors should be granted "read only" access, etc.

Management platforms should also be secured properly. These systems should be considered

high value, as they grant full access to the configuration of hypervisor platforms, virtual machines, virtual networks and storage components in use. Many management applications are installed on Microsoft Windows operating systems, and keeping these systems patched and locked down appropriately is critical to the overall security of the entire virtual environment. Regardless of OS, make sure to keep the management systems on a separate, carefully restricted network segment that is only accessible to approved administration teams, and institute sound log management practices for all access to the systems, failed logins, error messages, and other events dictated by security policies and compliance requirements.

Many management applications are installed on Microsoft Windows operating systems, and keeping these systems patched and locked down appropriately is critical to the overall security of the entire virtual environment.

TWEAKING SECURITY TECHNOLOGIES FOR VMs

There are many additional security technologies and processes that are likely affected by virtualization. For example, antimalware agents running on virtual machines must be configured to exclude certain virtual disk or configuration files (to prevent corruption), and file system scans must be scheduled very carefully, to avoid multiple virtual machines using shared hardware resources simultaneously, potentially leading to a local denial-of-service or other undesirable consequences.

Intrusion detection systems and firewalls may not have granular visibility into the virtual environment to enforce access controls or detect anomalous or malicious traffic. For this reason, many security product vendors have created virtual appliances for these devices, allowing internal virtual switch traffic to be monitored and controlled much like that in traditional physical networks.

McAfee, Symantec, Sourcefire, HP TippingPoint, and many other vendors have virtual offerings for intrusion detection and prevention systems. A number of companies offer products specific to virtual network access control and traffic analysis, such as Altor Networks (now Juniper), Reflex Systems, and HyTrust.

Virtual appliances for mail and network antimalware gateways are available, and VMware has a number of security products available in their vShield line, including traditional and application-centric access control systems, as well as antimalware capabilities. Open-source offerings such as the Snort and Shadow IDS engines, as well as the host-based OSSEC IDS can be downloaded as virtual appliances or installed into virtual machines, too. In general, most security professionals feel that virtualized security tools should be used to augment existing security technology instead of replacing it, but these new tools will most certainly be more readily adopted over time.

Although many IT teams may make the argument that virtualization simplifies the infrastructure, the opposite may be true for security professionals. The use of virtualization technology adds additional layers of complexity and interaction between applications, operating systems, hypervisor engines, and network components. New management systems, storage requirements and data protection scenarios, such as automated migration of virtual machines from one system to another, make security and controls maintenance challenging as virtualization continues to grow. Many best practices are still applicable, however, and by diligently applying security to design, discovery, and configuration processes, it's possible to create a secure virtual infrastructure today.

Dave Shackleford is a founder and principal consultant with Voodoo Security and also a certified SANS instructor. Send comments on this article to feedback@infosecuritymag.com.

NOTHING GETS PAST RED

Get Comprehensive Network Protection - including Application Control!

WatchGuard's new Application Control for XTM appliances allows businesses to control what's being used on their networks – from Facebook to Skype – for tighter security and increased productivity. With sophisticated behavioral analysis and more than 2,300 signatures, it allows IT to control over 1,500 web 2.0 and business apps with ease.

- Find out how you can take back control of your network with our free white paper at **www.watchguard.com/appcontrol**.
- See how WatchGuard outperforms every other major UTM brand on the market at **www.watchguard.com/utmmarketreview**.

For more information, call **1.800.734.9905** or visit **www.watchguard.com**. Get **red.** Get secu**red.**

WatchGuard™

There are a lot of risk assessment frameworks out there. Here's what you need to know in order to pick the right one.

Sizing Up Risk

BY RICHARD E. MACKEY, JR.

MANY REGULATIONS and virtually all security frameworks require some objective assessment of risks. The reason is simple: Security controls should be selected based on real risks to an organization's assets and operations. The alternative—selecting controls without a methodical analysis of threats and controls—is likely to result in implementation of security controls in the wrong places, wasting resources while at the same time leaving an organization vulnerable to unanticipated threats.

A risk assessment framework establishes the rules for what is assessed, who needs to be involved, the terminology used in discussing risk, the criteria for quantifying, qualifying, and comparing degrees of risk, and the documentation that must be collected and produced as a result of assessments and follow-on activities. The

goal of a framework is to establish an objective measurement of risk that will allow an organization to understand business risk to critical information and assets both qualitatively and quantitatively. In the end, the risk assessment framework provides the tools necessary to make business decisions regarding investments in people, processes, and technology to bring risk to acceptable level.

Two of the most popular risk frameworks in use today are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), developed at Carnegie Mellon University, and the NIST risk assessment framework documented in NIST Special Publication 800-30. Other risk frameworks that have a substantial following are ISACA's RISK IT (part of COBIT), and ISO 27005:2008 (part of the ISO 27000 series that includes ISO 27001 and 27002). All the frameworks have similar approaches but differ in their high level goals. OCTAVE, NIST, and ISO 27005 focus on security risk assessments, whereas RISK IT applies to the broader IT risk management space.

OCTAVE, NIST, and ISO 27005 focus on security risk assessments, whereas RISK IT applies to the broader IT risk management space.

How does a company know which framework is the best fit for its needs? We'll provide an overview of the general structure and approach to risk assessment, draw a comparison of the frameworks, and offer some guidance for experimentation and selection of an appropriate framework.

ASSET-BASED ASSESSMENTS

All risk assessment methods require organizations to select an asset as the object of the assessment. Generally speaking, assets can be people, information, processes, systems, applications, or systems. However frameworks differ in how strict they are in requiring organizations to follow a particular discipline in identifying what constitutes an asset. For example CMU's original OCTAVE framework allowed an organization to select any item previously described as the asset to be assessed, where the most recent methodology in the OCTAVE series, Allegro, requires assets to be information.

There are advantages and disadvantages associated with any definition of asset. For example, if an asset is a system or application, the assessment team will need to include all information owners affected by the system. On the other hand, if the asset is information, the scope of the assessment would need to include all systems and applications that affect the information. Practically speaking, it is important to define the asset precisely so the scope of the assessment is clear. It is also useful to be consistent in how assets are defined from assessment to assessment to facilitate comparisons of results.

A critical component of a risk assessment framework is that it establishes a common set of terminology so organizations can discuss risk effectively. See p. 30 for a list of terms used in most frameworks.

Framework Terminology

Risk assessment frameworks establish the meaning of terms to get everyone on the same page. Here are terms used in most frameworks.

Actors, motives, access: These describe who is responsible for the threat, what might motivate the actor or attacker to carry out an attack, and the access that is necessary to perpetrate an attack or carry out the threat. Actors may be a disgruntled employee, a hacker from the Internet, or simply a well meaning administrator who accidently damages an asset. The access required to carry out an attack is important in determining how large a group may be able to realize a threat. The larger the attacking community (e.g., all users on the Internet versus a few trusted administrators), the more likely an attack can be attempted.

Asset owners: Owners have the authority to accept risk. Owners must participate in risk assessment and management as they are ultimately responsible for allocating funding for controls or accepting the risk resulting from a decision not to implement controls.

Asset custodians: A person or group responsible for implementing and maintaining the systems and security controls that protect an asset. This is typically an IT entity.

Impact: The business ramifications of an asset being compromised. The risk assessment team needs to understand and document the degree of damage that would result if the confidentiality, integrity, or availability of an asset is lost. The terms impact, business impact, and inherent risk are usually used to describe, in either relative or monetary terms, how the business would be affected by the loss. It's important to note that impact assumes the threat has been realized; impact is irrespective of the likelihood of compromise.

Information asset: An abstract logical grouping of information that is, as a unit, valuable to an organization. Assets have owners that are responsible for protecting value of the asset.

Risk magnitude or risk measurement criteria: The product of likelihood and the impact described above. If we consider likelihood a probability value (less than 1) and impact a value of high, medium, or low, the risk magnitude can be "calculated" and compared to risks of various threats on particular assets.

Security requirements: The qualities of an asset that must be protected to retain its value. Depending on the asset, different degrees of confidentiality, integrity, and availability must be protected. For example, confidentiality and integrity of personal identifying information may be critical for a given environment while availability may be less of a concern.

Threats, threat scenarios or vectors: According to OCTAVE, threats are conditions or situations that may adversely affect an asset. Threats and threat scenarios involve particular classes of actors (attackers or users) and methods or vectors by which an attack or threat may be carried out.

glossary

RISK ASSESSMENT METHODOLOGY

The heart of a risk assessment framework is an objective, repeatable methodology that gathers input regarding business risks, threats, vulnerabilities, and controls and produces a risk magnitude that can be discussed, reasoned about, and treated. The various risk frameworks follow similar structures, but differ in the description and details of the steps. However, they all follow the general pattern of identifying assets and stakeholders, understanding security requirements, enumerating threats, identifying and assessing the effectiveness of controls, and calculating the risk based on the inherent risk of compromise and the likelihood that the threat will be realized. The following is a basic methodology, largely derived from the OCTAVE and NIST frameworks.

1. Identify assets and stakeholders

All risk assessment methods require a risk assessment team to clearly define the scope of the asset, the business owner of the asset, and those people responsible for the technology and particularly the security controls for the asset. The asset defines the scope of the assessment and the owners and custodians define the members of the risk assessment team.

NIST's approach allows the asset to be a system, application, or information, while OCTAVE is more biased toward information and OCTAVE Allegro requires the asset to be information. Regardless of what method you choose, this step must define the boundaries and contents of the asset to be assessed.

2. Analyze impact

The next step is to understand both the dimensions and magnitude of the business impact to the organization, assuming the asset was compromised. The dimensions of compromise are confidentiality, integrity, and availability while the magnitude is typically described as low, medium, or high corresponding to the financial impact of the compromise.

The exercise of analyzing the value or impact of asset loss can help determine which assets should undergo risk assessment.

It's important to consider the business impact of a compromise in absence of controls to avoid the common mistake of assuming that a compromise could not take place because the controls are assumed to be effective. The exercise of analyzing the value or impact of asset loss can help determine which assets should undergo risk assessment. This step is mostly the responsibility of the business team, but technical representatives can profit by hearing the value judgments of the business.

The output of this step is a document (typically a form) that describes the business impact in monetary terms or, more often, a graded scale for compromise of the confidentiality, integrity, and availability of the asset.

3. Identify threats

Identify the various ways an asset could be compromised that would have an impact on the

The Value of Formal Assessments

A thorough analysis of risk helps justify security spending

Formal, methodical risk analysis allows organizations to reason about the magnitude of business risk given the value of the system or information at risk, a set of threats, and a set of security controls like authentication, firewalls, and monitoring. The magnitude of the risk is a function of the degree of damage or loss that would occur if the threat is realized and the likelihood of the realization of the threat. This kind of thoughtful and objective approach not only helps to meet regulatory requirements, but also provides a practical way to manage security expenditures.

The value of assessing risk in this manner is that it transforms risk discussion from a conversation among technical people into a one relating technical vulnerabilities and controls to business impact. The process requires technical and business representatives to come to an understanding of what the business risk is and how it relates to technical risk. It also facilitates the economic discussion of whether investments in technology and processes are justified by the damage that may result from an attack or incident and the likelihood of the event. In short, it steers organizations away from being held hostage by the fear mongers or being starved for security investment by business people who do not appreciate the dangers posed by insufficient security controls. ›

–RICHARD E. MACKEY, JR.

business. Threats involve people exploiting weaknesses or vulnerabilities intentionally or unintentionally that result in a compromise. This process typically starts at a high level, looking at general areas of concern (e.g., a competitor gaining access to proprietary plans stored in a database) and progressing to more detailed analysis (e.g., gaining unauthorized access through a remote access method). The idea is to list the most common combinations of actors or perpetrators and paths that might lead to the compromise an asset (e.g., application interfaces, storage systems, remote access, etc.). These combinations are called threat scenarios.

The assessment team uses this list later in the process to determine whether these threats are effectively defended against by technical and process controls. The output of this step is the list of threats described in terms of actors, access path or vector, and the associated impact of the compromise.

4. Investigate vulnerabilities

Use the list of threats and analyze the technical components and business processes for flaws that might facilitate the success of a threat. The vulnerabilities may have been discovered in separate design and architecture reviews, penetration testing, or control process reviews. Use these vulnerabilities to assemble or inform the threat scenarios described above. For example, a general threat scenario may be defined as a skilled attacker from the Internet motivated by financial reward gains access to an account withdrawal function; a known vulnerability in a Web application may make that threat more likely. This information is used in the later stage of likelihood determination.

This step is designed to allow the assessment team to determine the likelihood that a vulnerability can be exploited by the actor identified in the threat scenario. The team considers factors such as the technical skills and access necessary to exploit the vulnerability in rating

the vulnerability exploit likelihood from low to high. This will be used in the likelihood calculation later to determine the magnitude of risk.

5. Analyze controls

Look at the technical and process controls surrounding an asset and consider their effectiveness in defending against the threats defined earlier. Technical controls like authentication and authorization, intrusion detection, network filtering and routing, and encryption are considered in this phase of the assessment. It's important, however, not to stop there. Business controls like reconciliation of multiple paths of transactions, manual review and approval of activities, and audits can often be more effective in preventing or detecting attacks or errors than technical controls. The multidisciplinary risk assessment team is designed to bring both types of controls into consideration when determining the effectiveness of controls.

Business controls like reconciliation of multiple paths of transactions, manual review and approval of activities, and audits can often be more effective in preventing or detecting attacks or errors than technical controls.

At the conclusion of this step, the assessment team documents the controls associated with the asset and their effectiveness in defending against the particular threats.

6. Calculate threat likelihood

After identifying a particular threat, developing scenarios describing how the threat may be realized, and judging the effectiveness of controls in preventing exploitation of a vulnerability, use a "formula" to determine the likelihood of an actor successfully exploiting a vulnerability and circumventing known business and technical controls to compromise an asset.

The team needs to consider the motivation of the actor, the likelihood of being caught (captured in control effectiveness), and the ease with which the asset may be compromised, then come up with a measure of overall likelihood, from low to high.

7. Calculate risk magnitude

The calculation of risk magnitude or residual risk combines the business impact of compromise of the asset (considered at the start of the assessment), taking into consideration the diminishing effect of the particular threat scenario under consideration (e.g., the particular attack may only affect confidentiality and not integrity) with the likelihood of the threat succeeding. The result is a measure of the risk to the business of a particular threat. This is typically expressed as one of three or four values (low, medium, high, and sometimes severe).

This measure of risk is the whole point of the risk assessment. It serves as a guide to the business as to the importance of addressing the vulnerabilities or control weaknesses that allow the threat to be realized. Ultimately, the risk assessment forces a business decision to

treat or accept risk.

Anyone reading a risk assessment method for the first time will probably get the impression that it describes a clean and orderly process that can be sequentially executed. However, you'll find that you need to repeatedly return to earlier steps when information in later steps helps to clarify the real definition of the asset, which actors may be realistically considered in a threat scenario, or what the sensitivity of a particular asset is. It often takes an organization several attempts to get used to the idea that circling back to earlier steps is a necessary and important part of the process.

WHICH FRAMEWORK IS BEST?

Over the years, many risk frameworks have been developed and each has its own advantages and disadvantages. In general, they all require organizational discipline to convene a multi-disciplinary team, define assets, list threats, evaluate controls, and conclude with an estimate of the risk magnitude.

OCTAVE, probably the most well known of the risk frameworks, comes in three sizes. The original, full-featured version is a heavyweight process with substantial documentation meant for large organizations. OCTAVE-S is designed for smaller organizations where the multi-disciplinary group may be represented by fewer people, sometimes exclusively technical folks with knowledge of the business. The documentation burden is lower and the process is lighter weight.

One of the benefits of the OCTAVE series is that each of the frameworks provides templates for worksheets to document each step in the process.

The latest product in the OCTAVE series is Allegro, which has more of a lightweight feel and takes a more focused approach than its predecessors. Allegro requires the assets to be information, requiring additional discipline at the start of the process, and views systems, applications, and environments as containers. The scope of the assessment needs to be based on the information abstraction (e.g., protected health information) and identify and assess risk across the containers in which the information is stored, processed, or transmitted.

One of the benefits of the OCTAVE series is that each of the frameworks provides templates for worksheets to document each step in the process. These can either be used directly or customized for a particular organization.

The NIST framework, described in NIST Special Publication 800-30, is a general one that can be applied to any asset. It uses slightly different terminology than OCTAVE, but follows a similar structure. It doesn't provide the wealth of forms that OCTAVE does, but is relatively straightforward to follow. Its brevity and focus on more concrete components (e.g., systems) makes it a good candidate for organizations new to risk assessment. Furthermore, because it's defined by NIST, it's approved for use by government agencies and organizations that work with them.

ISACA's COBIT and the ISO 27001 and 27002 are IT management and security frame-

works that require organizations to have a risk management program. Both offer but don't require their own versions of risk assessment frameworks: COBIT has RISK IT and ISO has ISO 27005:2008. They recommend repeatable methodologies and specify when risk assessments should take place. The ISO 27000 series is designed to deal with security, while COBIT encompasses all of IT; consequently, the risk assessments required by each correspond to those scopes. In other words, risk assessment in COBIT—described in RISK IT—goes beyond security risks and includes development, business continuity and other types of operational risk in IT, whereas ISO 27005 concentrates on security exclusively.

ISO 27005 follows a similar structure to NIST but defines terms differently. The framework includes steps called context establishment, risk identification and estimation, in which threats, vulnerabilities and controls are considered, and a risk analysis step that discusses and documents threat likelihood and business impact. ISO 27005 includes annexes with forms and examples, but like other risk frameworks, it's up to the organization implementing it to evaluate or quantify risk in ways that are relevant to its particular business.

Organizations that do not have a formal risk assessment methodology would do well to review the risk assessment requirements in ISO 27001 and 27002 and consider the 27005 or NIST approach. The ISO standards provide a good justification for formal risk assessments and outline requirements, while the NIST document provides a good introduction to a risk assessment framework.

With practice, an organization can establish a methodology based on this approach. However, it is worthwhile to review the OCTAVE family and, in particular, the Allegro framework. Its focus on information, its forms and relatively lightweight approach (when compared to other OCTAVE methods) provides a good alternative to NIST and will allow an organization to build a customized method that meets its own requirements.

CONSISTENCY IS KEY

In the end, the most important aspect of choosing a framework is ensuring that the organization will use it. Auditors will seldom inspect the details of your risk assessment method, but will look at whether you have a systematic method and apply it regularly. It's an organization's prerogative to accept risks that are too difficult or expensive to mitigate. However, one can only accept risks that one understands. Consistent and repeatable risk assessments provide the mechanism to not only understand risk, but also to demonstrate to auditors and regulators that the organization understands risk.

Whether your goal is to simply achieve good security or also meet regulatory requirements, creating a risk assessment method based on a well-known framework is a good place to start.›

Richard E. Mackey, Jr. is vice president of consulting at SystemExperts, an information security-services firm. Send comments on this article to feedback@infosecuritymag.com.

CALL FOR NOMINATIONS

It's Time to Recognize the Industry's Best Security Professionals

Information Security magazine and SearchSecurity.com announce that nominations are open for the seventh annual Security 7 Awards. Find the nomination form at: http://www.surveygizmo.com/s3/462797/Security-7

Prestigious Industry Accolades

The honor roll of past Security 7 Award winners is a prestigious list of distinguished security practitioners and dignitaries, including Dorothy Denning, Gene Spafford, Michael Assante and Christofer Hoff. Since 2005, we've recognized the most innovative and stalwart security practitioners in the industry. It's time to do it again.

Seven Industries, Seven Winners

The Security 7 Award honors innovative security practitioners in seven vertical markets. We recognize the achievements and contributions of practitioners in the financial services, telecommunications, manufacturing, retail, government/public sector/non-profit, education and healthcare/pharmaceutical industries.

How to Nominate Your Peers

Do you know someone worthy of recognition? Nominate them by filling out the form. A panel of editors and industry experts will review the nominees and select our winners.

–MARK WEATHERFORD

2008 Security 7 Government winner

Former CISO for the states of California and Colorado and current CSO at the North American Electric Reliability Corporation (NERC)

INFORMATION SECURITY®

For more information, please visit our website: www.searchsecurity.com

Recognize the Security Industry's Best Today!

The Client Side

ATTACKS ON APPLICATIONS LIKE ADOBE READER AND JAVA REQUIRE EFFECTIVE AND TIMELY PATCHING OF USER SYSTEMS.

BY MICHAEL COBB

THE PERVASIVENESS OF Microsoft Windows has made it a favorite target for hackers for years, but client-side applications like Adobe Reader and Flash Player are even more ubiquitous – a fact that hasn't escaped criminals. Dangerous vulnerabilities turn up in Adobe products on a regular basis. But it's not just Adobe vulnerabilities that put systems at risk. Serious security flaws have been found in other common client-side applications, such as Java, Apple QuickTime, Mozilla browser extensions, and Opera widgets.

Microsoft and many large vendors now release security updates and patches to a known timetable, and Microsoft products like Office can be automatically patched using the Windows Automatic Update. However, patches for other common applications such as Adobe Reader, Firefox, and Java can't. Relying on end users to manually install these patches distributes the patching workload but in no way is this ideal as users can't be relied upon to get all the patches installed on a timely basis.

The timely patching of software vulnerabilities is critical to maintaining the operational availability and integrity of enterprise IT systems. Patching proactively prevents the exploitation of vulnerabilities but the failure to keep application software patched is one of the most common reasons why hackers are successful. Most major attacks in the past few years have targeted known vulnerabilities for which patches already existed. Although many organizations are competent at keeping their critical servers patched, the same level of attention isn't given to their users' desktops and laptops, even though statistically this is where most vulnerabilities occur.

According to vulnerability research company Secunia, the average computer needs about 76 patches per year from 22 different software companies. The logistics involved in keeping this number of applications patched is one of the reasons many applications remain unpatched. Read on for insight into how enterprises can manage the security of client-side applications and integrate fixes into existing vulnerability management programs.

STANDARD BUILD

The single most effective method of improving patch management of client-side applications is to implement a standard build for desktops and laptops. A standard build will satisfy the vast majority of an enterprise's workforce and will help improve overall security. It reduces day-to-day maintenance and support costs, the number of different vendor alerts to follow and patches to test and deploy, and reduces the cost and time and overall burden of patch management. If every PC is configured differently, it becomes impossible to test patches on every permutation, leading to roll out problems and increased downtime.

Some employees will need non-standard applications and configurations but this should be the exception not the rule. An application whitelist and controls to prevent users loading their own software will help control the number of applications you have to manage. To ensure non-standard machines are correctly maintained and patched, an up-to-date register of hardware and software should be established, recording installed applications, version information and all patches installed. If this register doesn't exist, Nmap is a free tool that can quickly gather this information. Each machine should be grouped both by function, configuration and network location and assigned a priority level. This helps to quickly identify which systems are most at risk to a particular vulnerability.

Even with standardization, most businesses will still need to support a variety of applications from multiple vendors.

AUTOMATED TOOLS

To avoid the risky situation of unpatched machines on the network, most enterprises need to use an automated tool that pushes patches for different applications from different vendors from a central point. One such tool is Secunia's Corporate Software Inspector (CSI). Its Network Appliance Mode enables you to setup a CSI Agent as a remote-controlled dedicated scan engine, capable of automatically scanning complete network segments at scheduled intervals.

It can identify about 13,000 applications from 2,300 companies on any network connected machine, providing a complete software asset register, listing all the programs and plug-ins installed on each machine and whether they're patched and up-to-date. The enterprise version allows you to automatically repackage a large number of patches from different vendors for direct deployment using groups and configurations from Microsoft's Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM).

Application patch status is checked by comparing installed programs against Secunia's Vulnerability Intelligence database. The breadth and depth of this database means it can produce very accurate and detailed status reports, including criticality ratings for each insecure program along with detailed information about why it's insecure. It shows the full installation path, version details, and direct links to patches and Secunia Advisories which provide additional details and metrics about the vulnerability as well as other useful information for alternative mitigation strategies.

Reports can also be used to verify that patches have been properly applied, old insecure versions have been removed and to track the installation of non-approved applications, which is great for audit and compliance reports. It even lists end-of-life programs. Software which has reached end-of-life should not be used due to a lack of vulnerability information and the end of the vendor's commitment to providing security updates.

Other automated tools include Desktop Central, which supports managing both Microsoft and non-Microsoft patches as well as pushing standardized application configurations to Windows machines on the network. It automatically identifies the new and latest updates, identifies the systems that need them and installs them. ManageSoft Security Patch Management provides a similar service, distributing and installing patches to Windows, Linux, UNIX, and Mac machines. It's important to note that any central patch management server needs hardening and protecting against malicious attack to prevent it being used as a tool to distribute malicious code.

When considering an automated system, you need to ensure that it can patch and update the software applications in use within your organization.

When considering an automated system, you need to ensure that it can patch and update the software applications in use within your organization. How it handles rollbacks of troublesome patches and tracks implemented patches for audit purposes are also important features to provide assurance that vulnerabilities have been identified and appropriate patches have been installed. Enterprise patch management tools are less efficient when unique deployments have to be managed, which is another reason why standardization is good idea.

PATCH PRIORITIZATION

Knowing which patches to install and when is another key element of good patch management. When a patch is released, attackers immediately try to reverse engineer it to identify the

vulnerability and develop exploit code. This means the risk of attack increases immediately after the release of a patch due to the time lag in obtaining, testing, and deploying it. Vulnerability criticality ratings are an important aid to help you prioritize your patch process and accepted practice is to concentrate efforts on patches rated as critical and leave the others until a more convenient time. However according to CERT, hackers are now starting to focus on vulnerabilities with lower ratings because they know it's likely that the relevant patches won't necessarily be installed so quickly.

This complicates the process of patch prioritization and is why a risk-based approach is so important. All patches applicable to your software need to be recorded, but the first check is to see if it is relevant to your environment: Does it correct a vulnerability or problem in an application as it is being used within your organization? For example, if your organization disables browser scripting languages, then applying patches that fix scripting languages vulnerabilities is not a priority. Other security controls may also automatically mitigate certain threats, again reducing the urgency to apply certain patches. If the vulnerability does put the organization at risk, prioritize the patch by evaluating the impact it would have if exploited; for example, unauthorized system access, information confidentiality, arbitrary code execution, or denial of service.

A virtual test lab is essential for the efficient testing of patches on different platforms and configuration.

If the overall degree of risk is not acceptable, then you must either apply the patch or pursue non-patch remediation; assume that exploit code is available for any vulnerability for which there is a patch. The next step is to determine whether the fix will affect the functionality of other software applications or services through research and testing. Testing should be performed on a selection of systems that accurately represent the configuration of the systems in deployment, since so many possible system configurations exist that a vendor can't possibly test against all of them. Check that all related software still operates.

A virtual test lab is essential for the efficient testing of patches on different platforms and configuration. It greatly reduces your investment in hardware, space, and general overheads. It also means local administrators don't have to duplicate patch testing on their particular systems as they can all be replicated in the test lab.

VIRTUAL PATCHING

If applying a patch will impact business processes, you will need to agree to an appropriate time for patch installation and necessary downtime with system owners. When patch deployment has to be delayed, it may be possible to for some other compensating controls to be put in place. Known as virtual patching, changes such as a new firewall rule can eliminate the vulnerability by controlling inputs or outputs from the affected application; even the temporary removal of the application may be a sensible temporary option.

However, certain client-side applications and plug-ins, such as Adobe Reader, are going

to be difficult to do without. In such instances, look for other ways of thwarting any potential exploits. For example, most users will not be inconvenienced if executable code embedded in a PDF document is disabled. Disabling JavaScript within Adobe will help prevent some of the more common exploits and you can still read a PDF document without JavaScript enabled. Many attacks can be successfully frustrated by ensuring that your users aren't logged on to their system with unnecessary elevated privileges; the majority will not need to have administrator rights on their desktop. This makes it a lot harder for an attacker to take complete control or cause widespread damage. Local administrators need to be informed of all vulnerability and remediation decisions.

PATCH DEPLOYMENT

Change management procedures should always be used when deploying patches as systematic and documented processes are far more likely to result in a successful install. Even emergency patches need to go through this change control process. Budgeted and approved resources, such as off-hours testing and overtime need to be in place to make sure that they can be handled with the necessary priority. Manual methods may need to be used for operating systems and applications not supported by automated patching tools, such as experimental systems or those not part of Active Directory or a domain. For such computers, there should

Java Exploits on the Rise

Cisco researchers say criminals now prefer Java over PDF.

Criminals last year began targeting Java more heavily than PDF to launch exploits, according to researchers at Cisco Systems.

According to the Cisco 2010 Annual Security Report, Java exploits made up 1.5 percent of Web malware blocked by Cisco ScanSafe in January 2010. By November, that number jumped to 7 percent. In comparison, PDF exploits dropped from slightly more than 6 percent to just 2 percent in the same time frame.

Cisco researchers surmise that the shift has to do with a number of factors, including increased availability of public Java exploit code and decreased availability of public Adobe Reader and Adobe Acrobat exploits. Some users also have shifted to other PDF readers or disable JavaScript in Reader.

The Blackhole, Crimepack and Eleonore exploit software packages make heavy use of Java, according to Cisco, which notes that Adobe Reader and Acrobat remain strong threat vectors online.

McAfee Labs, however, said malware developers heavily exploited weaknesses in Adobe products–Flash and particularly PDF technologies–throughout 2010. Malicious PDFs targeting Acrobat topped the number of unique samples collected by McAfee Labs, "making them the favorite target of client-side exploitation," the company said in its Q4 2010 Threat Report. The company expects the trend to continue this year as more mobile devices and non-Microsoft operating systems support Adobe technologies.› –MARCIA SAVAGE

be written and implemented procedures for the manual patching process.

Even with standardized configurations and after thorough testing, it's still best practice to roll out patches to a small user group first before deploying them enterprise-wide. This allows user feedback and keeps disruption to a minimum if the patch does cause a problem for some unforeseen reason. Patches should certainly be deployed to standardized systems first before updating nonstandard and legacy machines.

Post roll out tasks include verifying the patch installed properly by reviewing patch logs, checking that the vulnerability has been mitigated using a vulnerability scanner, updating configuration documentation, and documenting the decisions behind installing or rejecting specific patches.

Even with automated technologies in place, system administrators still need to subscribe and follow vendor alerts, vulnerability announcements, patch and non-patch remediations, and emerging threats. Relevant Internet forums, such as those offered by CERT, are also a great source of warnings of patch installation problems and problem solving advice. As with any security function, organizations need to measure the effectiveness of their patch and vulnerability management efforts, basically how quickly they can identify, classify, and respond to a new vulnerability and mitigate the potential impact within the organization. This helps highlight any shortcomings in procedures or tools.

DIPLOMACY REQUIRED

Keeping enterprise users' machines secure is a tough task, given the relentless attacks on client-side applications like Adobe Reader and Java. Implementing effective patch management for user systems requires both technical and diplomatic skills. Getting business managers to accept that it is a regular business activity and not an optional one requires senior management support. Done well, it reduces the time and money spent responding to security breaches and helps protect the enterprise from legal and regulatory fines. Patching is much more cost-effective than responding to breaches; it's not possible to save money by neglecting patches.

Any opportunity to highlight the role patching plays in protecting the bottom line should not be missed as manual patching of computers is getting harder to do effectively. Even moderate-sized organizations need a budget for a vulnerability scanner and an automated patching tool to make the process as effective and painless as possible for everyone.

Michael Cobb, CISSP-ISSAP, CLAS, is a renowned security author with more than 15 years of experience in the IT industry. He is the founder and managing director of Cobweb Applications, a consultancy that provides data security services delivering ISO 27001 solutions. He co-authored the book IIS Security *and has written numerous technical articles for leading IT publications. Send comments on this article to feedback@infosecuritymag.com.*

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

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

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

Check out The Academy Pro at
www.theacademypro.com

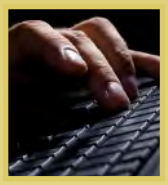
the academy pro

Sponsored by:

www.theacademypro.com

COMING IN APRIL





Cloud Security

Before undertaking any cloud computing initiative where data and network infrastructure interacts with the cloud, it's critical that security managers insist on an audit of network security. You'll learn about processes and tools to audit your network infrastructure for vulnerabilities and configuration errors that could put data at risk as it moves between your network and the cloud.

Application Whitelisting

Enterprise frustration with antivirus is growing as malware continues to slip past antivirus signatures. One option that is being revived is an old concept—application whitellisting. This article will look whether it really is a viable alternative for businesses and best practices.

Incident Response Planning

Enterprises spend copious amounts of time developing security policies and processes to prevent breaches and data loss. However, they often fail to complement their prevention efforts with an incident response plan. This feature will describe the basics of incident response, who needs to be involved, whether it can be bought and how to evolve it over time.

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.

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 7

- **Entrusting Endpoints**
- **Guarding the Gateway**

See ad page 19

- **The Essential Guide to Mitigating Risk and Optimizing Your Enterprise**

See ad page 10

- **IT Audit, Security, Governance and Risk Certifications**
- **Get Certified - Register Here**

- Mad Security, inc.
- Milestone Systems, inc.

See ad page 13

- Identity Governance Buyer's Guide Second Edition

See ad page 4

- Trend Micro Deep Security 7.5 vs. McAfee and Symantec
- How Security is Changing to Support Virtualization and Cloud Computing

See ad page 27

- **Compare WatchGuard head to head with all other major brands**
- **See how Data Loss Protection can help your business avoid embarassing situations**