[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. March 2012 * SPECIAL

RSA® CONFERENCE 2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

SECURITY AS A SERVICE

NOW AVAILABLE AT A BROWSER NEAR YOU

Software-as-a-Service (SaaS) has been described as the most disruptive delivery model to ever face the enterprise software market for one simple reason: ***it works***

Qualys is the first company to deliver an on demand solution for security risk and compliance management. QualysGuard® is the widest deployed security on demand platform in the world, performing over 150 million IP audits per year — with no software to install and maintain.

For a free trial, go to a browser near you.

www.qualys.com/SaaSTrial

TABLE OF CONTENTS

Below is an index of companies featured in this issue, along with the page number.

Every year it's the same - as I take the short ride on the large mobile staircase of the Moscone Center, I can feel the excitement in the air as another RSA Conference opens its doors.

This year's most important gathering of information security professionals was the best I've attended in the past decade. While talking to colleagues and exhibitors, I realized I was not the only one with such a positive feeling. You could feel a lot more people at the conference, and the show floor was booming.

What you have before you is the first special issue of (IN)SECURE Magazine, and what better topic than the biggest infosec show on the planet?

Mirko Zorz
Editor in Chief

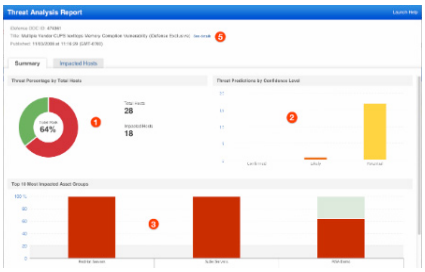
Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - mzorz@net-security.org
News: Zeljka Zorz, Managing Editor - zzorz@net-security.org
Marketing: Berislav Kucan, Director of Operations - bkucan@net-security.org

Distribution

0-day risk analysis service by Qualys



Qualys launched Zero-Day Risk Analyzer, a new service to help companies protect their IT systems against zero-day attacks which is delivered as part of the QualysGuard Cloud Platform and it includes Verisign's iDefense zero-day vulnerabilities and global threats.

The service allows customers to analyze zero-day threats and estimate their impact on their assets and critical systems based on information collected from previous scan results.

"Zero-day attacks are becoming more prevalent and such attacks can happen to any of us," said Philippe Courtot, chairman and CEO of Qualys.

"With this new service, we provide customers a proactive solution to estimate the impact of such critical threats on their assets and decide what mitigating controls to put in place until real patches are available," he added.

The true state of cloud security

Alert Logic released its first State of Cloud Security Report, a semi-annual quantitative analysis comparing real world security incidents observed in hosted and cloud environments with those observed in traditional on-premise environments.

Counter to the conventional wisdom that infrastructure in service provider managed cloud environments is inherently less secure, the analysis found these environments tend to face a lower level of risk than on-premise environments.

Kevin Mitnick presenting to a large crowd at the Qualys booth.

CSA launches mobile and innovation initiatives

The **Cloud Security Alliance** announced two significant new initiatives for 2012, addressing growing areas of need in cloud security – mobile computing and innovation.

The initiative will comprise both a working group within the CSA, as well as a for–profit entity working with innovators and other stakeholders. Innovators can develop relevant solutions with or without CSA assistance, and then request that the CSA-II working group assesses the value of the solution within the community. The CSA-II working group will also recommend resources to innovator, to help meet the challenges mentioned above.

Automated encryption for cloud storage

Sophos announced the latest version of its data protection solution, SafeGuard Enterprise, which offers the industry's first enterprise cloud encryption capabilities, protecting critical data in public, private and hybrid cloud environments.

SafeGuard Encryption for Cloud Storage automatically encrypts files uploaded to the cloud from any managed endpoint. This simple process requires little more than choosing a password, which allows secure file access from anywhere – thereby improving collaboration and increasing productivity.

SafeGuard FileShares uses central keys to give access to files for authorized users or groups, while keeping these files encrypted for everyone else. More importantly, SafeGuard ensures that all files remain encrypted regardless if copied or moved to another drive, network or device.

Eliminating malware resident on file shares

FireEye announced its File Malware Protection System that detects and eliminates advanced malware found on file shares. The solution prevents the lateral spread of malicious code into central data stores and addresses the security weaknesses introduced by Web-based email, social networking, online file transfer tools, personal storage devices and other manual means that bring files into the network.

The File MPS extends the FireEye security platform to protect companies and federal agencies from another key stage of an advanced targeted attack.

Software sensor for wireless intrusion detection

Fluke Networks announced a new version of its WLAN security and performance monitoring solution, AirMagnet Enterprise, Version 10, which offers a Software Sensor Agent (SSA), allowing customers to use both software and hardware sensors to optimize cost, deployment and security monitoring needs.

With Fluke Networks' new software-based option, organizations can now turn any Windows-PC into a software-based WLAN sensor.

This deployment option allows network professionals to choose between standard hardware sensors, which are the core technology for monitoring WLANs, and a software alternative for multi-site healthcare, retail and concession operations needing basic PCI or HIPAA compliance monitoring.

The new software sensor is one of several new capabilities included in the new version, which also includes new performance monitoring and WLAN platform support.

Hugh Thompson, RSA Conference Program Committee Chair hosting Innovation Sandbox.

Transformable security engine from Stonesoft

Stonesoft introduced the Stonesoft Security Engine, a transformable security engine that is capable of delivering seven enterprise-class product configuration modes to provide contextually-aware security capabilities.

It is a security solution that can be configured to act as a traditional and/or next generation firewall, traditional and/or next generation intrusion prevention systems, layer-2 firewall, VPN or UTM product. The solution is delivered through one integrated technology platform and managed through a single management center.

Eradicating malware from enterprise web sites

Qualys announced a new service to help enterprises detect and eradicate malware from their web sites.

Delivered as part of the QualysGuard Cloud Platform and suite of integrated applications for security and compliance, the new Enterprise Edition of the QualysGuard Malware Detection Service allows businesses to proactively scan their web properties for malware infections, receive automated alerts and create in-depth reports for identification and removal of malware from these web sites.

Information security within emerging markets

by Brian Contos

Throughout my career I've been fortunate enough to work all over the world. I've pretty much been everywhere in North America a dozen times, and close to the same in Western Europe and Northern Asia. Over the last few years my focus has shifted to emerging markets – particularly in Latin America, South East Asia, Africa, and the Middle East. From a business perspective, regardless of the geography, population, economic maturity, and political stability, there are always a few verticals that invest in information security proactively.

Government, telecommunications, and financial services exist in virtually every country and are motivated to embrace information security. Other verticals which may or may not be administered by governments and invest in information security include critical infrastructure such as power and energy, healthcare, and various forms of manufacturing. Of course there are other types of businesses that invest in information security within emerging markets, but it has been my experience that these are the most proactive.

Threats

The threats confronting organizations within emerging markets are similar to those faced in the United States, Germany, and Japan: malicious and careless insiders, opportunistic attacks such as automated botnets and random malware, and targeted attacks for political or financial gain.

These targeted attacks are often focused on intellectual property (IP). The attacks sometimes make use of malicious insiders that are planted or recruited and can severely hamper investment, innovation and competition.

Protecting sensitive data in a country where IP laws don't exist or are poorly enforced yields great opportunity for those with nefarious intent and increases the risks associated with foreign and domestic investment.

The United States publishes the Special 301 Report which is an annual review of the global state of IP rights protection and enforcement. Countries like Mexico and Russia have very positively enacted legislation to address these issues, while countries like Chile and Indonesia are still struggling and as such are on the report's Priority Watch List.

When attacks are perpetrated by nation-states, they can have a macro level impact on national security and economic stability. Some examples include the 2007 conflict between Estonia and Russia and the 2008 conflict between Georgia and Russia. In both examples there where non-kinetic attacks, i.e. cyber attacks. It is suspected that the Russian military received a force multiplier when sympathizers around the world launched cyber attacks in support of Russia. In conjunction with the non-kinetic attacks, kinetic warfare, i.e. armed troops and military vehicles were also used.

These attacks demonstrated one of few examples of the convergence of non-kinetic and kinetic warfare.

There have been several cases where electric power generation and transmission has been the target of extortion.

Financially motivated organized cyber criminals can also wreak havoc on emerging markets. There have been several cases where electric power generation and transmission has been the target of extortion.

A study titled "In the Dark: Crucial Industries Confront Cyberattacks" was released by the Center for Strategic International Studies in cooperation with McAfee. Of the executives surveyed, 80 percent of respondents in Mexico and 60 percent in India stated that their electric infrastructure had been a target of extortion with threats of cyberattacks.

Trends

Like threats, trends in IT within emerging markets aren't disparate from the trends in other regions. For example, there is broad adoption of mobile devices, especially in countries that haven't previously made substantial investments in traditional telephone systems. In fact in India, more people have mobile phones than regular access to toilets.

Social media is big around the world. If Facebook were a country, with 800 million plus users, it would be the third largest country in the world after China and India. But there are other social media sites that are also extremely large like Renren for China, Orkut for Brazil, Cyworld for Vietnam and other parts of Asia, Badoo for Russia, and hundreds of others.

Because of limited and legacy IT infrastructure and supporting resources, virtualization is popular trend. When I was in Costa Rica I saw the use of desktop virtualization as a method to achieve greater ROI from endpoints like laptops that may have been ready for end-of-life. The virtualization of applications, and servers brings tremendous advantages for organizational efficiency, consolidation, manageability, security, and reduced power consumption.

Cloud capabilities are also relevant - especially Security SaaS that can be used across a number of areas such as endpoint, email, web, and network. When I visited the Philippines it was clear that organizations were looking to cloud services to help save time, effort, costs, and realize faster time-to-protection with Security SaaS.

Workforce

Many countries lack the technically savvy workforce and educational opportunities to address the threats and trends outlined above. When I was working in Peru, I noticed that there were limited opportunities for technology-focused education; therefore Peru has a small pool of technically savvy workers.

This slows Peru's ability to embrace industries that require a higher level of technical sophistication. This is an all too familiar story in emerging markets where there is a simple lack of qualified workers to build and operate IT

security controls necessary to combat today's threats and enable business by embracing new trends.

Regulatory mandates

Many emerging market countries lack the government-enforced regulatory mandates that are valuable for creating a minimum baseline for information security practices and an enforcement mechanism through audit.

I was pleasantly surprised in Mexico and South Africa when I discovered they have a heavily regulated financial services industry designed to combat corruption and other forms of abuse. As such, their regulatory mandates have matured organically and are crossing into other business verticals.

Infrastructure

When confronted with the challenges of maintaining and upgrading underlying infrastructure, information security can often be deprioritized. I've been to several countries where power outages are a common occurrence. In Sao Paulo, Brazil and Bangkok, Thailand the streets flood because of heavy rains and a lack of sufficient storm drains, so the roads, and therefore the cities, pretty much shut down. When visiting a telecommunication firm in Malaysia I discovered power lines that pre-dated shield wiring and were wrapped in cloth. My mobile and Internet service in Costa Rica was unpredictable at best with connectivity blackouts lasting hours.

Doing more with less

Emerging markets are truly the poster children for doing more with less. These countries face similar threats and trends as other countries. However, in many cases they have less reliable infrastructure, limited government regulatory mandates, and a smaller pool of skilled laborers.

They need to protect their intellectual property, attract investment, keep the lights on, and defend from attacks that might threaten national security and economic stability. This has to be accomplished while embracing trends in mobility, social media, virtualization, and the cloud. Organizations in these countries require a more holistic, agile, and connected approach to security.

Gone are the days of silos where each problem required a separate technical solution existing in a vacuum. Organizations within emerging markets can't scale when there is a requirement for so many disparate products – each requiring their own agents, consoles, servers, databases, licensing, support, training, administrators and so on, across endpoint, network, and data controls.

The cost and complexity is simply too great as there are no resources to address security in this older, and flawed paradigm of information security.

A connected security framework that is dependent on a fewer number of disparate vendors is needed.

These solutions should enrich each other – that is – endpoint controls should improve network controls and together they should enhance data controls. This will reduce risk by creating greater efficiencies around key areas of information security such as discovery, protection, detection, response, management, and audit. It will also provide a more agile, rapid and willing framework for embracing new trends.

Brian Contos, CISSP, is senior director, vertical & emerging market solutions at McAfee. He has nearly two decades of security experience, is the author of several books, and has worked with government organizations and Forbes Global 2000 companies throughout North, Central and South America, Europe, Africa, the Middle East, and Asia.

Authentication Advanced

Entrust offers many of the most advanced mobile authentication solutions on the market. And each is managed on the versatile Entrust IdentityGuard strong authentication platform.

Security Everywhere

Entrust brings identity-based security and authentication to smartphone and tablet platforms, including Apple iOS, RIM BlackBerry, Google Android and Microsoft Windows Mobile.

One Platform

Whether you need mobile soft tokens, physical and logical access, device certificates, or eGrid authentication, Entrust IdentityGuard is the comprehensive manangement platform.

SECURITY ON : Mobile

Visit entrust.com/mobile-security

Entrust.com 888.690.2424 entrust@entrust.com

Entrust®
Securing Digital Identities & Information

A platform to stop APTs and malware

Bit9 announced the Bit9 Advanced Threat Protection Platform that protects all enterprise endpoints, servers and private clouds from cyber-attacks that bypass older antivirus and behavioral security solutions. The platform stops advanced persistent threats as well as dangerous malware and protects enterprises against intellectual property theft. "The largest unsanctioned transfer of intellectual property in history is occurring right now," said Patrick Morley, President and CEO of Bit9.

"As companies increasingly rely on their IP to give themselves a competitive advantage in the global marketplace, nation states, hacktivists and cybercriminal groups are making trade secrets and other proprietary information a prime target."

RSA enhances its threat intelligence delivery platform

RSA announced that RSA NetWitness Live service now provides 30 percent more threat content, customized content distribution capabilities and new integration with RSA's analytics platforms.

The RSA NetWitness Live service is a cloud-based 24x7 threat intelligence delivery platform that is engineered to aggregate, analyze and spotlight the most relevant security content from approximately 100 trusted sources, including insights derived from RSA's proprietary threat research.

Detection and securing of built-in passwords

Lieberman Software announced that the company's privileged identity management product, Enterprise Random Password Manager, now offers a solution to identify known, built-in administrator passwords in the network.

The new "known password discovery" feature scans the network, detecting and securing default and well-known privileged logins that make it easy for unauthorized individuals and malware to gain control of sensitive data.

Desktop isolation technology for secure browsing

OPSWAT announced the launch of Secure Virtual Desktop, a desktop isolation solution that protects users and organizations from data loss by creating an isolated environment for accessing the web and working with sensitive data.

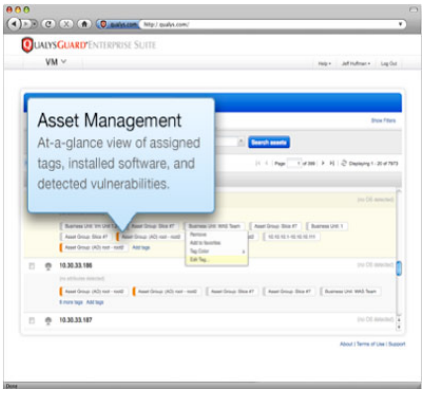
All traces of activities performed within the secure session, such as downloads, file revisions, cookies and browser history, are completely erased when the session ends, enabling data leak prevention even on public computers, hotel business centers and shared laptops.

Protection against malicious URLs and attachments

Building off of its approach to breach prevention which focuses on seamless delivery of untrusted content in secure virtual environments, **Invincea** now provides its commercial and government clients with the capability to capture and contain the primary attack vehicles used in spear phishing, poisoned search results, and user-initiated infections.

As a result, even the most well-crafted phishing attempts using zero-day malware are contained before they can successfully take root in the end-user system, preventing the adversary from infiltrating the network. Invincea solutions perform seamless delivery of untrusted content in secure virtual environments, a system which enables signature-free malware discovery, without risking system infection, while providing pre-breach forensic analysis feeds to inform and improve other defense mechanisms.

Automated managing of enterprise assets



Qualys announced the availability of hierarchical Dynamic Asset Tagging for its QualysGuard Cloud Platform and suite of applications for security and compliance.

The patent-pending technology enables customers to easily manage assets in any size environment with the scalability and flexibility to support millions of assets in large, highly dynamic enterprise environments.

QualysGuard Dynamic Asset Tagging automates the process of inventory management, and is seamlessly integrated with many workflows throughout the QualysGuard application.

Philippe Courtot, Qualys CEO, during his keynote.

Cloud-based targeted attack prevention

M86 Security announced its strategy to deploy its core malware and threat research capabilities for Web and email into the cloud, beginning with the launch of the company's new cloud-based Targeted Attacks Service in the M86 MailMarshal Secure Email Gateway (SEG).

The new blended threats technology protects organizations from targeted attacks that use malicious embedded URL links in emails as the initial infection method. M86 Security's Targeted Attacks Service scans emails for embedded URL links to potentially malicious websites as they are accessed.

Only 34% of businesses enforce encryption on removable devices

Imation revealed the results of a recent survey of 302 IT decision makers in the US and Canada, which say that 37 percent of them reported that their business had unintentionally exposed corporate data through theft or loss of removable devices in the past two years.

Despite this, only 34 percent enforce encryption on all removable devices allowed on their networks.

Cloud web application firewall by Qualys

Qualys unveiled its new QualysGuard WAF service for securing web applications.

The new service, delivered as part of the QualysGuard cloud platform and suite of integrated applications, provides protection against known and emerging web application threats. Additionally, the service provides increased web site performance through caching, compression and content optimization to subscribers.

The top ten finalists for the "Most Innovative Company at RSA Conference 2012" presented to a great crowd and a panel of judges.

Once again, the Innovation Sandbox proved to be one of the most interesting events at RSA Conference 2012, as ten creative companies got a moment in the spotlight to present their newly developed technologies to over a couple of hundreds of interested conference goers.

The companies were chosen from out of more than 50 submissions and after an informal talk with one of the judges, this year's competition was fierce.

The Innovation Sandbox started with the representatives of these ten companies having their five minutes on the stage to introduce their concepts. Cloud security was the hot topic, as half of the companies presented offerings in this arena.

After the presentations and a Q&A with the judges, the audience swarmed the booths in order to see detailed demos of the products in question. The turnaround was impressive and it was really tough to get a 1-on-1 with almost anyone from the exhibiting parties.

The winner of this year's title of the most innovative company at RSA Conference 2012 was Appthority. With their flagship product, the Appthority Platform, businesses can protect themselves against risks lurking behind mobile apps, including known and new malware used in targeted attacks, corporate data exfiltration, and intellectual property exposure.

“Recent issues in security continue to push the information security industry to think in new, innovative ways, and the top 10 finalists represent some of the best new solutions and brightest industry minds,” said Sandra Toms LaPedis, Area Vice President and General Manager of RSA Conference. “Appthority demonstrated they were the most innovative by demonstrating the ability to answer immediate and growing need for more effective application security in a mobile world."

SANS Secure Europe 2012 AMSTERDAM

Amsterdam, Netherlands | 5-19 May 2012

Largest European SANS Event of the Summer!

Offering 10 Hands-On Immersion Training Courses – Over Two Weeks

Three New Courses

– Foundations of Auditing Information Systems

– Virtualization and Private Cloud Security

– Mobile Device Forensics

NetWars – Tournament Play

Register at www.sans.org/secure-amsterdam-2012

5% discount to readers of (IN)SECURE Magazine

Enter the code **INSECMAGSSE12** when registering

The maxim “may you live in interesting times” is often quoted as an ancient Chinese curse, but whether you believe that the ancient Chinese actually coined this phrase or not, there's little doubt we live in rather interesting times as multiple trends in smartphones and mobile computing accelerate. They are coming together and converging into a “perfect storm” of mobile device users, technology, and criminals.

Technology, cost, capability, and popularity are fueling a rapidly expanding market for these new devices. They are also fueling trends in the criminal world which see these popular devices as feature-rich targets of high density, high value information to be exploited.

The trends around us

Smartphones started off as bulky, expensive, not very attractive items. They have decreased in size, becoming very stylish, highly portable devices while often sporting larger screens than their bulkier forerunners. This makes them more convenient and personal to the user but it makes them much more vulnerable to damage, loss, or theft.

One major factor in smartphone adoption has been the cost factor. The cost of existing technology has come down to the point where very inexpensive smartphones are competitive with many of the feature phones.

We've seen the introduction of faster dual core processors with more and more memory and should see more of the newer high-end devices sporting quad core processors this year.

Advances in mobile capabilities extend beyond just raw computing power. Newer capabilities are being added. Soon we'll see near-field communications (NFC) being added to phones for “tap and go” payment systems that could replace some credit card transactions.

In short, smartphones have become pocket supercomputers.

Another major trend with smartphones and tablets has been the rapid rise in thousands of very inexpensive or applications. A plethora of games such as Angry Birds and Words with Friends can be very addictive, making these "phones" must haves for young and old.

It's not just the consumer market where demand for these devices has been expanding. The last couple of years have also seen a rapid uptake in the business market with BYOD, or Bring Your Own Device.

Partly because smartphones have become so powerful, partly because they have been delivered by vendors burdened with a number of unwanted applications, and partly driven by the technology community's obsessive nature to "tinker," a rich grass-roots movement has evolved for modifying smartphones.

Individuals are now jailbreaking, or removing the application limitations on devices such as those running the iOS operating system; rooting, a process allowing users of mobile phones, tablet PCs, and other devices to attain system level privileges; and otherwise "modding" or modifying the operating system custom modified firmware (mod roms). The terms jailbreaking and rooting may sound ominous, but there are legitimate and desirable reasons why smartphone users are doing this.

This explosion in popularity, technology, applications, and capabilities has had the net result of concentrating more and more very personal and very sensitive information into a very small, powerful device. There are lots of avenues for getting at this information - casually being carried around on smartphones in these feature-rich targets of opportunity - and the criminals are well aware of them.

The last couple of years have also seen a rapid uptake in the business market with BYOD, or Bring Your Own Device.

Trends on the darkside

Malware writers have certainly taken notice of the popularity of the mobile platforms. Malware exists to exploit almost every platform and operating system but has had, so far, limited impact.

Malware can steal personal information, such as banking information, directly from the phone or may exploit premium SMS messaging services to bleed money from an owners account. In some cases, criminals have taken popular games or utilities and repackaged them as Trojanized applications, offering them on the market for free or with reduced prices. Previous criminal activity suggests this is only going to get worse.

Criminal activity is not just limited to malware on mobile devices, however. Obviously, the devices can be stolen but there are other tricks for accessing them. Mobile devices can often be accessed through their standardized micro USB ports to either steal information or inject damaging malware. In one interesting demonstration, malware from a rigged public charging station was injected into phones. In another case, exploits were demonstrated where smartphones could imitate USB mice and keyboards when plugged into larger computers.

One of the more interesting attack vectors is through QR (Quick Response) codes. These codes are the squarish 2D barcodes that have been popular in Asia and Europe for a while and are now appearing on billboards, in magazines and even on TV shows and commercials.

There have already been incidents of malicious QR codes on billboards and discussions of pasting them over legitimate QR codes, making them difficult to detect. They may also be delivered via SMS / MMS messaging or e-mail to a target's phone.

Trends to the rescue

Fortunately, there are major efforts underway to address these threats. Software companies

are delivering products for a wide range of security issues. Research is going on into virtualized isolated profiles for protecting enterprise data on employee phones. Some enterprise vendors are rolling out end-point control systems to remotely manage phones and configurations to ensure integrity.

App markets are taking more precautions in what sort of applications are available for sale or download. Google has now begun to scan the thousands of apps published in their market with a scanner called “Bouncer,” while Apple has always been cautious and restrictive of what is available from them.

These are all good things and the presence of security-focused applications is encouraging.

Conclusion

More must be done to protect the smartphone users from themselves. They need to know that these are not merely phones but are significant computing platforms. They need to protect themselves now with what's already available. They must understand the risks and the value of the data they have contained in these compact devices.

Users must avoid doing things that place them at risk and take precautions to protect themselves. Some of that is education, some of that is application, and some of that is just pure physical security – a lot depends on the individual.

Users should avoid downloading apps from untrusted sources. A free game may be tempting to a teen but may have an unwanted surprise for the parent. Even apps from trusted markets and sources should be carefully scrutinized.

Anti-virus software may be a choice for some but, certainly, some remote security from a trusted market is a must. There have been stories of people locating and tracking a lost smartphone from several states away using remote location applications and the smartphone GPS facilities.

When scanning QR Codes, the barcode reader app should always prompt the smartphone user with the data before taking action. Do not scan barcodes that look suspicious or appear to have been tampered with in any way.

Backups are as important as protecting the phone itself. This protects your data from loss if the phone is lost or stolen and needs to be wiped.

Ironically, people that jail-break, root, and mod-rom their phones may be less likely than others to be compromised. Given the free availability of tools to break phones, they are not less secure, but those who have root access on their phones have better security tools available in the app markets. And, there have been no significant attacks that have specifically targeted these users. However, it's not a good recommendation for the average person who is not technically savvy to attempt using these tools. While no broken phone is entirely secure, those with the technical skills can benefit from using security apps.

The enterprise must also be prepared to deploy security applications and tools on employee phones, whether the device is provided by the enterprise or provided by the individual. After all, it's the enterprise's data that is at risk. It should also be recognized that the smartphone security equation can not be isolated from the human factor. Different people in an organization are going to have different needs, abilities and vastly differing platforms.

All the trends point toward increasing capacity, capability, versatility, popularity, and information density among smartphones. They also point toward increasing threat, risk, and the need for efforts to protect their users. It is possible to avoid this perfect storm with common sense and the use of available security precautions.

Mike Warfield is a Senior Security Researcher and Threat Analyst for the X-Force Threat Analysis Team of IBM Security Systems. With computer security experience dating back to the early 1970s, Mike is responsible for doing research into security vulnerabilities and intrusion protection techniques.

Most executives don't pay attention to cyber risks

The advanced findings from the latest 2012 **Carnegie Mellon** CyLab Governance survey of how corporate boards and executives are managing cyber risks reveals the issue is still not getting adequate attention at the top.

One of the most important advance findings is that boards and senior management still are not engaging in key oversight activities, such as setting top-level policies and reviews of privacy and security budgets to help protect against breaches and mitigate financial losses.

Security for MySQL and Teradata databases

McAfee announced its new McAfee Database Activity Monitoring solution offering real-time protection for business-critical databases.

The solution enables organizations to achieve much greater security management efficiency through its incorporation into the McAfee ePolicy Orchestrator centralized security management platform.

We are at another inflection point, says Microsoft

At the RSA Conference 2012, Scott Charney, corporate vice president of **Microsoft** Trustworthy Computing, shared his vision for the road ahead as society and computing intersect in an increasingly interconnected world.

In a new paper, “Trustworthy Computing (TwC) Next,” Charney encouraged industry and governments to develop more effective privacy principles focused on use and accountability, improve end-to-end reliability of cloud services through increased fault modeling and standards efforts, and adopt more holistic security strategies including improved hygiene and greater attention to detection and containment.

Firewalls for service providers and carriers

Fortinet announced two additions to its next-generation firewall product family that are designed to meet the growing threat protection and IT infrastructure control requirements of large enterprises, service providers and carriers that provide complex, multi-tenant cloud-based services.

Designed from the ground up as a next-generation firewall that tightly integrates application control technologies with an intrusion prevention system, the FortiGate-3240C exerts granular control over more than 1,900 discrete applications and provides real-time protection against current and emerging Advanced Persistent Threats. The compact 2-RU format appliance delivers up to 40 Gbps of firewall throughput

Malware extraction and analysis

Solera Networks announced the latest enhancement to its DeepSee platform - the Real-Time File Extractor, which enables immediate, automatic identification and alerting of advanced and zero-day threats. In addition, by integrating with malware detection and analysis systems, the DeepSee platform enables organizations to leverage existing tools to respond faster and more accurately to attacks.

Full-disk encryption with wireless pre-boot authentication

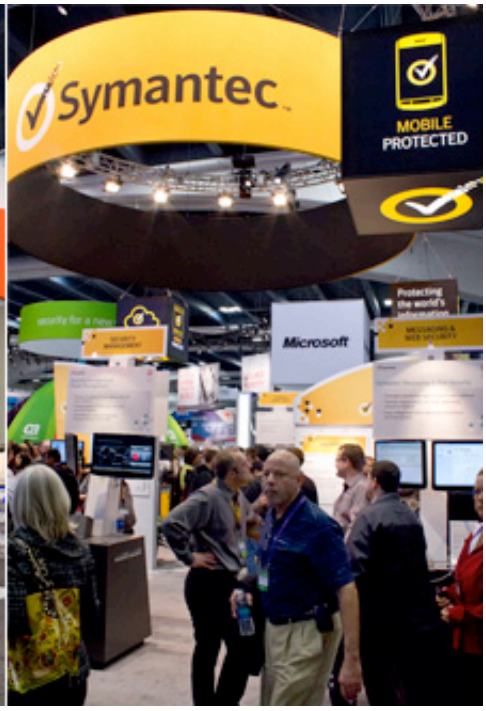
WinMagic launched SecureDoc Version 5.3, which adds wireless capabilities to its PBConnex pre-boot network authentication.

Enhancements include single sign-on support for PBConnex and Microsoft Active Directory accounts to enable faster boot log-in and security and support for the new Intel Anti-Theft 3.0 platform.

Software app kits for accelerating security apps

Netronome announced an upgrade to its Network Flow Management (NFM) software framework including new application kits for NGFW, IPsec, IPS and SSL inspection.

NFM provides a suite of production-ready reference software for the NFP-3240 network flow processors that accelerates a wide variety of cyber security applications to industry leading throughputs.



Turning mobile devices into enterprise credentials

Entrust is extending its Entrust IdentityGuard strong authentication platform to offer smart credentials on mobile devices for enterprise-grade security.

Taking advantage of NFC and Bluetooth standards, Entrust embeds biometrics and digital certificates on smartphones to create trusted identity credentials for stronger and convenient enterprise authentication.

Cloud-based security with embedded wireless access

Cybera announced the Cybera ONE Platform now delivers its full suite of cloud-based security services, as well as remote backup and recovery, over high-speed wireless 3G and 4G connections.

Cybera ONE delivers all the important network security services in a single cloud-based solution at a fixed annual cost.

Christopher Young, Senior Vice President, Security & Government Group, Cisco.

Non-profit org aims to solve Internet's security issues

The Trustworthy Internet Movement is a vendor-neutral organization with a mission to resolve major lingering security issues on the Internet, such as SSL governance and the spread of botnets and malware and to ensure that security is built into the very fabric of private and public clouds.

Founding principal and veteran of the information security industry Philippe Courtot, Chairman and CEO of **Qualys**, has personally pledged $500,000 in seed money to get the initiative off the ground.

"With two billion people relying on the Internet for much of their personal and business lives, it is incumbent upon the industry to put its collective heads together and resolve the problems of online security, privacy, and reliability once and for all," says Courtot. "This is no longer just an issue of technology but of society as a whole."

Are Hackers Finding a Way Into Your Network?

GFI LANguard

Award-winning vulnerability management software

To lower the security risk you need GFI LANguard, a solution that provides network vulnerability scanning, patch management and auditing in one integrated package. This award-winning solution allows you to scan, detect, assess and rectify vulnerabilities on your network faster and more effectively.

GFI

WEB & MAIL SECURITY
ARCHIVING & FAX
NETWORKING & SECURITY

Download your FREE trial version from **www.gfi.com/lannetscan/**

tel: +1 (888) 243-4329 | fax: +1 (919) 379-3402 | email: ussales@gfi.com | url: www.gfi.com/lannetscan/

RSA Conference announced the honorees of its 15th annual awards program. Award applicants were judged in the fields of mathematics, public policy and security practices.

Excellence in the Field of Mathematics Award

Eli Biham, Professor, Technion-Israel Institute of Technology, Computer Science
Dr. Mitsuru Matsui, Senior Researcher, Mitsubishi Electric Corporation

Professor Eli Biham and Dr. Mitsuru Matsui have both contributed groundbreaking work on the cryptanalysis of symmetric-key ciphers. Biham, a professor and dean of the Computer Science department at the Technion-Israeli Institute of Technology, co-discovered the technique of differential cryptanalysis with Adi Shamir in the late 1980's.

Dr. Matsui, inspired by Biham and Shamir's work, discovered the technique of linear cryptanalysis in 1993. The following year, he was the first to publicly report an experimental cryptanalysis of DES.

Excellence in the Field of Public Policy Award

Congressman Mac Thornberry (R-TX), Chair of the House Republican Task Force on Cyber Security

Mac Thornberry, a lifelong resident of the 13th District of Texas, has established himself as a leader in national security. In early 2011, Thornberry was tapped by the Speaker of the House and Majority Leader to spearhead a Cyber Security Task Force to guide House legislative action on the growing national security and economic threat. Charged with making recommendations in a number of areas including protecting critical infrastructure and sharing cyber security information, the Task Force released its recommendations on October 5, 2011 to favorable response from both sides of the House and the Senate, as well as the White House, private businesses and other outside organizations.

Excellence in the Field of Security Practices Award

Phil Agcaoili, Chief Information Security Officer, Cox Communications, Inc. and Cyber Security Committee Co-Chair of the FCC CSRIC

Phil Agcaoili has been a change agent and transformation leader in the Technology and Information Security industries for over 20 years and is the Chief Information Security Officer at Cox Communications. He has helped shape the direction of cyber security for US Telecoms through his appointment as the committee co-chair of the FCC CSRIC, and is helping to shape cyber security as a founding member of the NCTA Cyber Security Work Group. He is also guiding the direction of cloud computing as a founding member of the Cloud Security Alliance and as a co-inventor and co-author of the CSA Cloud Controls Matrix (CCM), GRC Stack, and STAR (Cloud Security Registry), and provides privacy and trust guidance as a Ponemon Institute Distinguished Fellow.

Lifetime Achievement Award

Martin E. Hellman, Professor Emeritus of Electrical Engineering, Stanford University

Martin E. Hellman is best known for his invention, with Diffie and Merkle, of public key cryptography. In addition to many other uses, this technology forms the basis for secure transactions on the Internet. He has also been a long-time contributor to the computer privacy debate, starting with the issue of DES key size in 1975 and culminating with service (1994-96) on the National Research Council's Committee to Study National Cryptographic Policy, whose main recommendations have since been implemented.

Prior to joining Stanford's faculty in 1971, Hellman was at IBM's Watson Research Center and served as an Assistant Professor of EE at MIT. Hellman received his B.E. from New York University in 1966, and his M.S. and Ph.D. from Stanford University in 1967 and 1969, all in Electrical Engineering.

The biggest problem in application security today

by Jeremiah Grossman

No question, the biggest problem in application security today is the huge shortage of qualified application security people. Have you seen the flood of job postings? I'm certainly not the first to have noticed. A recent LinkedIn poll provides further evidence that hiring is the top issue.

The reason is that essentially every aspect of a successful application security program requires some amount of specialized human expertise. This includes vulnerability assessments, pen-tests, source code reviews, Web application firewalls, threat modeling, software architecture, QA, and on and on.

Qualified application security people are necessary no matter what technology product an organization purchases, or processes they adopt.

There is no silver bullet to kill the software insecurity beast and there will likely never be. All you can expect from technology is to make people more efficient and processes more consistent. So, people must be trained to use application security products and trained to manage the processes they are integrated into.

Where the hiring problem becomes really interesting is when you estimate the number of people the application security industry will demand in the future. This exercise helps one better understand where the industry is heading. OWASP has a useful way to organize the three main application security job functions, so we'll use that as a framework.

Builders: Those who develop secure code.

Breakers: Those who locate vulnerabilities in written code.

Defenders: Those who fend off active website attacks.

Builders

Gary McGraw (CTO, Cigital) says roughly 1% of all programmers should be software security pros, or "Builders" in our case. Gary arrived at 1% by surveying dozens of software security programs among large companies and measuring what they do.

With a worldwide population of 17 million programmers this equates to a need for 170,000 Builders. I'd guesstimate 1-3% of THOSE people exist today. Maybe.

Breakers

At a bare minimum there are 1.2 million "important" websites (supporting SSL), out of 550 million total websites that should be assessed continuously and comprehensively for vulnerabilities.

For Breakers, we'll use a ratio of 1 person per 100 websites. This ratio comes from our internal metrics at WhiteHat Security generated from assessment conducted over the last 8 years and encompassing more than 5,000 websites.

The quality of these assessments is equal to or better than those of any top consulting firm. The math says we need 12,000 Breakers, where there might be 2,000 in existence today. The Breaker total could be easily driven up if there was some way to estimate the number of QA / Staging environments.

For the last several years, big software producers like Google, Microsoft, Adobe, Salesforce, and others have been hiring every good application security person in sight. The unemployment rate for those with these skills is effectively zero.

Defenders

I honestly have no idea how to even begin to estimate the need for Defenders, but it'll be in the tens of thousands at least. I think so by considering the vast number of website assets that must be protected, the 1 billion online users that someone needs to ensure are playing nice, and monitoring the serious volume of Web traffic they generate.

It is possible that everyone monitoring an IDS/IPS screen, a number I haven't been able to find, could be trained up and converted.

Collectively, that's roughly 200,000 qualified application security personnel that will be needed. This is an astronomical number and it has a profound impact on anyone building an application security program.

For the last several years, big software producers like Google, Microsoft, Adobe, Salesforce, and others have been hiring every good application security person in sight. The unemployment rate for those with these skills is effectively zero.

The talent void is a big reason why after so many organizations have spent so much of their precious security dollars purchasing just appsec technology that their programs fail and their websites continue getting hacked. Shelf-ware doesn't scale. Shelf-ware doesn't make anything secure.

The talent void is a big reason why after so many organizations have spent so much of their precious security dollars purchasing just appsec technology that their programs fail and their websites continue getting hacked.

This analysis drives companies who do business online, especially those experiencing an application security labor shortage, to make a key decision.

They must either:

A. Continue competing for qualified applicants in the shallow labor pool. Constantly be hiring, training, and trying to retrain their application security teams.

B. Outsource what skilled and heavy people-dependent processes they have, particularly to security vendors. Organizations can make a business decision to transfer the scalability problem of staffing up to someone else.

For the vast majority of organizations who do not have the cash or cachet of the likes of Google, Microsoft, and Adobe, Option B (outsourcing) is the only available option.

Security vendors, by nature of their core business, are technically in a better position to hire, train, and retain application security talent than the average non-security company. I say "technically" because security vendors then become the entity responsible for solving the qualified people shortage problem and, unfortunately for customers, few have done so.

What we also know is that there's great job security for those who choose this field and trainers are going to have more work than they know what to do with.

The bottom line is that if an organization's biggest application security problem is a shortage of qualified application security people, then it is of vital importance to take into consideration these industry dynamics. Ask yourself how many qualified employees (and with what type of skills) your program is going to need and where they are going to come from. Doing so will help you set out on the path to success and avoid unnecessary failure.

Jeremiah Grossman is a world-renowned expert in Web security, co-founder of the Web Application Security Consortium, and CTO at WhiteHat Security (www.whitehatsec.com). He has authored dozens of articles and white papers, and is credited with the discovery of many cutting-edge attack and defensive techniques.

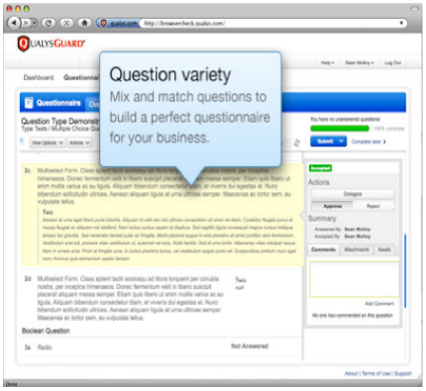
Employees are deliberately disabling security controls

Corporate mobile devices and the BYOD phenomenon are rapidly circumventing enterprise security and policies, say the results of a new global study sponsored by **Websense**.

77 percent of more than 4,000 respondents in 12 countries agree that the use of mobile devices in the workplace is important to achieving business objectives, but only 39 percent have the necessary security controls to address the risk their use entails.

Organizations often don't know how and what data is leaving their networks through non-secure mobile devices, and that traditional static security solutions are not effective at stopping advanced malware and data theft threats from malicious or negligent insiders.

Surveying policies, controls and compliance



Qualys unveiled a new service for its QualysGuard Cloud Platform and suite of integrated applications for security and compliance to help businesses further automate their compliance tasks and reduce the time and effort for manual assessment of IT and non-IT controls.

The QualysGuard Customizable Questionnaire service enables customers to build questionnaires using the Unified Compliance Framework, as well as leverage existing business process workflows to evaluate controls, gather documents and evidence and validate compliance.

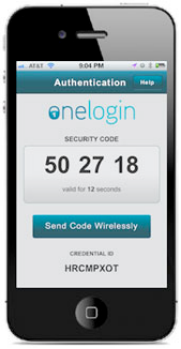
Encryption critical to improved security posture

Encryption is finally seen as a strategic issue and organizations are increasing their investment in encryption across the enterprise in response to compliance regulations and cyber-attacks, says **Thales**. Germany, the US and Japan show the greatest use of encryption. However, what is clear is that encryption is growing in importance in all the countries, with companies increasingly deploying encryption as part of an overall data protection strategy.

The Rise of Hacktivism panel.

Mobile one-time password app

OneLogin announced the debut of its mobile one-time password (OTP) app, which lets users perform multi-factor authentication with the click of a button.



Available on all major smartphone platforms, including iPhone, Android, Windows Mobile and BlackBerry OS 6 and 7, the app is free with every OneLogin plan.

Federated identity solution based on virtualization

Radiant Logic announced the release of RadiantOne 6.0, a complete on-premises federated identity service based on identity virtualization.

Featuring a dynamic set of tools including identity remapping, aggregation, correlation, and synchronization, the suite includes the advanced virtual directory of VDS+, the Cloud Federation Service (CFS) to connect identities with the cloud, and an identity correlation and synchronization engine.

Virtual scanners for consultants, enterprises and the cloud

Qualys announced virtual scanner appliances for its QualysGuard Cloud Platform and suite of integrated applications for security and compliance.

The new software-based virtual scanner appliance has already been formally qualified to run on many of the most common virtualization and cloud platforms including VMware and Amazon EC2.

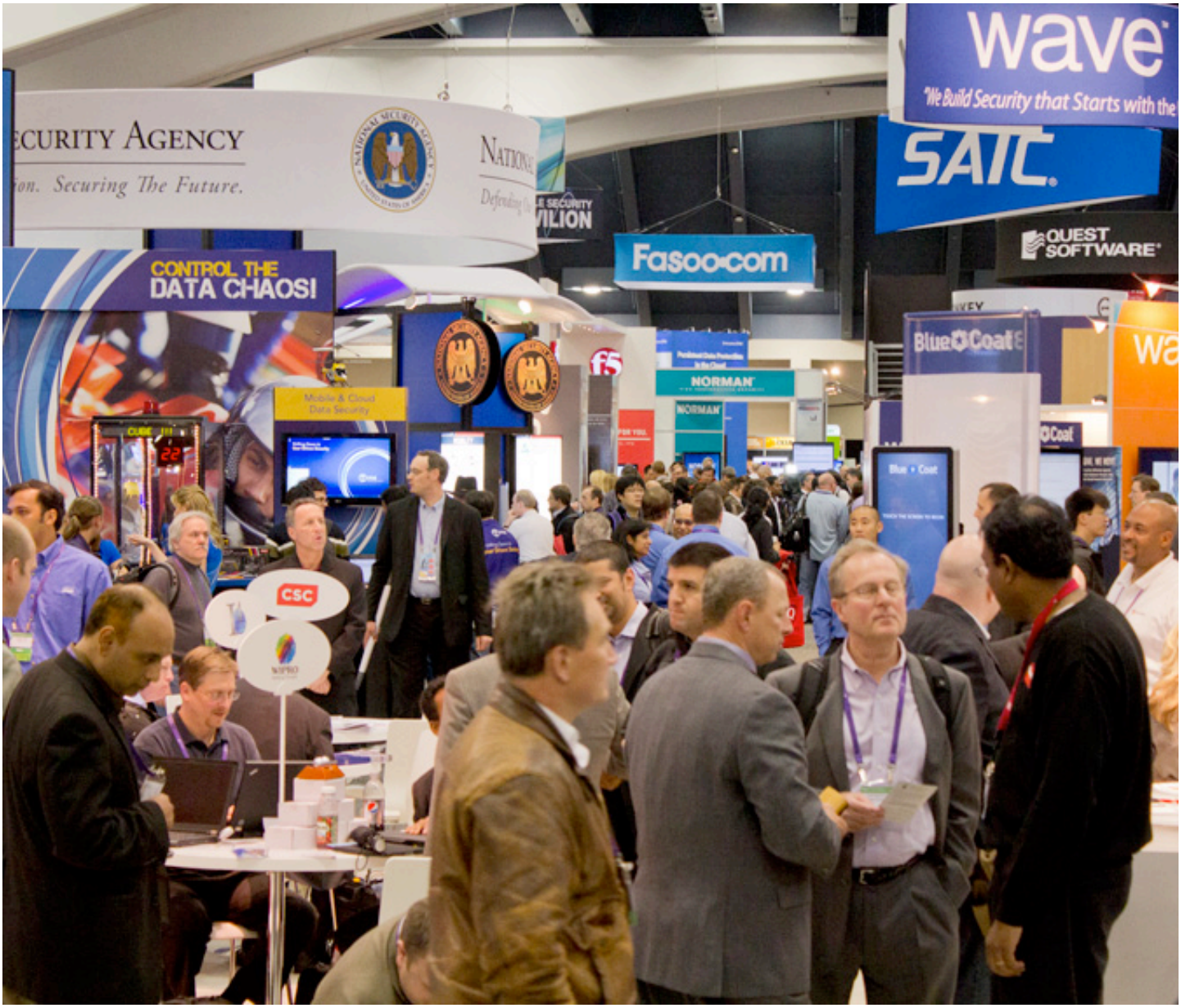
Voltage Security unveils Mobile Plus initiative

Voltage Security announced Voltage Security Mobile Plus, an initiative to extend its existing mobile security solutions to protect the new generation of mobile devices, applications and data.

With Voltage, the data itself is protected so that it can move between applications and devices without disrupting existing processes and user experience. Voltage solutions use Voltage Identity-Based Encryption to deliver stateless key management, scalable to millions of users.

Identity, app and mobile device monitoring

Lancope unveiled the latest version of its StealthWatch System, which harnesses the power of NetFlow and other flow data from existing infrastructure to deliver visibility for improved network and security operations. Version 6.2 introduces new virtualized appliances, as well as enhanced capabilities for identity, application and mobile device monitoring.



Trusted Computing Group unveils new membership option

The **Trusted Computing Group** has created a new membership option, the Associate, targeted to enterprise users, service providers, and to integrators and resellers. The new membership category lets users with a stake in security issues participate in the organization's class of work groups, which are focused on developing solutions through the definition of frameworks and enabling techniques using the foundational work for the TCG's specifications and standards.

Protection for data in the cloud

Fasoo announced three security solutions that enable protection for data in the cloud.

The Fasoo Usage Tracer (FUT) enables information governance by allowing organizations to overcome the limitations of security silos, often a consequence of cloud-driven infrastructure fragmentation. It maintains detailed activity logs for all protected documents throughout their entire lifecycle and can trace activities by a specific user or document.

Real-time session monitoring by Cyber-Ark

Cyber-Ark Software announced real-time session monitoring capabilities that enable immediate termination of suspicious activity. With the recent release of its Privileged Session Management Suite (version 7), Cyber-Ark is unveiling enhanced capabilities to better isolate, control and monitor activity to protect databases, virtual environments, network devices and servers from insider threats and external cyber attacks.

WHY ATTEND INFOSECURITY EUROPE 2012?

- Access Europe's most extensive & free to attend **knowledge enhancing educational programme**
- Meet **over 300 leading information security suppliers** – identify best of breed, cutting edge technology & see real solutions in action
- Hear from **real experts & respected public & private sector IT practitioners** to discover how they spent their budget on the right products, services and solutions
- **Network** with your peers through a wide range of activities including workshops & evening receptions
- **Earn CPE credits** by attending the free educational programme

infosecurity® EUROPE

24-26 April 2012
Earls Court , London UK

Organised by: Reed Exhibitions®

Register free now: infosec.co.uk/netsec