SMBs UNDER ATTACK

INFORMATION SECURITY®

NOVEMBER 2011

ONE IMAGE TO SECURE THEM ALL

VIRTUAL DESKTOP INFRASTRUCTURE CAN STREAMLINE YOUR DEFENSES

also

RISK ASSESSMENT CHALLENGES

TechTarget

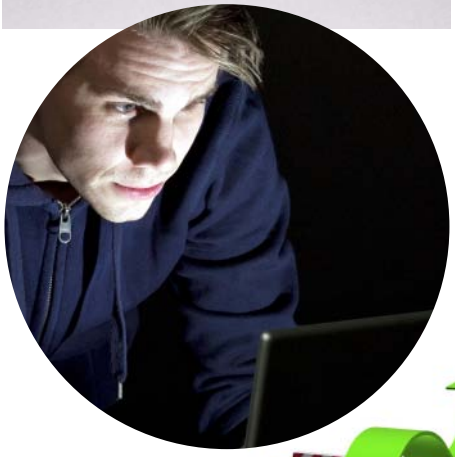
INFOSECURITYMAG.COM

FROM OUR SPONSORS

contents

NOVEMBER 2011
VOLUME 13 NUMBER 9

FEATURES



DEPARTMENTS

ALSO

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™

Time for Cyber Discourse on China

China is being accused of hacking corporate, government and military networks in the U.S. for economic gain. Policy makers need to be versed in cybersecurity and figure out how to respond. BY MICHAEL S. MIMOSO

JAMIE METZL CAUSED quite a stir late this summer with an article he wrote for the *Wall Street Journal* in which he blasted China's computer hacking efforts. Metzl, executive vice president of Asia Society and a former higher-up in the State Department and National Security Council, condemned China's actions as "running roughshod over global norms" to advance its economic interests.

Unfortunately for him, he used McAfee's Shady Rat research—which received criticism from several experts in the industry—as the backbone for his diatribe against China. Regardless, the bigger point here is China's 10 percent annual economic growth, a staggering number according to bean counters, isn't exactly being built solely on blood, sweat and tears. Metzl and others we've talked to and listened to say China is relentless in its efforts to steal intellectual property, trade and corporate secrets, and anything else that will give them an economic edge—or growth spurt. I've had more than one casual conversation land on the topic that some product some startup has been slaving over suddenly shows up on the China market months ahead of a potential launch here.

Metzl and others we've talked to and listened to say China is relentless in its efforts to steal intellectual property, trade and corporate secrets, and anything else that will give them an economic edge—or growth spurt.

Are we covering new ground here? No. But it's worth reminding those who will listen that the Chinese are on our networks and are leveraging state-sponsored or politically motivated computer hackers to steal anything that isn't nailed down.

China's efforts aren't limited to big business either. Despite Art Coviello's best efforts

to tap dance around the obvious, I'll take some journalistic license to read between the lines and conclude the Chinese were behind the SecurID attack. The attacks that compromised the company's flagship SecurID authentication technology have been the security story of the year. The seriousness of the attacks quickly came to light when it was revealed they were merely a jumping off point for a downstream attack on the defense industrial base as Lockheed Martin and others subsequently reported they too had been breached.

China computer hacking is also the suspected culprit behind the Aurora attacks on Google, Adobe and upwards of 20 other enterprises, manufacturers and defense contractors in 2009. Plus, two Department of Defense reports released in the last 20 months name China as active in moving digital assets off American networks—corporate, government and military. Can we stop the politically correct pretense and examine closely in public circles the impact of these intrusions upon our economy and national well-being? Granted, if we cast that spotlight on the Chinese, we're likely to get an equally bright light shined upon U.S. activities in China, Iran (hello Stuxnet) and other foreign interests. So be it. It's time for ground rules and time to tame the Wild West before real lives are lost, not just nuclear centrifuges and software source code.

There needs to be discourse at a policy level in Washington on cybersecurity and a clear understanding from legislators on these activities and their ramifications. The call for "offensive" weapons in cyberspace is also rattling around offices at the NSA and DoD and clearly some have been developed (hello again Stuxnet), but there are no rules of engagement written in stone yet in terms of how to react and reply to cyberattacks. How long before a physical, military response from either side follows up a cyberattack perpetrated by either side without a means for attribution of the attack or channels of communication between policymakers well versed in cyber?

The Chinese aren't shy about taking land or IP by eminent domain it seems. Pretty much anything is in scope to advance their economic agenda, according to Metzl's op-ed in the *Journal*. If so, it's time to bring cyber to prominence in Washington and internationally begin some real forward thinking before real companies are unable to compete in their respective markets, or worse, real lives are lost.›

Michael S. Mimoso is Editorial Director of the Security Media Group at TechTarget. Send comments on this column to feedback@infosecuritymag.com.

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

Trend Micro and VMware allow you to fully capitalize on the game-changing benefits of virtualization and cloud computing. Our innovative, complementary solutions include the first and only agentless antivirus solution for virtualized desktops and datacenters, and a breakthrough key management and encryption solution for both public and private clouds. The result is more than great security. It's a business advantage.

» LEARN MORE AT WWW.TRENDMICRO.COM/CLOUD OR CALL 877-21-TREND

vmware®

TREND MICRO™

*IDC, *Worldwide Endpoint Security 2010-2014 Forecast*, December 2010 **IDC, *Worldwide Quarterly Server Virtualization Tracker*

What's Wrong With Security?

We all have an explanation for weak security, but everyone needs to do their part to improve it. BY ELIZABETH MARTIN

AS WE ALL KNOW, non-stop reports of data breaches, data losses and hacking claims have put the spotlight on the state of information security. The constant negative attention on security is causing my mom, friends and neighbors to constantly ask, "What is wrong with security?! Why can't these companies get it right?!"

My answers are numerous and complicated; they are black, white, and gray. I ask myself, my peers, clients, vendors and security friends the same question and their answers are numerous, complicated and subjective, to say the least. The reality is each and every one of us is responsible for what's wrong with security. Each participant in security must step up and improve the effectiveness of his or her involvement. Here's what I hear as some of the most common explanations for the lack of computer security, along with my suggestions for improvement:

Security manager

"I do not have time to deal with the audits, the scan results, the IDS events, the firewall policy changes, the security policy, etc. across the entire organization. I only have three people on my staff. We do what we can, but we will not get to (insert important security issue here) in the next six months. If you gave me the staff and the budget I could address it, but the headcount won't be approved by management."

Find a way to make security real for senior management. Perhaps present a lunch-and-learn seminar on botnets and online fraud. Explain to senior management how they can protect themselves from online fraud. If they apply security to their personal lives, they will incorporate it into the professional lives.

Security engineer

"I submitted a change-control request to the networking team to disable all of those firewall rules and six months ago. I also asked for a list of active hosts to scan and the list they produced was half the size of what I found through discovery; they clearly do not manage the network very well. If management forced the issue, it could improve, but we do not have support for security on the networking team."

Try to find a creative way to penetrate (no pun intended) the networking and IT teams: Make friends, do favors, buy drinks, but most importantly, get to the root of their problems and find out what makes their jobs difficult. If you can solve their job woes and make their lives easier, you will make things more secure, but you have to take the time and go to bat for them.

Generic security team member

"We do not have an IDS, so I can't tell if any packets hitting that host contained SQL injection or not; I can tell if the firewall let a packet through over port 80, but that's it. No, I cannot tell you if a brute force was executed against the domain controller; we do not retain the logs. I have submitted requests for an IDS/IPS and log management solutions two year ago, but they haven't been approved."

Demonstrate the business value of security tools to the IT and development teams. Try to position the tools you need as a service offering and show them the value to their everyday lives. If your approach is to lay down the hammer and refuse to help if you don't have certain tools in place, you're less likely to build a successful business case.

IT director

"I met with security vendor X yesterday and they are touting security product A. This guy is a sales guy trying to push his product and I can tell you right now, I'm not buyin' it."

It's true—salespeople are trying to sell their stuff; that's how they make a living. I bet some of them would even admit to having to pay a mortgage, like most of us. There are some very good security sales folks who help you find the right solution for your business and some not so good ones who simply try to sell the next hot thing based on FUD. Please, people in purchasing positions, find the right partner and someone you can trust.

Developer

"I don't see the need to buy security monitoring product X; if you write good code that should take care of all of the problems. In addition, we can write a tool that can be more useful and do it better than the vendor."

You're very good at creating the widget; that's your core business. Please focus your energy on securing your code and open your hearts and minds to buying those security tools that are not your core business.

Security sales guy

"I thought that breach would happen. They have practically no tools in place. I worked on a deal for a year and a half with them; it was a product they really needed but they never got the budget approved and a few folks in the organization didn't see the value, so it was dropped." Or, "Client, this is the one and only security product you need. If you buy this product, it will achieve all of your compliance requirements."

Don't be a tool and oversell your products. Don't use the FUD factor; it won't work. Build trust with your clients and bring them solutions that meet their needs, not your portfolio.

Security consultant

"I spoke with the entire security team, the IT team, and the developer team and let me tell you, they have some problems. The security team has no staff, not enough time, and not nearly enough tools. The IT, developer, and networking teams do not see the value in security, so at the management level they have little buy-in and things simply do not get done, whether it is buying and implementing product or implementing policies and procedures. I delivered 35 findings from a one-week engagement; they are going to have a tough time getting those resolved. However, my 150-page report was very comprehensive; I should get a few more engagements out of it."

Please don't sell your client services they don't need. If you walk into a client site and know the state of their security within five minutes, don't sell them an $80K gap assessment—offer to help fix the issues. Offer value that goes beyond the dollars your client spends in everything you do; send them security tidbits here and there that are specific and applicable to them. Build partnerships and relationships and understand their business. Oh, and please do not give them a 150-page report; instead provide a simple one-page set of recommendations. Your value is not necessarily based on the length of your reports.

Security community (via Twitter)

"Doh! <Company> hacked because they accidentally posted SSNs on website—guess that guy is getting fired"

"Seriously? Did they actually think that telling us they were breached by an APT would reduce their culpability? Idiots"

"<Hacker Group Z> posted email addresses and passwords from <Company> on Pastebin-haha!!!

"It is almost funny how easy it is to do a Google search on SQLi or XSS…"

Spend a portion of your time providing solutions to the public. I consistently see new vulnerabilities, zero days, and other problems publicized, but don't always see solutions. Don't publish a new vulnerability or an opinion without a fix; it doesn't help. Avoid commentary that may be perceived as judgmental. These statements discourage other security individuals from joining the security community and prevent them from asking for help in solutions. For example, if a breach of company X is made public and we as an echo chamber call that company an "idiot," do you think it will openly reach out to us for help and collaboration? Not so much.

There are a lot of things wrong with security, but I also truly believe we are currently in an upswing, in terms of focus and effort. If we each do our part, we have the opportunity to improve the industry as a whole; it has to be a collective effort.

Elizabeth Martin has 15 years of experience in the information security, compliance, and risk management industry. She has extensive experience in the automotive, retail, financial, health care, and government verticals, and in managed security services. Send comments on this column to feedback@infosecuritymag.com.

(We'll help you make sense of it all.)

The social media stats are staggering — with thousands of updates every minute from hundreds of millions of users worldwide. And some of them work at your company. How can you **protect** your organization while enabling the best uses of the social web? Read our "Global Survey on Social Media Risks" to learn more.

Learn More

Mobile, social, and cloud technologies drive productivity. But they also open the door to data theft and advanced attacks that can slip right by antivirus and firewall defenses. Websense® TRITON™ solutions keep you a step ahead with best of breed web, email, and DLP security. Shared analytics, flexible deployment options, and a unified management console make TRITON the must-have solution for today's dynamic environments.

websense®

ANALYSIS | PCI COMPLIANCE

Point-to-Point Encryption Certification in the Works

PCI Security Standards Council plans to release a list of certified components in April. BY ROBERT WESTERVELT

AFTER ISSUING validation requirements for hardware-based point-to-point encryption, the PCI Security Standards Council is now developing a new program to certify point-to-point encryption products. A list of certified components is due out in April.

Bob Russo, general manager of the PCI SSC, says the program will be modeled after certification procedures used for payment applications and PIN pad devices. The point-to-point encryption certification program will focus on securing and monitoring the hardware, developing and maintaining secure applications, and secure key management methodologies.

"We looked at existing standards and referenced some best practices to come up with this program and certify some of these things," Russo says. "I want to caution that anybody who thinks they are going to pick out a solution from this list and automatically be compliant is going to be surprised; there are still PCI compliance activities at the foundation of what they've got to do."

Point-to-point or end-to-end encryption has been touted by providers as a way to eliminate credit card data from merchant systems and streamline PCI compliance. Early adopters have deployed the technology to encrypt cardholder data from the time a credit card is swiped at a point-of-sale terminal, to the time it reaches a card processor. Russo says the certification program is important because merchants have had no easy way to verify the claims made by point-to-point encryption providers or determine whether the technology will reduce the scope of a PCI DSS assessment.

The new program will initially certify hardware-based point-to-point encryption systems. It will eventually be expanded to include hybrid and software-based encryption

technologies, Russo says. Hardware-based point-to-point encryption systems use PIN transaction security (PTS) devices combined with hardware security modules, which perform the decryption.

Guidance documents and certification lists help reduce the confusion for merchants, says Russell D. Vines, qualified security assessor (QSA) and chief security advisor for Montvale, N.J.-based consultancy Gotham Technology. Vines says he has seen software vendors successfully dupe companies into purchasing poorly configured security software. A list of certified products is a good starting point and could reduce fraud, he says.

"It helps because the whole environment of the number of devices is so enormous that one QSA couldn't be completely knowledgeable in everything," Vines says. "My clients seem to like the guidance because it makes it a lot easier for them to navigate the path to certification. They can get their infrastructure assessed faster, easier and with fewer headaches."

"My clients seem to like the guidance because it makes it a lot easier for them to navigate the path to certification. They can get their infrastructure assessed faster, easier and with fewer headaches."

–RUSSELL D. VINES, qualified security assessor (QSA) and chief security advisor, Gotham Technology

The goal of the council's point-to-point encryption guidance is to define the minimum criteria for taking systems out of scope, says Richard Moulds, vice president of product strategy at France-based Thales Group, which sells the hardware security modules used in the encryption process. Moulds took part in the working group that helped create the validation requirements, which will be the basis for the certification program. Early adopters of the technology have had to work hard to convince QSAs that certain systems were out of scope of an assessment, Moulds says.

"Enterprises are desperate to find ways of taking applications and domains that have no ability to see any cardholder data out of scope," Moulds says. "Up until now, enterprises relied on convincing the QSA that [point-to-point encryption] is being done properly."

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

The Shrinking SIEM Market

by *Information Security* staff

Consolidation in the security information and event management (SIEM) market accelerated in October with IBM's acquisition of Q1 Labs and McAfee's purchase of NitroSecurity. The market for the technology, which is driven largely by compliance requirements, has been slowly contracting for several years now, leaving fewer stand-alone SIEM players. Here's a snapshot of some of the deals and trends in the SIEM space:

July 2011 → SolarWinds buys TriGeo

2010 → HP buys ArcSight for $1.5 billion. Trustwave acquires Intellitactics.

2006 → EMC acquires Network Intelligence. Novell acquires e-Security

$987 million → Gartner estimate of market in 2010

In Memoriam

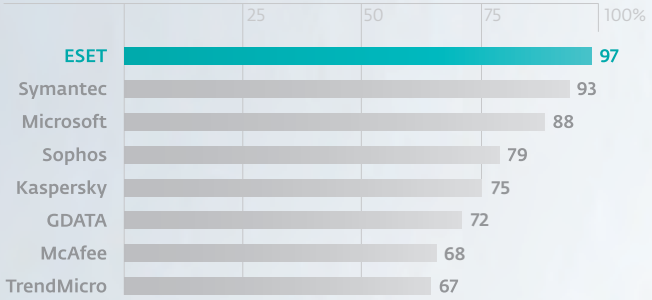
The information security industry is mourning the loss of Gene Schultz, who passed away Oct. 2. In his 30-year career, Schultz amassed an impressive array of accomplishments. He was a professor of computer science at several universities, including Purdue University and the University of California at Berkeley, founded and managed the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC), and worked as a consultant to a variety of companies. Schultz authored or co-authored five books and 120 papers, was a certified SANS instructor, and provided expert testimony to both Senate and House Congressional committees. He received numerous awards for his work, including the NASA Technical Excellence Award. Friends and colleagues remember him for his compassion, sense of humor and thoughtfulness. He will be sorely missed.

World's No. 1

Antivirus and Internet Security

ESET leads the industry in the consecutive number of "VB100" awards from Virus Bulletin testing organization.

Virus Bulletin Awards Success ratio (%)



Selected Antivirus Vendors (not a complete list)
Source: www.virusbtn.com, May 1998 - August 2011

Limited time offer: 1 year FREE

Buy two years, get the third free

Offer valid on 25 seats or more of ESET NOD32 Antivirus Business Edition and ESET Smart Security Business Edition

10/1-12/31/11. For terms, visit www.eset.com/q4promo

eset®

www.eset.com

2011 Information Security's READERS' CHOICE AWARDS global winner

A CHAT WITH MARCUS RANUM & RICHARD BEJTLICH

Security expert and Information Security *magazine columnist Marcus Ranum continues a new bimonthly feature where he goes one-on-one with a fellow security industry insider. This month, Marcus talks to Richard Bejtlich, CSO and vice president, Mandiant Computer Incident Response Team (MCIRT) at security firm Mandiant.*

Marcus Ranum: Richard, thanks for taking the time to talk; it's been a while and we've got a lot to catch up on! In the last couple of years we've seen a marketing push over advanced persistent threats (APT), a campaign attacking security companies, and the Aurora/Shady Rat attacks. I assume you're still a fan of network security monitoring? It's always seemed to me we, as a community, have been cutting costs in the wrong place. We need more monitoring, analysis and brainpower. Where do you see things going?

Richard Bejtlich: It's been quite a ride the last few years, indeed. Overall, I think there's a growing sense that becoming an intrusion victim is a possibility for lots of organizations, and a certainty for many depending on the sector and assets at stake. Enough of a variety of organizations have been compromised that many executives are asking, "Are we next? How would we know?" and similar tough questions. As a result, we're seeing increased interest in "Are we compromised?" assessments, rather than "Are we vulnerable?" assessments. It's one thing to have holes, but quite another to determine an intruder is actively exploiting them.

Marcus: That's the name of all of our pain, it seems. I don't think a week has gone by where I haven't gotten a question in the form of, "What do we do about APT?" It seems a lot of organizations sort of declared victory at the point where they could get a rudimentary handle on malware, but very few have the right mindset and tools in place to detect a seriously professionalized attack. I'm sure everyone in the security community had a moment of serious self assessment when the RSA and HBGary breaches happened—it's certainly made me reassess what "good enough" security really is. Obviously one piece of the puzzle is designing your processes to withstand attack—but let's talk about detection: Are you still as much of a proponent of security monitoring as you used to be?

Richard: Yes, monitoring is one way to achieve visibility. Visibility helps in several ways: 1) Visibility should guide your defenses toward countering actual threats to actual vulnerabilities, rather than theoretical threats to assumed vulnerabilities; 2) Visibility should tell you when your defenses have failed, so you can conduct incident response;

and 3) Visibility should provide metrics and assessment of all aspects of the risk equation. Note, I say "should" for all those elements. Many assume deploying a SIEM, logging packets dropped by the firewall, or running alert-centric intrusion detection systems provide "visibility" when they likely do not.

Marcus: I love the way you think about this stuff! You've touched on a ton of important issues in that one response. What you're really talking about is an information ecosystem in which all the components feed backward and forward into each other. If you've got an idea what should be happening, then you can invert that to get an idea of what shouldn't be happening. If you've got an idea where you're succeeding, then maybe everything else ought to be examined more closely, because it is a possible failure. I completely agree with you that a lot of organizations go out and buy a SIEM, then wait for magic to happen, but it doesn't, because that information ecosystem is not populated with the knowledge that is necessary in order to achieve the benefits of having the SIEM in the first place. I get very disappointed when I hear discussions about SIEM begin and end with, "What reports does it give me about what it's able to learn about my network?"

Many assume deploying a SIEM, logging packets dropped by the firewall, or running alert-centric intrusion detection systems provide "visibility" when they likely do not.

–RICHARD BEJTLICH

It seems to me the direction this needs to go is to figure out how to build policy- and purpose-centric systems that let us loosely specify what ought to happen on our networks, then subtract, "what probably ought to happen" from "what is happening" and look closely at what's left. I have one friend who is working on getting his HR department to forward the security team information about the job purpose of employees, so they can try to construct positive forward-looking activity maps. After all, if someone was hired to be in the research team, their internal network connectivity ought to mostly be with systems in the research cluster, etc. Do you think that kind of approach is going to work? Or do you think it'll be bypassed as "too much work?"

Richard: I like the sound of that approach, but I do think it will be considered "too much work." It seems like correctness, at multiple levels—platform, application, usage—would be a more successful methodology. However, I don't know how possible it is for security to determine what is correct. If you ask business owners, they usually can't describe how their assets should be used. One idea would be to have new systems deployed with documentation describing expected usage. Unfortunately, locations that demand such documentation, such as industrial automation and control systems, often lack documentation too! It's probably more realistic to deploy tools that do a good job describing what live systems do, and then involve humans who can say, "Yes, that's ok" or "No, that is weird."

Marcus: What you're talking about there is fast-feedback workflow systems. Do you know anyone who's made any good progress with that approach? I used to daydream about trying to see how far that model could be pushed if every effort was made to make the workflow update as easy and rapid as possible:

"Are you interested in this event? [yes] [no] [always events like it] [never events like it] [involving this system] [not involving this system] [involving this application]" etc.

I notice a lot of the stuff we're talking about here is not part of the commercial mainstream of security, because it's thought and effort-intensive; customers want to buy something they can install, which requires no tuning and no analysis.

Richard: When you mentioned that approach, it reminded me of a host-based firewall that asks if you want to allow application X to connect out to IP Y, or listen on port Z. It also reminds me that most of our analytical tools don't allow the application of analyst knowledge through integration. For example, you can't usually "tag" NetFlow logs or "mark" packets such that other people can learn or make decisions. Some commercial tools probably do that, but the majority of tools and techniques are still for rendering only, not knowledge integration and decision support—never mind the possibilities of "social analysis" where groups analyze data together. There's a good research project for someone!

Marcus: One final question: Are you working on any more books? I still feel your extrusion detection book is full of important concepts that more people should read. What are you up to these days?

Richard: I would like to write one or two more books. I posted this with some ideas to my blog. Basically, I'd like to write another technical book, but then also write more of a strategy book.

Marcus: Thanks so much for your time!

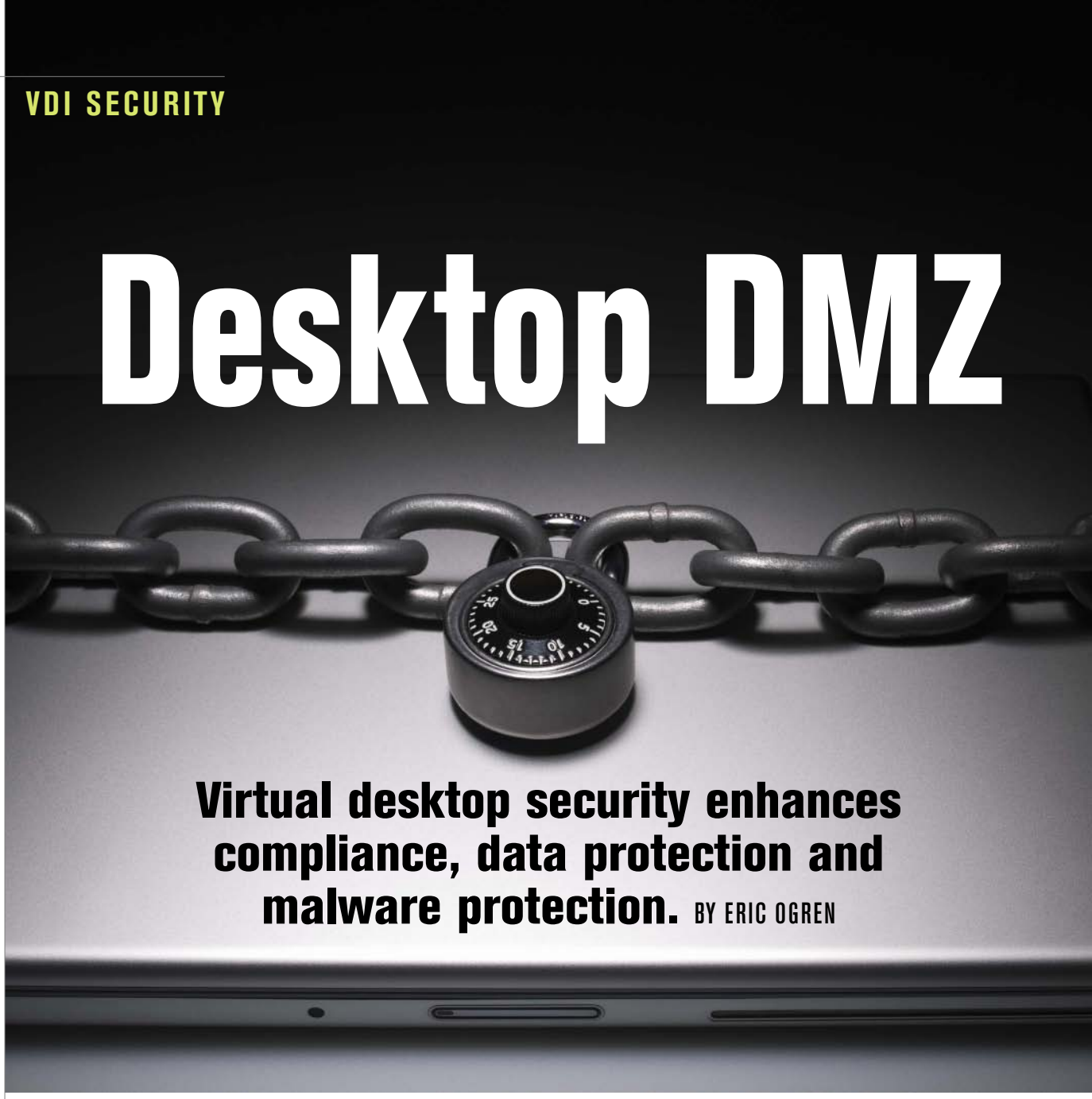
Perimeter E-Security Chosen Again as the only **Top Player** in Analyst Report

For the fourth consecutive Hosted Exchange market report by industry analyst, The Radicati Group, Perimeter E-Security continues to be rated the premier provider of messaging and security services.

See for yourself why Perimeter E-Security has been repeatedly selected as Top Player. Visit **www.perimeterusa.com** to download a copy of the report!

PERIMETER
E-SECURITY

Desktop DMZ

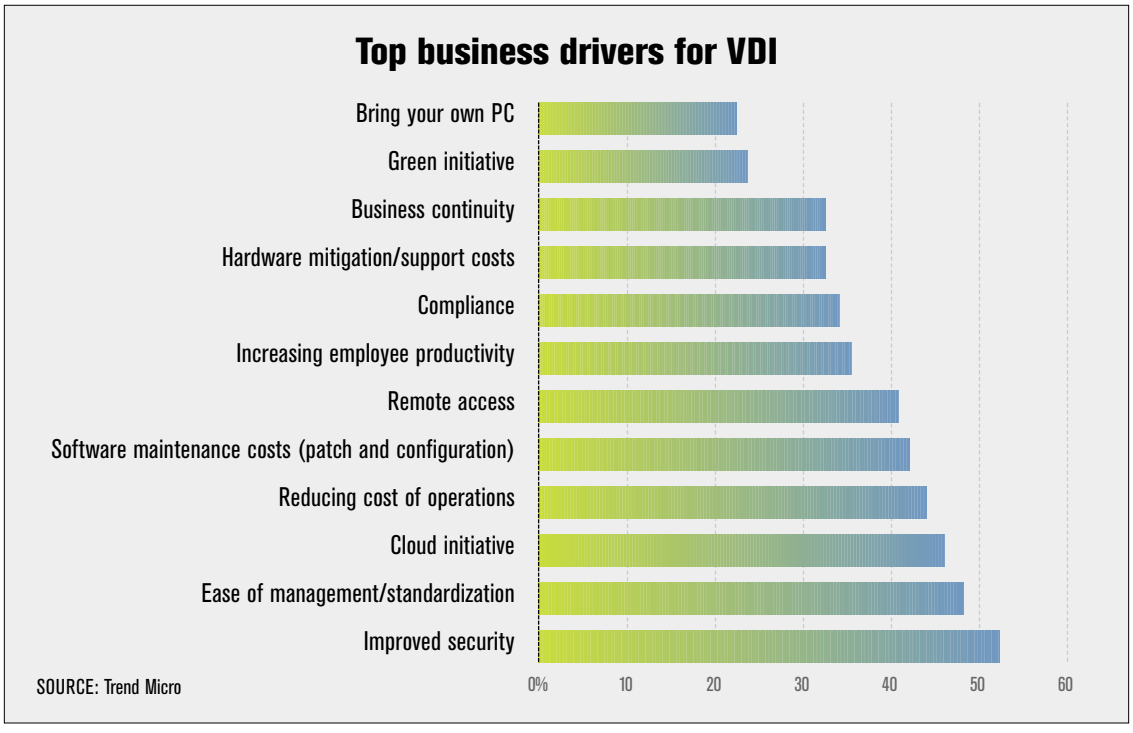


Virtual desktop security enhances compliance, data protection and malware protection. BY ERIC OGREN

ORGANIZATIONS ARE EMBRACING virtual desktop infrastructure (VDI) with the expectation of persistent security enhancements and reduced desktop operating costs across the enterprise. This strong coupling between desktop security and IT operations (see chart, "Top Business Drivers for VDI") backs up the thinking among early VDI adopters that centrally controlled desktop configurations are more resistant to malware and keeping regulated data off of distributed physical desktops reduces the business risk of a data loss incident. However, realizing these security benefits requires more than simply recreating traditional security in a virtual world; it requires a practical approach to inevitable breaches of desktop security.

While defense-in-depth prevention is still critically important to the business, a VDI-based approach favors active strategies for continuous malware resistance and compliance, data protection and incident response. These approaches are based on the following desktop security observations:

- It is inevitable that desktops will be breached in the coming year. The traditional approach to desktop security is to build a compliant desktop image and then deploy layers of security software to protect that image. However, experience shows that desktop applications are commonly breached and the VDI-based approach starts with the assumption some desktops in the network are already infected.
- It is very difficult to determine how long a desktop has been breached to gauge the exposure of regulated data. Once a traditional desktop breach has been detected, security teams embark on a labor-intensive investigation and recovery process. VDI offers security teams an automated mechanism for responding to security incidents that is focused on restoring business productivity.
- The cost of continuous endpoint management is increasing, particularly with the increase in hard to maintain remote devices. While automated patch and software upgrade products have helped to reduce the time a vulnerability can be exploited, it remains costly to maintain a compliant infrastructure—and the problem gets worse as business complexity scales. Virtual desktops can always be reached for software maintenance activities such as patches, upgrades, and removal of unsupported software.



Security executives apply lessons learned from deploying virtual applications in the data center to solve desktop security problems and gain cost-saving efficiencies in continuous desktop compliance management. Improved security is consistently the primary business driver for VDI for most organizations, followed by ease of management, enabling strategic cloud initiatives, and enhancing remote access—especially via non-Windows devices such as tablets and smartphones. VDI not only saves significant operational expenses, increases resistance to advanced persistent threats, and removes obstacles towards increased use of the cloud, but it enables security executives to promote active desktop security strategies including:

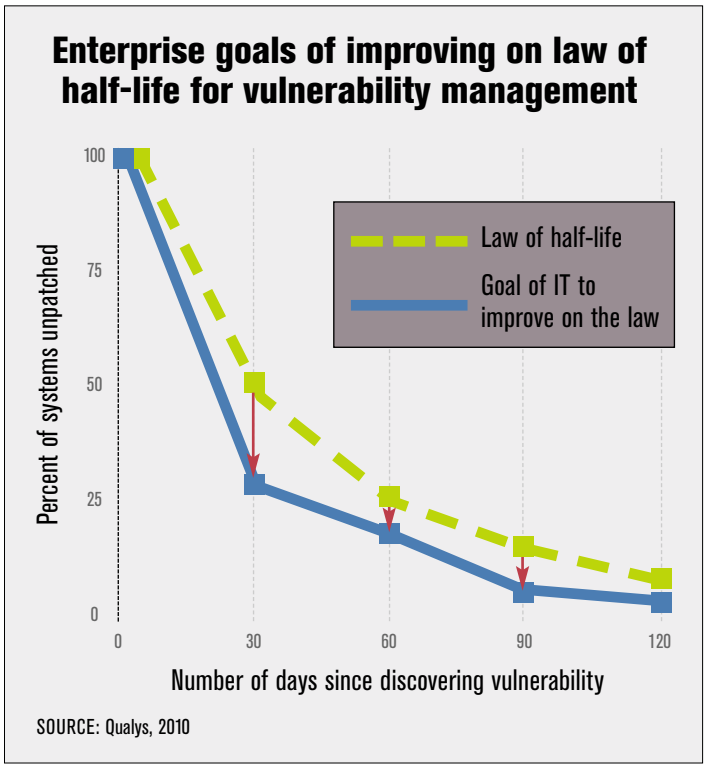
- **Streamline a continuous desktop management security strategy.** Maintaining a malware-resistant infrastructure is costly and time-consuming. Security executives are using VDI to fundamentally change approaches to software installation, patching and upgrades, fault detection, removal of unsupported software, and service desk activities. Security teams can deliver a more secure environment to the business while controlling operating costs.
- **Implement an automated data protection strategy**. While the business requires the sharing of sensitive information, the loss of regulated data can result in costly and disruptive public disclosure events. Security teams that cannot practically enforce data protection policies on all physical endpoints are evaluating VDI to maintain visibility and control of critical data by restricting operations on that data to the protected data center.
- **Instill an active incident response strategy.** Desktop infections and intrusions are inevitable—browsers in desktop virtual machines are be infected with malware just as easily as browsers operating in traditional physical machines. Security executives realize the potential of virtual desktop infrastructures to reduce the risk of serious security incidents by automating the return of desktop configurations to compliant states and using cloud-based services for high availability of desktops.

Traditionally, security executives focus on strategies for protecting desktops from malware and networks from intruders. The challenges today are to evolve the reactive device-centric approach with active strategies for protecting data and users. The opportunities to drive security benefits through desktop virtualization are compelling, including the sophisticated evolution of incident response strategies, data protection approaches, and streamlined maintenance of compliant desktops.

STREAMLINE A CONTINUOUS DESKTOP MANAGEMENT SECURITY STRATEGY

Security executives cannot control when or where malware will strike, but they can control endpoint software configurations to keep the infrastructure compliant with security policies and as resistant as possible to infection. This is reflected in many of the security

performance metrics that organizations use to drive security operations, such as the time required to patch a critical vulnerability in a percentage of corporate desktops, the number of calls to the service desk due to non-compliant endpoints (including disabled security software), the rate of discovery for critical vulnerabilities, the number of PC refreshes (with loss of user productivity) necessary to recover from a malware incident, and the total cost of security per desktop. However, it is becoming increasingly difficult in a physical desktop environment for security to improve on these performance metrics since desktops can be powered down or disconnected from the network—there will always be endpoints that remain unpatched or desktop applications that have not been upgraded. The chart (above), based on Qualys' Laws of Vulnerabilities in 2010, illustrates how long it takes to even approach 100 percent coverage of a critical software patch. In fact, 100 percent completion is often unattainable as there are desktops unavailable for extended periods of time.



A strategy toward a malware-resistant compliant infrastructure relies upon virtual desktops to simplify desktop management, reducing the risk of security incidents and returning operating costs to the business. VDI has the attractive properties of creating virtual desktops from centralized images where it is easier for security operations to maintain compliant desktop configurations and ensure that users operate under the most recent versions of authorized software. The ability to provision new desktops from pristine images, and to automatically re-provision desktops when users logout gives security executives the chance to evolve towards the next-generation infrastructure.

- Centralized provisioning allows security to create virtual desktops from authorized images. Instead of chasing and assessing distributed endpoints, security operations in a next-generation approach only have to patch, upgrade, and check vulnerabilities of desktop applications on the centralized servers. This has the potential to significantly improve security performance metrics, including those for patch coverage and time to remove critical desktop vulnerabilities.

• Once security has built a compliant desktop, terminating idle virtual desktops during off hours and re-provisioning automates the delivery of compliant desktops to the user, effectively reducing the possibility of desktops drifting out of compliance. This not only allows IT to easily deploy new software agents, replace software that is not easily patched such as obsolete versions of Adobe, Java, or custom built applications, but it also means that malware is less likely to persist on the desktop because the malware disappears when the virtual desktop is terminated. Organizations that allow virtual desktops to persist on the server are losing one of the key benefits of VDI.

• Security software can be shifted from individual desktops to become a shared resource on the virtual server. For example: Antivirus that is designed for VDI shares signature pattern files and coordinates system scans across all virtual desktops resident on the server; transparent disk encryption can be enabled for sensitive data; virtual patching allows security to plug a critical vulnerability at low levels in the server without disrupting users' desktops; and high performance application whitelisting is being utilized to ensure the integrity of the virtual desktop. This approach reduces the complexity and costs of managing desktop security—and antivirus will always be active with the most up-to-date patterns.

• User virtualization technology removes user preferences from the desktop allowing users to move freely between virtual desktops, remote desktops, and mobile devices and tablets. As organizations evolve from physical to virtual desktop infrastructure, user virtualization can provide the consistent look and feel across devices to increase user satisfaction and increase the chances of a successful VDI roll-out.

The operational cost savings of a virtual desktop infrastructure can be significant. For example, Ogren Group research finds that it is not uncommon for roughly one percent of corporate desktops to require service each month from normal operations. Reducing that percentage, and reducing the costs of a desktop refresh, with a continuous desktop management strategy based on VDI promises to sharply reduce this operating expense and increase user productivity. Security teams are hitting the limits of improving key security performance metrics with physical infrastructures where each distributed desktop needs to be accessible. The next-generation approach that is based on virtual desktop infrastructure promises to reduce the burdens of securing endpoints and delivering a compliant desktop infrastructure to the business.

IMPLEMENT AN AUTOMATED DATA PROTECTION STRATEGY

Modern attackers are much more interested in avoiding discovery and stealing intellectual property than they are in damaging infected desktops. Security executives are responding to this trend by prioritizing data protection strategies along with creating a cost effective automated desktop management infrastructure and an active incident response strategy.

Virtual desktops allow security teams to more tightly control regulated data, and to respond to security incidents with actions including:

- Simplify data loss prevention (DLP) strategies by restricting sensitive data to the data center with virtual desktops. Since the data never leaves the data center, not only is there less risk of costly disclosure incidents due to data loss, there is also less demand to purchase and administer device control and DLP software on desktops.
- Sensitive data can be transparently encrypted, and data center resources can be used for automatic backup and recovery of desktop data. The separation of data from the physical constructs of the PC also allows security executives to evaluate the cost savings of cloud-based storage.
- Just as a single copy of antivirus can serve all virtual desktops hosted on a server, for protecting data a single copy of a data loss protection (DLP) product can block sensitive data from flowing to unauthorized locations. DLP can be expensive to operate, partly because it must reside on each individual PC to offer effective corporate coverage. Security teams are working with DLP vendors to reduce administration overhead by integrating DLP with servers hosting virtual desktops.

The costs of compliance reporting are greatly driven by the number of security products that must be checked—the more software products the more time must be taken.

The costs of compliance reporting are greatly driven by the number of security products that must be checked—the more software products the more time must be taken. Using virtual desktops to reduce the number of individual agents is reducing the cost of security while protecting critical corporate information.

INSTILL AN ACTIVE INCIDENT RESPONSE STRATEGY

Unfortunately, it is not enough to operate a continuously compliant infrastructure that offers enhanced security with reduced operating costs. Attacks will still infect browsers and applications in virtual desktops just as they exploited vulnerabilities in physical desktops. Being virtualized does not change that. However, with VDI security executives can establish a pragmatic incident response strategy that expedites mitigation actions, is less disruptive to the users, and keeps the business running. Again, the keys are the ability of VDI to automate the provisioning and termination of virtual desktops with capabilities such as:

- Isolate infected desktop VMs and easily block access to the network to reduce the risk of data loss and a malware conflagration that runs throughout the company. While it is very difficult to isolate a physical desktop, virtualization servers can rapidly isolate

infected VMs in response to a security incident such as an unauthorized change to a desktop virtual machine.

- Apply virtual patches by correcting network flows in the server before the traffic reaches the virtual desktops. This allows security teams to implement a correction while waiting for a released patch from the affected vendor. Protecting desktops with patches on the virtual server allows security to shrink the window of vulnerability—the critical time between discovery of a vulnerability and application of a released patch.
- Disable access to the network and applications by simply terminating the user's virtual desktop when the user leaves the company or security suspects an intrusion. The termination action disconnects the user and removes any malware along with the desktop VM.
- Reduce the costs of a disaster recovery plan by shifting virtual desktops to remote data centers. Rather than purchasing extra hardware in stand-by data centers, business continuity services maintain copies of the provisioning server to be able to recreate virtual desktops and reconnect users to the business.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
SNAPSHOT
RANUM CHAT
VDI
CYBERCRIME
RISK ASSESSMENT
SPONSOR RESOURCES

Finding an effective incident response strategy to minimize disrupting user productivity has bedeviled the security industry since the inception of 'scan and hope' antivirus software. The traditional approach of refreshing an infected desktop is time consuming and costly. An active and pragmatic incident response strategy automates the termination and reconstruction of desktop VMs, flushes malware before it can spread, and gives security teams the flexibility to leverage off-premise services for disaster recovery.

Organizations are leveraging virtual desktop infrastructure to enhance security, reduce operating costs, and pave the way for cloud-based computing.

Organizations are leveraging virtual desktop infrastructure to enhance security, reduce operating costs, and pave the way for cloud-based computing. Security executives were tasked with protecting the business even while security for VDI was poorly understood. However, security executives are now turning to VDI for security to drive the costs out of desktop management and improve corporate resilience against attacks. They are using the powers of virtualization to evolve towards a continuously compliant desktop management infrastructure, establish a rational and active incident response plan, and elevate the priority of protecting important information. Virtualization has been a game-changer in the data center and the time is rapidly emerging where virtualization will also be a game-changer for desktop security.›

Eric Ogren is founder and principal analyst of the Ogren Group, which provides industry analyst services for vendors focusing on virtualization and security.

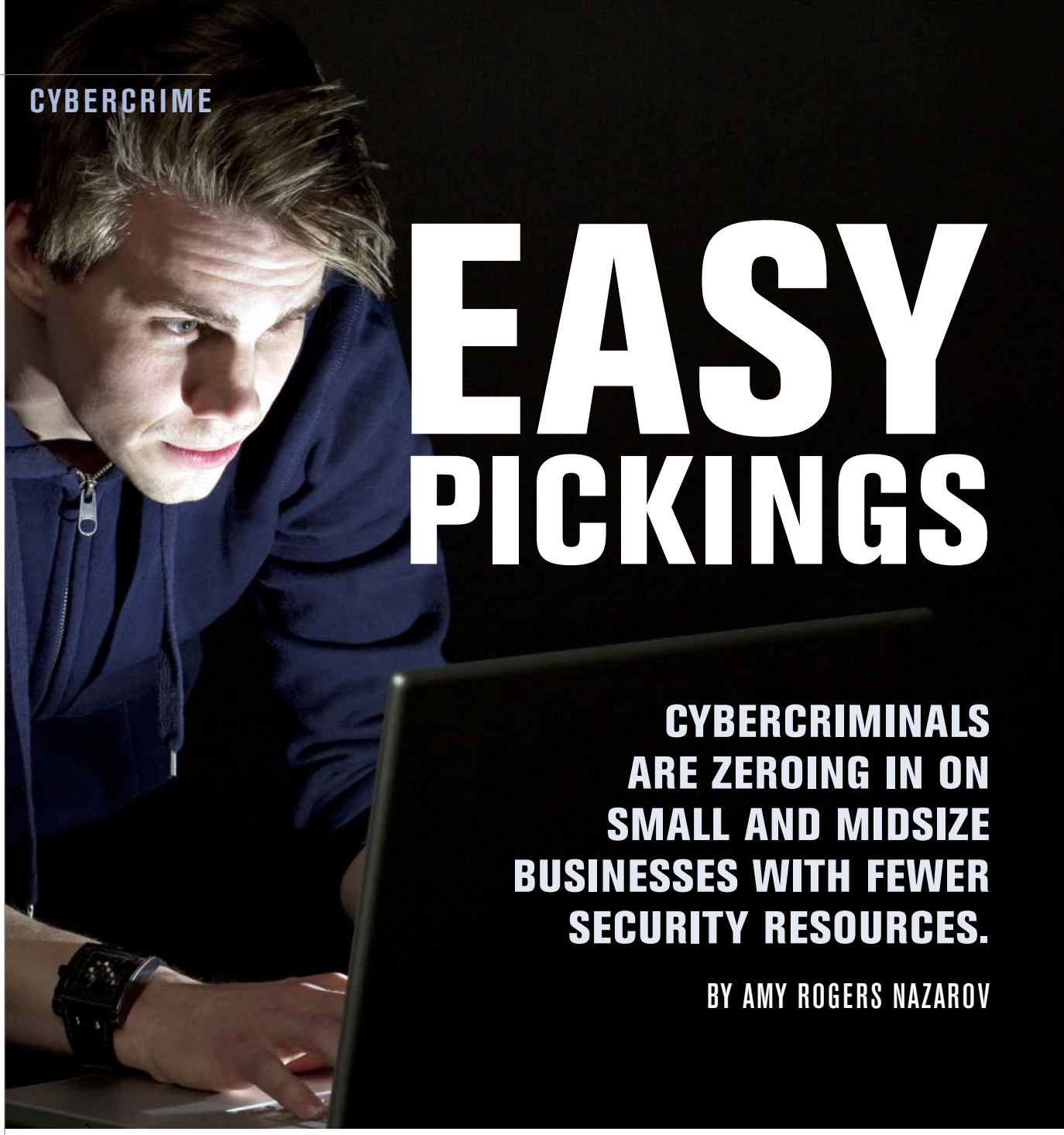
TODAY'S CYBERCRIME IS WORLD CLASS.

ARE YOU UP TO THE CHALLENGE?

HP ArcSight Express instantly alerts you to the complex threats faced by organizations by correlating millions of events occurring across the enterprise.

For more information go to www.hpenterprisesecurity.com.

ENTERPRISE SECURITY



EASY PICKINGS

CYBERCRIMINALS ARE ZEROING IN ON SMALL AND MIDSIZE BUSINESSES WITH FEWER SECURITY RESOURCES.

BY AMY ROGERS NAZAROV

TO THE CYBERCRIMINAL tapping away on his laptop in Kiev or Baton Rouge, the server your small retail shop, architectural firm, or medical office depends on is just as appealing a target as a box maintained by Wells Fargo, Twitter, or the U.S. Department of Defense.

In some ways, your server is more interesting to the guy. After all, you don't have a full-time staff charged with guarding your network. You never bothered to change the default password or update your patches. Maybe your Facebook-addicted employee clicked on another "You've gotta see this!" link, allowing the crook to implant a little code on his or her machine. He'll remember that place—or rather, the code he banged out in 15 minutes will—and he'll be back later when it's time to wake up the zombie farm to carry out a DoS attack. Worse yet, he might tunnel into your network and snatch sensitive customer or business data.

Organized criminals are using exploits and malware to generate revenue and they value ROI as much as SMB owners. Easy, repeatable attacks that skim off a little bit of money from a lot of places for very low effort are extremely appealing, says Erik Goldoff, a longtime IT security consultant. In this new age of cybersecurity threats, volume often trumps size.

"There are a handful of companies with millions of dollars, and millions of companies with a handful of dollars," Goldoff says. "If I could get $10 from every company I can touch, I don't care how big you are."

In the current threat landscape, attackers simply jiggle a lot of cyber doorknobs, find out who's left their "house" unlocked, and set about helping themselves to whatever they want: financial data, private emails, customer account information and other goodies. At the same time, targeted attacks on specific companies are on the rise.

Sure, plenty of small and midsized businesses are telling their staff not to write their passwords on sticky notes, not to click on links whose origins they don't know, and not to give any email sender purporting to be Nigerian royalty even one thin dime. But, "while there is a lot more training going on, those gains have been offset by the sophistication of the adversary," says Anup Ghosh, founder and CEO of Fairfax, Va.-based security supplier Invincea and professor of information security at George Mason University.

BAD GUYS KEEP GETTING SMARTER

Steve Surdu keeps tabs on those adversaries every single day, especially those working out of China or Eastern Europe. As vice president of professional services at Mandiant, an information security firm based in Alexandria, Va., Surdu says about one-fifth of his business is working with SMBs who want to bolster their defenses—and more often than not are seeking to limit the damage already done by an attacker.

"There are state sponsored attackers going after little [defense contractors] of 200 people or fewer, because of the very specialized things they do."

–STEVE SURDU, vice president of professional services, Mandiant

"There are state sponsored attackers going after little [defense contractors] of 200 people or fewer, because of the very specialized things they do"—and the intellectual property relevant to that work, such as blueprints for emerging weapons systems. "The larger defense contractors know about the threat and have been working for years to protect themselves, but that's caused the attackers to say, 'Let's take it down a notch.'"

Verizon's 2011 Data Breach Investigations Report [DBIR], released earlier this year, supports Surdu's observation. According to the DBIR, of the 761 data security breaches analyzed, SMBs with fewer than 1,000 employees sustained 556 of the attacks. Of those, 436 incidents targeted companies with 11 to 100 employees.

Half of the breaches examined in the DBIR utilized some form of hacking, and half incorporated malware (with both malware and hacking up about 10 percent over the previous year). Interestingly, 29 percent—up from 14 percent in 2009—of the attacks had an element of physical attack, such as someone gaining access to a PC simply by walking into an office masquerading as an air conditioning repair person.

Some of the most effective attackers have built workflows as honed and efficient as anything taught in business school, says Chris Porter, a principal in Verizon's risk management unit, which worked in tandem with the U.S. Secret Service and the Dutch National High Tech Crime Unit to gather and interpret the findings.

"Some of the most effective attackers have built workflows as honed and efficient as anything taught in business school."

–CHRIS PORTER, a principal in Verizon's risk management unit

"They might write and issue, say, a tool looking for specific default credentials and specific point-of-sale devices" sitting unprotected on the Web, Porter says. As the devices are identified, "they log into each and create a list of attack targets for the next team, which does malware installation."

After that's been installed, data exfiltration begins: credit card information, email addresses or some other desirable asset, Porter says. The next group monetizes the information, perhaps by selling the addresses to another crime organization that will use them for a range of nefarious purposes. One popular tactic is the cybercriminal's "canary in a coal mine": tacking a small charge onto each account to see whether it gets processed. Those that go unchallenged might prove fertile ground for another, larger-dollar heist, perhaps executed by yet another group of "specialists."

Cybercriminals' ingenuity knows no bounds. "They have some really innovative attack processes," Porter says.

What's more, bad guys excel at getting more bang for the buck than ever before. Think back to the Episilon attack in the spring, which was thought to have compromised tens of millions of email addresses belonging to customers of everything from CitiBank to LL Bean to Marriott. Chances are criminals have since used that email haul to compromise specific machines, set up spam relay points, initiate spear phishing attacks and much more.

SMBs ON THE DEFENSIVE

Even tech-savvy small business owners like Matt Wade, who runs an ISP in Washington D.C. with business partner and spouse Martha Huizenga, has had to tweak policies and procedures to combat phishing and other tactics that use an organization's name and reputation with clients for criminal ends.

Wade recently contended with a phishing attack in which someone created an email purporting to come from his company, DC Access. The email asked customers to provide their password and other information in order to complete an "upgrade" to the system. Wade acted fast, reminding customers via email that DC Access would never request such data in such a manner.

Elizabeth Shea, CEO of a 17-person public relations firm, SpeakerBox Communications, was surprised and distressed in 2008, when her company's website was hacked—and stayed down for three weeks. The ordeal cost her company at least one client and forced Shea to replace the IT services firm she had retained.

Nervous that business proposals and other sensitive information were in danger of being compromised, Shea chose to outsource the company's networking to a private cloud service provider for about $200 per month, about ten percent of what she used to spend on her former IT services provider.

SMBs must defend against both opportunistic attacks and targeted ones, experts say.

In targeted attacks, socially engineered methods – the creation of an email that appears to have come from a legitimate source, for example – make even a security-savvy recipient think they are opening a safe attachment. Or, consider a bogus LinkedIn profile filled with accurate company information that can later serve as a launching pad to for other exploits.

"All [the bad guy has] to do is get users to click on a link. If I can get you to do that, I can set up a back door and remotely log in.

–ANUP GHOSH, founder and CEO, Invincea

"All [the bad guy has] to do is get users to click on a link," says Invincea's Ghosh, a former DARPA scientist. "If I can get you to do that, I can set up a back door and remotely log in. Later, I can move laterally within your network"—to the payroll department, or the president's PC, or a customer database.

Opportunistic attacks, Ghosh says, are simply the price of using the Internet in a work capacity. From SEO poisoning to malicious links, no one's targeting your firm, per se, but they are "feeding off your employees' [Web usage]."

INCREASED SECURITY AWARENESS

For an SMB, the exploitation of a physical, policy oriented or network infrastructure weakness has potentially much greater impact than it might on a larger company.

"Sony and T.J. Maxx have had bad breaches in the past few years, but they're big enough to be able to absorb costs" related to mitigating the attack, whether it's paying for customer credit card monitoring services, or reimbursing bogus charges, notes Charles Kolodgy, research vice president for secure products at IDC and a former National Security Agency (NSA) analyst. "But if you're a small grocery story and someone steals $300,000 from your

PROTECTION

Combatting Cyberthreats

Experts offer cybersecurity tips for SMBs. BY AMY ROGERS NAZAROV

Small and midsized businesses must realize they are vulnerable to cyberthreats simply by virtue of being on the Web. Here, our experts share their best tips for staying safe:

Know what you've got. If you're a pizza place or a clothing boutique running 7,500 credit card transactions a year, "plenty of people would like to skim your customers' credit card numbers," says Steve Surdu, vice president of professional services at Mandiant. Or maybe you're a small government contractor supplying a piece of equipment to Lockheed Martin for a weapons system. Guess what? Your name is in the publicly available documents surrounding the bid for the contract, and the IP you own around that weaponry could attract the wrong kind of attention. Figure out how to best protect the assets that might prove most appealing to a crook.

Find out how your people really work, and adjust accordingly. You might learn that some of your telecommuting employees carry company information in thumb drives or DVDs they burn at the office, says Frank Kenney, vice president of global strategy and product management at Ipswitch. Or maybe they're sending work-related emails from their own unencrypted accounts to get around attachment size limitations. If loss of that information or those devices would be risky, consider making adjustments such as minimizing your email program's attachment size ceiling in order to corral sensitive emails.

Build partnerships to enhance your security footing. "Have a strong relationship with another business that specializes in security and/or IT consulting," advises Matt Wade, a founder of ISP DC Access. That way, you can keep your focus on what you do best, whether it's selling shoes or consulting on health care matters.

Examine your assumptions. Wade thought he had chosen a highly hack-proof server OS until an incident several years ago. "We were starting to standardize on Linux when our Apache Web server running Linux was exploited," he recalls. "I'm not sure which Linux distribution we were using. But after a bit of research, I decided we should migrate to FreeBSD. We have not looked back."

Think like a company, not a consumer. Too many small businesses rely too much on off-the-shelf consumer equipment. "They'll walk into Best Buy, buy a server they think will suffice and get all bent out of shape when it crashes in six months," says Scott Samborn, a founder at Rockville, Md.-based Mosaic Solutions Group. "But the cost to invest in a reasonable good architecture will typically pale in comparison to the cost of fixing" a system when it's compromised.

Keep it current. "Your antivirus software is the bouncer at your door, and you don't want a 65-year-old bouncer," says security consultant Erik Goldoff. "And keep his mug-shot book current" by keeping up with the attack definitions your antivirus vendor pushes out to you, Goldoff adds.

Don't neglect the basics. At a bare minimum, "change default passwords and put a firewall up," says Verizon's Chris Porter. Verizon's 2011 Data Breach Investigations Report found 63 percent of breaches could have been prevented by simple, cheap measures such as these.

bank account, that might be the difference between life and death for you."

Regardless of the size of your organization, information security must be everyone's responsibility, experts say. That awareness, plus strategic use of appropriate technology, will help combat the cyber baddies who have come to view a lot of little "takes"—a few bucks from this SMB, a bunch of saleable emails from that one—as a nice revenue stream.

There is no excuse for SMB owners to not understand, even at a rudimentary level, why they need to be proactive about managing cybersecurity, says SpeakerBox's Shea. "You have to be informed about how systems become infected in the first place."

"You have to be informed about how systems become infected in the first place."

–ELIZABETH SHEA, CEO, SpeakerBox

"In companies with two people, you may not have a chief security officer per se, but there needs to be a basic understanding by both people about how to categorize the risk of data loss," says Frank Kenney, vice president of global strategy and product management at Lexington, Mass.-based Ipswitch. "If credit card data or addresses or emails are lost or breached, all employees need to know what the impact to the business would be."

Kenney sees a silver lining to all the media exposure of security breaches this year, in that "a better understanding of risk in general and information security in particular is permeating the layperson."

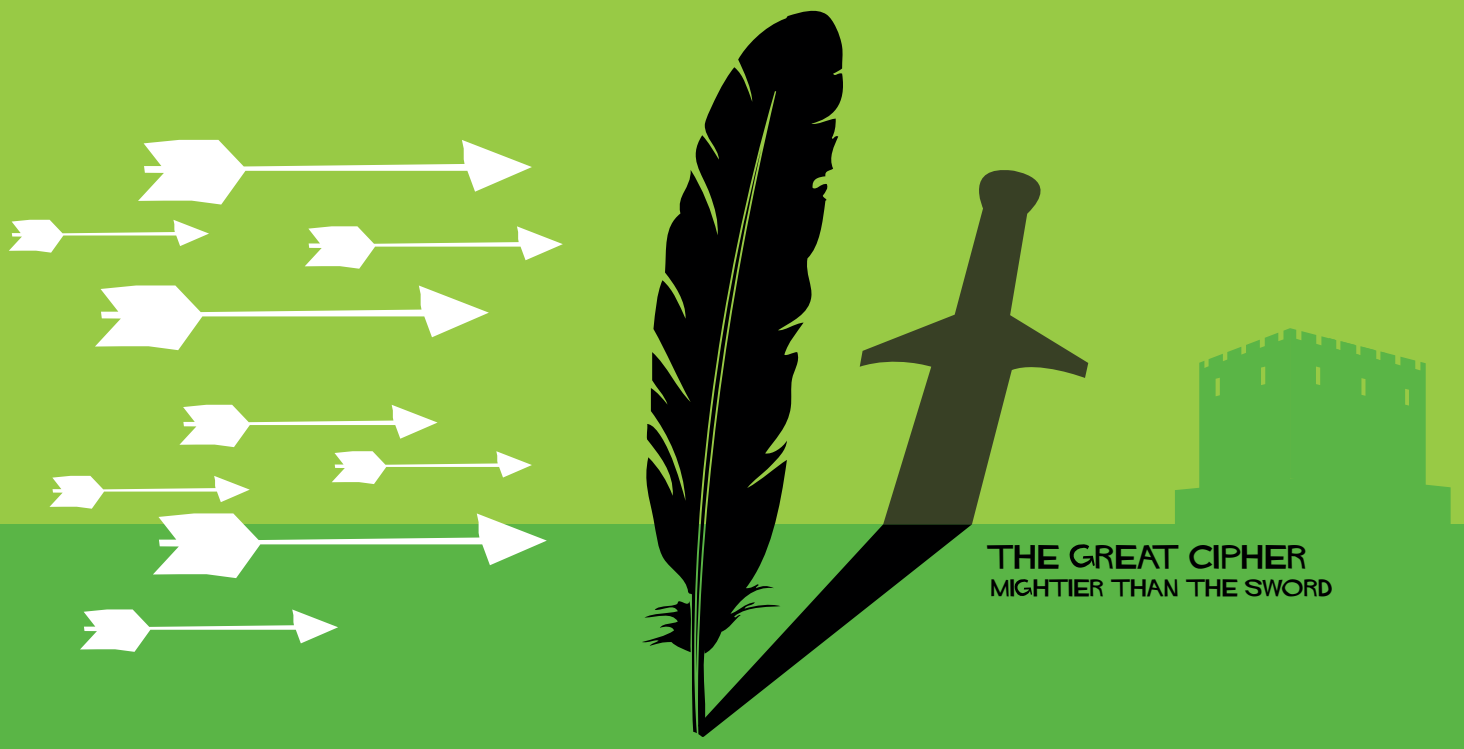
Ultimately, the fewer SMBs operating under the illusion that obscurity is tantamount to security, the better.

"Do at least what everybody else is doing" to protect their networks and assets, says Mandiant's Surdu. "The bad guys are looking for the weak link."

Amy Rogers Nazarov is a freelance writer based in Washington D.C. Send comments on this article to feedback@infosecuritymag.com.

RSA® CONFERENCE 2012

FEBRUARY 27-MARCH 2 | MOSCONE CENTER | SAN FRANCISCO



PROTECT YOUR KINGDOM. LEARN HOW AT RSA® CONFERENCE

Each day security professionals are faced with new enemies, tactics and threats—it's time to evolve your security strategy. RSA® Conference brings you five days of innovative sessions, inspiring keynotes, and collaborative strategy building. Gain insights on today's hottest topics, learn how to leverage the latest trends and technologies, and get access to new best practices on the most critical technical and business issues facing you today.

Join the community at RSA® Conference 2012 to empower yourself with new insights, solutions and allies to keep your organization secure.

REFINE YOUR EXPERTISE
Participate in over 220+ expert-led sessions.

EXPAND YOUR OUTLOOK
Attend world-class keynotes.

SHARE YOUR INSIGHTS
Collaborate with information security's best and brightest.

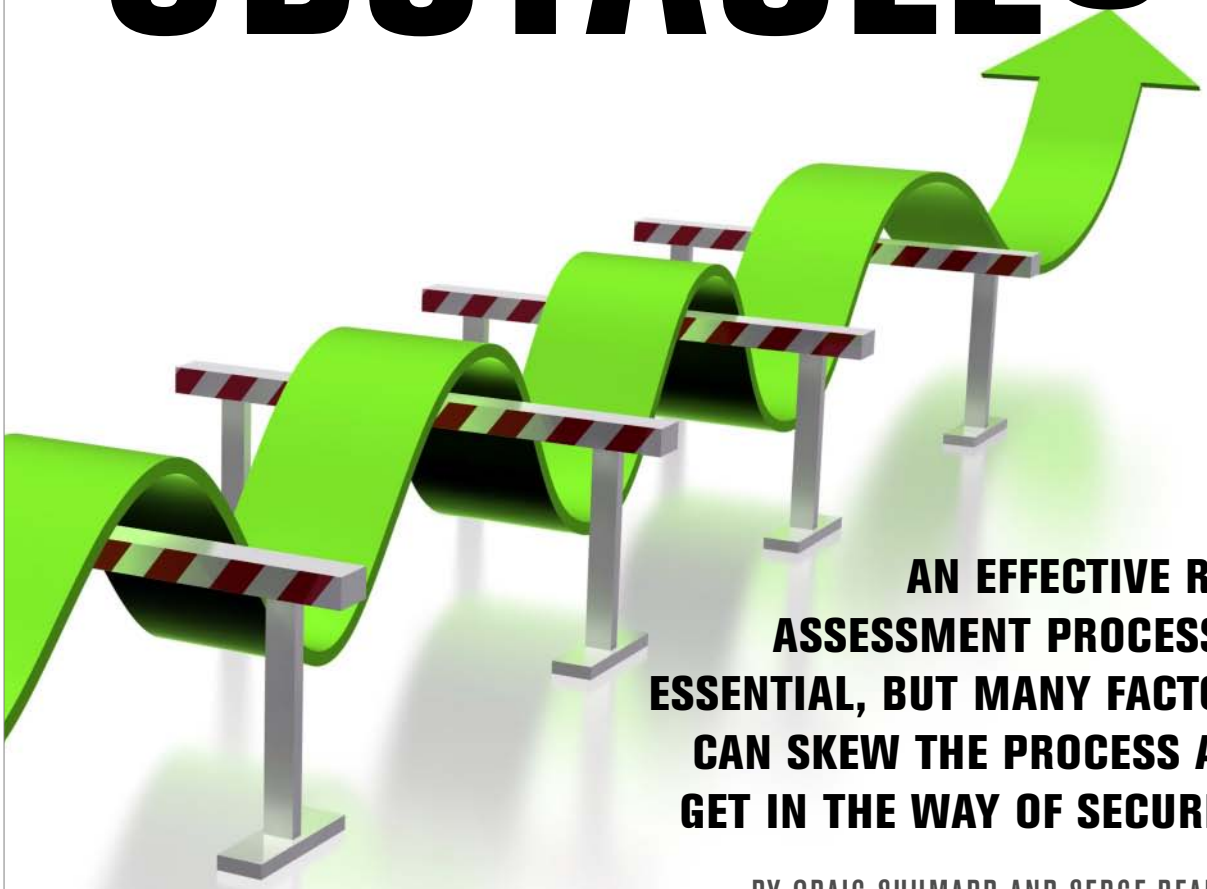
HARNESS YOUR STRATEGIES
Discover practical solutions to implement at the office.

SAVE $700
Before Friday, November 18, 2011

REGISTER NOW!

www.rsaconference.com/techtarget

OVERCOMING OBSTACLES



AN EFFECTIVE RISK ASSESSMENT PROCESS IS ESSENTIAL, BUT MANY FACTORS CAN SKEW THE PROCESS AND GET IN THE WAY OF SECURITY.

BY CRAIG SHUMARD AND SERGE BEAULIEU

INFORMATION SECURITY RISK assessments are a fundamental building block of any security program, much like security awareness training, policies, procedures, and technical safeguards. A risk assessment program is required by several regulations such as HIPAA, SOX, and FISMA. Risk assessment is also an essential element of all security standard bodies of generally accepted security practices such as ISO, COBIT, and NIST.

Ideally, an effective risk assessment program should ensure necessary security controls are in place or put in place based on the information risks or threats that an organization faces. The risk assessment process should identify and prioritize any gaps found. In other words, an effective risk assessment program should drive an organization's security initiatives and its program.

However, security risks assessments are subjective exercises. Risk assessments can be inadvertently and advertently skewed based on interpretations and result in not implementing necessary security controls. Reluctance to spend money, perform unplanned activities or change user experience are other factors that can affect risk assessment results. We'll take a look at these challenges and ways to overcome them in order to improve the risk assessment process.

METHODOLOGY DOESN'T OFFSET SUBJECTIVITY

Most risk assessment processes used today range from informal processes to more rigorous assessment methodologies such as NIST, COSO/COBIT, or OCTAVE. Most organizations rely on a qualitative assessment methodology; some companies include quantitative methods in the assessments. Regardless of the methodology used, all risk assessments are fundamentally subjective exercises. Its results are dependent on interpretation of threat level, probability of occurrence, impact, valuation of assets, etc. Therefore, risk assessments are susceptible to be skewed, unconsciously or consciously, to a pre-determined outcome.

Other factors affect the subjectivity of a risk assessment. These factors include the subject matter expertise of the assessor(s). Often, risk assessments are performed by people who do not possess the necessary security knowledge, or may not fully understand the security and privacy risks. Professional motivation also affects one's subjectivity; business units want to minimize costs while a security governance team wants to minimize risks.

RISK TOLERANCE

Who assumes the risk is critical to maintaining a consistent risk posture across the enterprise. Ultimately the business needs to make the call on clearly defined risks, but the question is who?

A project manager, a director, a VP, an EVP, the CFO, and the CEO all have a different view of risk and a different risk acceptance tolerance based on knowledge and experience. Unless there is an accepted "risk assumption" model or procedure that defines who can assume risks and at what levels, the structure for a viable and effective risk assessment process is missing. A project manager has a very different risk tolerance than a CEO. A project manager is judged on delivery time and budget and may view security controls as obstacles, while the CEO is focused on the reputational risk of the enterprise. Even the CFO and the CEO can have a different tolerance level of enterprise risk. There needs to be dialogue at the highest level of the organization to define what the risk tolerance of the organization is. Having a risk assumption model that includes the CEO will help crystallize the discussion around risks.

Another essential foundational element every organization should have is a repository of common threats, risks, and a common lexicon for explaining vulnerabilities and mitigating controls. Without a risk escalation process that identifies who can ultimately assume risks

Protecting the World's IP

Stopped Stuxnet
Stopped Aurora
Stopped Conficker
Stopped Zeus
Stopped 2011 Recruitment Plan
Stopped <Insert tomorrow's malware>

Free Trial at www.bit9.com/freetrial

Bit9

The Most Effective Protection Against
Modern Cybersecurity Threats

and a common lexicon for security risks, it's difficult to have an effective enterprise risk assessment process.

OTHER CHALLENGES

There are several other factors that drive an organization to skew the outcome of a risk assessment and, at times, use it to rationalize not implementing the necessary security controls. These include:

- **Cost**, especially unbudgeted costs. Regardless, business and even IT units do not want to spend money on security controls unless they are absolutely necessary and usually tied to regulatory compliance or an audit citation. The business unit will minimize the privacy or security risk to avoid spending the money. Let's face it, security controls cost money and take time to implement; they are a hard sell.

- **Unplanned activity**, especially if it is part of a system development effort or project with a tight deadline. Any unplanned activity, whether it is part of a project or part of a yearly operating plan, will generate, at minimum, tension or push back. Project teams and management in general are inherently averse to doing any tasks they did not plan for. It may affect project deadlines or the completion of operating plans that they get judged on and therefore may impact their performance rating, raise, and bonus.

- **Miscommunication.** Many times, security managers communicate in terms of missing control risks or a policy non-compliance risk, not in terms of the business or organizational risk. As a result, it's hard to achieve consensus to mitigate the risk(s), regardless of what control should be implemented.

- **User or customer impact.** Any security control that changes the user experience will create resistance. Even if it's as benign as increasing the length of passwords, it creates anxieties for business managers. Therefore, they will likely overstate implementation costs and try to delay implementation.

- **Overestimating the costs of security controls.** Sometimes the business or IT unit is uncertain about the implementation cost, and will overestimate the cost of the security control.

- **Improperly relying on mitigating controls that do not effectively address the risk.** A good example might be to rely on a manual review of system event logs instead of implementing an event monitoring system.

- Last but not least, many organizations do not understand most security controls are necessary. The vast majority of the controls outlined in the generally accepted security standards bodies, (e.g. COBIT, ISO, etc.) are required and need to exist in some shape or form in every organization that has an IT infrastructure, even if it is outsourced.

RISK ASSESSMENT TOOLS

There are many automated risk assessments tools and solutions in the marketplace; some are more sophisticated than others. Some are basic risk assessment documentation templates, while others are robust risk assessment knowledge systems with workflow and dashboard features to rollout and maintain an efficient organization-wide risk assessment program. There is no one-size-fits-all with risk assessment tools; different tools may work better for your industry or particular needs. The key success factor/feature should be how comfortable you are that the proper risks are being captured and addressed. Tools can help standardize the risk assessment process enterprise wide, maintain a risk repository, and help an organization harden or strengthen its risk assessment posture and program overall.

While worthwhile and necessary for large organizations, automated tools are still susceptible to problems and challenges outlined above. That's because ultimately they rely on people's input and judgment.

STEPS FOR IMPROVEMENT

First and foremost, there needs to be a paradigm mind shift in the enterprise that accepts the notion that most security controls are a necessary cost of doing business. The risk assessment process should include mitigating controls based upon generally accepted security control standards, such ISO, COBIT, and NIST. The risk assessment should not focus on whether a particular baseline control should exist, but rather whether the security controls as implemented sufficiently address the risks of the organization. Also, security standards typically lag new technology risks (e.g. SOA-based applications, cloud computing, iPads and other mobile devices). In those situations, new security controls and techniques may be required based on the security and privacy risks.

The risk assessment should not focus on whether a particular baseline control should exist, but rather whether the security controls as implemented sufficiently address the risks of the organization.

In addition, the risk assessment process should not be viewed as a compliance exercise; it should not be a process to demonstrate regulatory compliance or adherence to good security practices, as is often the case. A good risk assessment program should be the primary process that drives security initiatives, based on sound risk assessment analysis that's grounded on generally accepted necessary safeguards/controls (e.g. ISO) and new technology and/or business IT risks.

Finally, security organizations need to strengthen their risk assessment capabilities, specifically in terms of people, processes, and technology. They need people with the necessary communication skills, security knowledge, and most importantly, the analytical skills to

identify business and technologies risks, potential mitigating controls, and mitigation strategies when gaps exists. Security managers need to speak in business risk terms, not control risk terms.

The risk assessment process needs to include a formal risk assumption model that defines who can assume risk to ensure the enterprise maintains its desired risk level posture. Last, organizations should have a common risk assessment methodology implemented, a risk universe and results repository, and the necessary technology or system to implement and sustain an effective risk assessment program.

An effective risk assessment program is one of the fundamental building blocks of any information security program. The ability to understand your risks, mitigating controls and your company's risk tolerance/assumption posture will define your information security program and how well you are prepared to meet today's risks/threats.

Craig Shumard is retired CISO for CIGNA Corp. Serge Beaulieu, CISSP, CISM, is a security consultant and retired head of Security Technology Planning & Roadmaps at CIGNA. Send comments on this article to feedback@infosecuritymag.com.

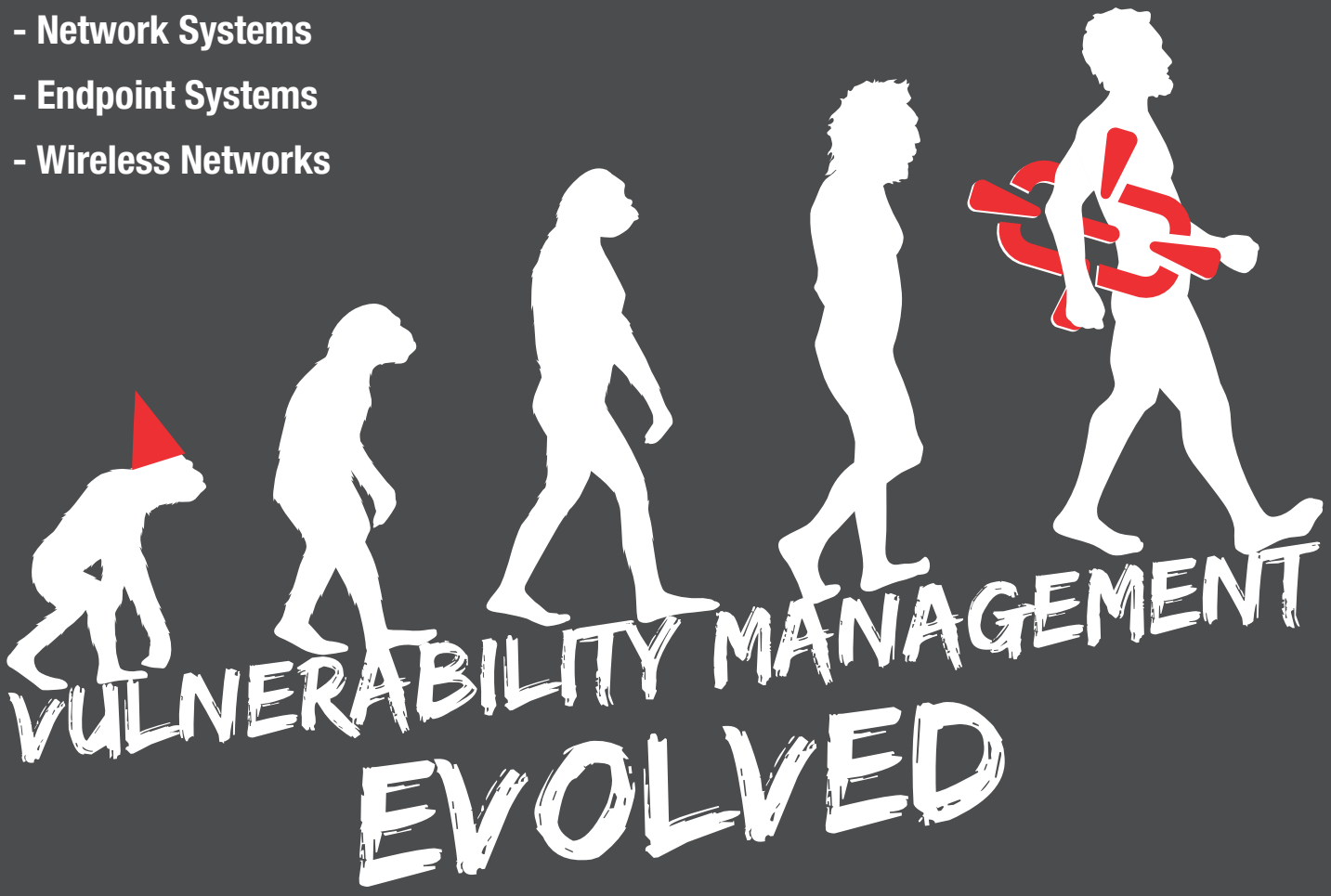
CORE IMPACT PROFESSIONAL

Find the gaps in your vulnerability management program ...

Click here to download a free gap analysis tool.

Penetration Testing Software for:

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



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

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

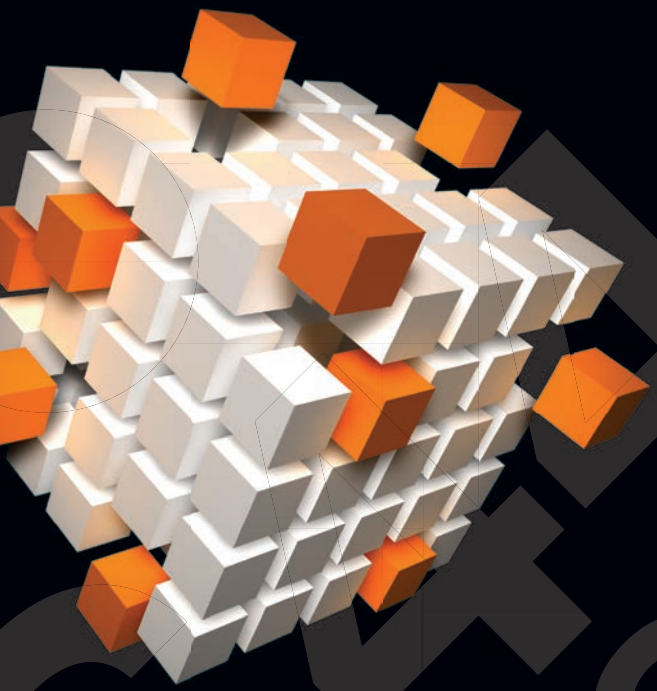
Learn more:
Visit www.coresecurity.com
or call us at (617) 399-6980

CORE SECURITY TECHNOLOGIES

Source 44 Consulting

www.source44.net

Network and Data Security Services



Threat Mitigation

Network & Security Technologies

Security Assessments

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

Support Services

Professional Services & Full Support
Security Infrastructure Management

Digital Forensics

Investigations
Data Recovery
e-Discovery
Litigation Support

IT Security Training

Training Courses

Contact us for a **FREE**

1-hour consultation

info@source44.net

905.237.4576

For your SPECIAL OFFER please scan the QR Code

www.source44.net

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR
Michael S. Mimoso

SENIOR SITE EDITOR Eric Parizo

EDITOR Marcia Savage

SENIOR MANAGING EDITOR Kara Gattine

NEWS DIRECTOR Robert Westervelt

SITE EDITOR Jane McPherson

ASSISTANT EDITOR Maggie Sullivan

UK BUREAU CHIEF Ron Condon

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum,
Lee Kushner, Mike Murray

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

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

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS
Amy Cleary

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kathleen Quinn

SALES DIRECTOR Tom Click

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER Bryce Dooley

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

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann
peichmann@techtarget.com

Sean Flynn seflynn@techtarget.com

Jennifer Gebbie
jgebbie@techtarget.com

Jaime Glynn jglynn@techtarget.com

Leah Paikin lpaikin@techtarget.com

Jeff Tonello jtonello@techtarget.com

Vanessa Tonello
vtonello@techtarget.com

George Whetstone
gwhetstone@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER
Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT
Kevin Beam

CHIEF FINANCIAL OFFICER
Jeff Wakely

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

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

COMING IN DECEMBER



Enterprise Rights Management

Authorized users have permission to interact with data in order to do their jobs. But what if those trusted users do more than is intended with sensitive corporate information? What if they're printing multiple copies of documents, emailing messages and attachments outside the company to personal email accounts, or cutting and pasting portions of sensitive documents to their desktops, mobile or portable storage devices? Companies may counter this data protection risk and solve some pesky compliance questions by implementing enterprise rights management technology. This feature will explain how ERM helps you enforce data protection policies, satisfy regulatory mandates and apply controls to documents and other content in order to keep internal and external threats at bay.

Breaking Vista

Well-known security researcher Chris Paget was on the inside at Microsoft five years ago, hired as part of a penetration testing team whose task it was to put the Vista operating system through the rigors. Paget saw firsthand the ins and outs of Microsoft's internal security processes for vetting code and shares her unprecedented access with *Information Security*. Share Paget's experiences through her own words and find out her surprising conclusions.

Don't miss our monthly columns and commentary.

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?

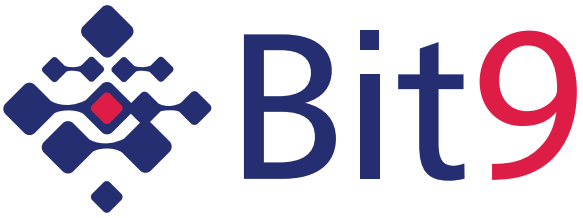
Balancing business priorities and risks is key to a solid approach.

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 37

- From the Frontline - Preventing APT
- New Tools to Stop Today's Hackers

See ad page 4

- Entrusting Endpoints
- Security in Layers

Co3Systems

- You've lost sensitive data - What now? Webinar: How To Tame Data Loss in 6 Easy Steps
- Free Webinar: Data Breaches & Compliance: What Are The Legal Implications and How Can You Prepare

See ad page 41

- **Optimizing Vulnerability Management**

See ad page 15

HP Enterprise Security

See ad page 27

- **Explore some of the most prolific digital asset threats and risks facing organizations today**
- **Read the results from the Ponemon Institute's Second Annual Cost of Cyber Crime Study**

PALISADE SYSTEMS | SECURING YOUR DATA IS OUR BUSINESS™

- Data Security Experts Discuss DLP for the Mid-Market
- Why DLP? An in-depth report on data loss prevention

PERIMETER E-SECURITY

See ad page 19

- Radicati's Top Hosted Exchange Player Wants to Play with You Too!
- Perimeter's SaaS Log Management Services Monitors, Alerts and Reports to You From the Cloud

RSA CONFERENCE 2012
FEBRUARY 27 – MARCH 2 | MOSCONE CENTER | SAN FRANCISCO

See ad page 34

- Follow the latest webcasts and blogs from our community of top security professionals
- Register for RSA Conference 2012 before November 18, 2011 to recieve Early Bird Savings of $700

TREND MICRO™ | Securing Your Journey to the Cloud

See ad page 7

- Trends in Targeted Attacks
- Total Cloud Protection: Securing Your Unique Cloud Journey

websense®

See ad page 11

- Websense Security Survey: IT Stresses as Data Breaches Put Jobs on the Line
- Facebook and Websense Partner to Protect Users from Malicious Links
- See how Websense ACE protects you

DELL SecureWorks

- Whitepaper: 8 Steps to Keep Your PC's Safe from Online Criminals
- Whitepaper: 10 Tips for Security in the Cloud
- The Total Economic Impact of Dell SecureWorks Managed Security Services