INFORMATION SECURITY®

FEBRUARY 2011

# Access Denied

Endpoint security is your checkpoint for device control. Here's what you can do.

also

2011 PRIORITIES AND ROLES

SCADA SECURITY IN THE CROSSHAIRS

TechTarget

INFOSECURITYMAG.COM


CDW


CORE
SECURITY TECHNOLOGIES


Guidance
SOFTWARE
The World Leader in Digital Investigations


ISACA
Trust in, and value from, information systems


SOPHOS

# contents

FEBRUARY 2011
VOLUME 13 NUMBER 1

## FEATURES



## DEPARTMENTS



## ALSO

SOPHOS


SECURITY SO SIMPLE YOU FEEL

# INVINCIBLE

WORRY LESS. ACCOMPLISH MORE. WWW.SOPHOS.COM

SOPHOS

simply secure

# The Patient is Alive and Well

*Automation hasn't killed the penetration tester—yet.*

BY MICHAEL S. MIMOSO



**THE MALINGERING DEBATE** over the viability and lifespan of penetration testing as an art form and penetration testers as a species is getting tiresome. Tiresome because those doing the arguing generally confuse terms, juxtapose vulnerability management with pen-testing, and generally don't understand what white-hats do during an enterprise poke-and-probe.

Let's get it straight once and for all: Pen-testing is not dead.

Some vendors and expert types would like you to believe that and will try some Jedi mind-tricks to convince you—for only a second, hopefully—that you can, for example, automate penetration testing. You can't.

Automated scans are great and are the center spoke of vulnerability management programs. They help with asset discovery and generally are good at telling you what machines are lacking which patches and if you've got a cockeyed configuration or two. But that's not a pen-test, and too many companies are confounding that as a pen-test.

Pen-tests are conducted by people who are contracted to infiltrate your organization and hammer away until they get in.

Pen-tests are conducted by people who are contracted to infiltrate your organization and hammer away until they get in. They assume the profile of an attacker and use the same tactics and technologies a persistent attacker would—and that includes vulnerability scanners, commercial and home-grown exploit tools, social engineering, bolt cutters, lockpicking kits, glasses and a fake nose, and lots more. And that's generally preceded by a bit of reconnaissance against the target.

Usually, pen-tests are carried out in context of consequences to the business. At the end, you got a pretty hefty document illustrating how Swiss-cheesy your network is and sometimes for added measure, you're handed the list of customer data you challenged the pen-tester to dig up from your unbreakable systems.

It's an eye-opening interaction. It's also expensive and usually reserved for the biggest and most resourceful of enterprise IT organizations. And some of that it is to blame for all this pen-testing-is-dead nonsense. So are regulations such as PCI DSS, which mandates annual pen-tests done by "a qualified internal resource or qualified external third party" and against the network and applications. As one of our resident experts Diana Kelley points out

in a recent blog post: "Show me where in there it says that the test should simulate an actual attack? How about where it says the test should be high quality? Or that it shouldn't leverage automation almost exclusively? Nope. If you're doing the testing solely to satisfy the requirement, your decision will be driven probably by economics within the parameters of the audit standard."

There's the rub, and it goes back to another tiresome security meme that companies prioritize compliance and think they're simultaneously secure. PCI's mandates are a minimum standard, yet organizations extrapolate that to "since we passed the audit and earned certification, aren't we secure too?"

Pen-testing isn't dead. But it is changing. David Kennedy, a corporate security manager, summarized a recent BSides Atlanta presentation he and Eric Smith did on the evolution of the art form on his SecManiac blog. From an economic perspective, companies are finding it tough to resist automated pen-tests. He wrote: "How do you go against a cheap vulnerability scan penetration test to something that will cost significantly more than that and be done right. Businesses don't understand the difference, they just go with the cheapest buyer, they don't know what they are about to purchase sucks."

Automated attacks don't test the effectiveness of awareness training and whether your admin will spill your password with some gentle coaxing.

Vendors such as Core Security and Rapid7 (Metasploit) are doing their best to automate the process by converging vulnerability scanners and exploit frameworks in order to turn your IT guys into pen-testers. Val Smith, founder of Attack Research, wrote recently on the Carnal 0wnage blog that organizations have a vested interesting in conducting a low quality test in order to pass a PCI audit, for example. Smith wrote: "Therefore hiring people who can emulate real attackers is overkill, too expensive, and likely to produce a test in which they fail, requiring a costly corrective action plan. Since these customers are the ones paying the money, they are what is driving and will continue to drive the industry."

Automation, however, removes the human element that distinguishes penetration tests. Automated attacks don't test the effectiveness of awareness training and whether your admin will spill your password with some gentle coaxing. Automation won't think on the fly and understand your business and conduct attacks in that context.

Pen-testing may be changing, and more companies might be cheapening out on them. But they're not dead—they're not even on life-support.›

---

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

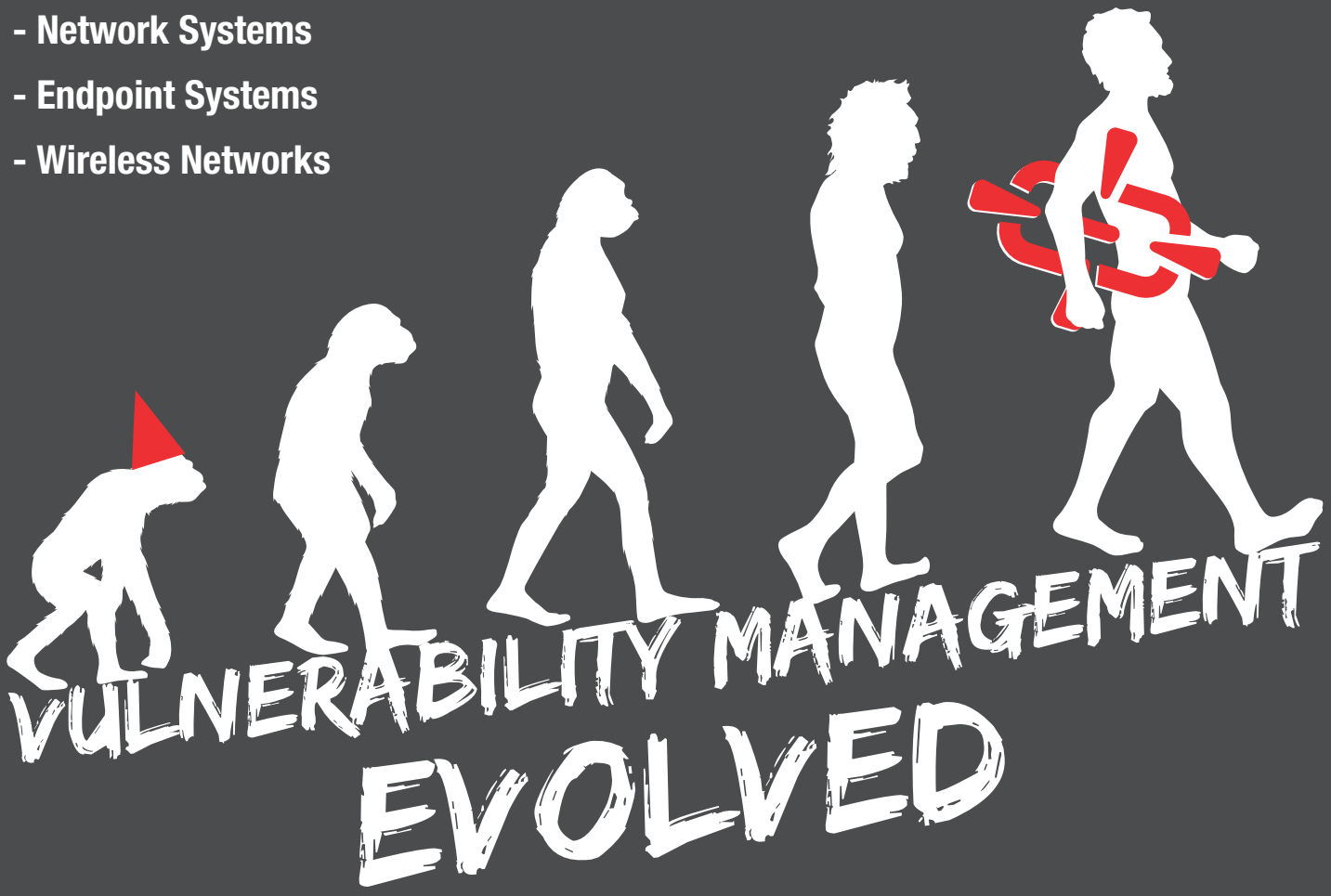
CORE IMPACT PROFESSIONAL

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

# Same Old, Same Old

*A look back at articles from the past shows that the same information security problems persist today.* BY DAVE SHACKLEFORD



**THE WORLD OF INFORMATION** security moves at a rapid pace. New threats emerge, new vulnerabilities have become a constant, and new technologies are built to protect our assets. However, many of the challenges we face, as well as the technologies we rely on, are only variations and adaptations of those we've had a decade ago.

I tend to be a packrat, as well as a bit of an information security history buff, and it was no surprise when I recently came across a stack of old *Information Security* magazine issues in my office with dates ranging from 2001 to 2003. Taking a trip down memory lane, I flipped through several issues to see what the major topics and trends at the time were. The good news is that a number of articles are still applicable in many ways today. Unfortunately, that's also the bad news. After reading some of the articles, I was a bit depressed about the apparent lack of progress we're making in information security. Here are several examples:

- "New Directions in Intrusion Detection" (August 2001): 85 percent of respondents to a reader poll had IDS installed, and most said that it was both important and reasonably good at protecting them. At the same time, the vast majority wanted more "intelligent attack analysis" and fewer false positives. The "new directions" that followed included "meta detection" or a powerful central console (today this is largely what drives the SIM market), using hardware appliances instead of software (today this is largely the norm), and network flow mirroring for IDS (our switch backplanes can handle this now).
- "Mastering Your Own Domain" (August 2001): This article describes DNSSEC and why the Domain Name System is a security issue. Brad Johnson of SystemExperts is quoted in the article saying, "if a hacker can trick a namespace manager [DNS], he can redirect traffic without the users ever knowing it." Sounds like 2008, when researcher Dan Kaminsky revealed his now famous cache-poisoning bug. Although implementing DNSSEC is a very large and difficult task, we have known DNS has issues for many years. Kaminsky's attack was simple—why didn't someone catch that?
- "Feeling Vulnerable?" (Feb 2002): The premise of this article is that sound vulnerability management practices can help cut down on alerts. The four-step process is basic: Inventory your systems, manage the flow of information (focus on what is relevant, in other words), assess the information (evaluate the risk), and plan for response. Sound familiar? It's the same fundamental vulnerability management process we're prescribing today! Most organ-

izations aren't doing a good job of vulnerability management, either—many "system inventories" I encounter while consulting are outdated spreadsheets. The problem keeps getting worse from there—focusing on vulnerabilities and managing risk is difficult for systems you don't know about. Most of the focus in the "plan for response" stage consists of patching and configuration management, and this is an area that is still woefully lacking in many organizations.

- "Practice Safe Software Coding" (September 2001): Gary McGraw and John Viega describe ten principles that still stand as best practices today. Concepts like failing securely, compartmentalizing code, using well-known crypto algorithms, and scrubbing code to remove sensitive data are all as valid today as they were in 2001—so why are we still having such a hard time following these recommendations?

We are not doing a good job of conveying the severity of the issues, convincing people to change behaviors, and building security into technology transparently.

To be fair, many of the most pressing issues in information security are complex and difficult to solve, and we've had our fair share of victories over the last decade, as well. For example, we've done a lot to curb fast-spreading worms and spam, VPNs are commonplace, and use of hard drive encryption is growing. However, the major themes are the same—secure code and coding practices are rare, signature-based IDS still needs tuning, and critical protocols and services need intense scrutiny to find weaknesses before attackers do.

Beyond just the technical issues, our greatest failure is actually more of a people problem. We are not doing a good job of conveying the severity of the issues, convincing people to change behaviors, and building security into technology transparently. Until we find better ways to convince people of security's importance, we'll likely keep fighting the same battles for a long time to come.›

---

*Dave Shackleford is a consultant and also a certified SANS instructor. Send comments on this column to feedback@infosecuritymag.com.*

ANALYSIS | MOBILE SECURITY

# Mobile Security Needs Different Approach, Experts Say

*Companies lack the tools to control the onslaught of mobile devices in the enterprise.* BY ROBERT WESTERVELT




**EMPLOYEES ARE BRINGING** smartphones into the office in greater numbers and they expect them to connect to the company network, but experts say IT security professionals are hard pressed to ensure the devices don't pose an additional data leakage risk.

That trend, coupled with predictions that mobile attacks could pose a major threat in 2011, are prompting some experts to point to emerging technologies to protect the devices and the corporate data that flows through them. Smartphones and tablet computers, such as the Apple iPad, have a relatively small footprint and lack the CPU power and bandwidth necessary to apply traditional security technologies, says Winn Schwartau, a noted security expert who sits on the board of directors of Mobile Active Defense, a fledgling security vendor attempting to address corporate use of mobile devices.

"The early testing of how to exploit these devices is well under way," says Schwartau. "Now is the time to really start looking at how you are going to start locking these devices down because the devices are here to stay, the bad guys are here to stay and if you choose to reject the last 30 years of history, it's on you because the bad guys are coming."

Many of the technologies designed to protect mobile devices will focus on network-based security, says Patrik Runald, senior manager of security research at San Diego-based Websense. In addition to device encryption and the ability to wipe devices if they are lost or stolen, many IT security professionals are dealing with the multitude of mobile platforms by forcing corporate data to flow through a VPN, Runald says. The Apple iPad's executive appeal, coupled with the fact that company executives want to access corporate email and servers with the device, make it a prime target.

"I believe that sometime in 2011 we'll see a targeted attack using the iPad as the platform to get into the network," Runald says. "The iPad will be hit using a zero-day via a targeted attack and used to launch a much broader attack on a company network."

The potential threat has forced James Leeder, senior manager of information security at a Michigan-based manufacturing firm, to limit access to corporate email and other servers from BlackBerry devices. But Leeder says his company usually takes a cautionary approach to new technology.

"No one has been asking to connect with other devices, but that's because they know the answer is going to be no," Leeder says. "We're not yet comfortable enough to go down that road."

Network security expert Marcus Ranum, CSO at Tenable Network Security, agrees that it's only a matter of time before smartphones and other portable devices are used as a launching pad for an attack in the enterprise. An employee is going to lose an iPad and it's likely that some of the information they browsed to will be cached locally, says Ranum. "The big part of the problem is that a lot of these devices being produced don't have security features at all."

"Everyone asks why I'm so cynical and dark about this and I tell them that it's just a probability thing," Ranum says. "If you've got 4,000 employees and you allow people to carry work data around with them, you know that at the very minimum someone is going to lose it."

"Everyone asks why I'm so cynical and dark about this and I tell them that it's just a probability thing. If you've got 4,000 employees and you allow people to carry work data around with them, you know that at the very minimum someone is going to lose it."

–MARCUS RANUM, CSO, Tenable Network Security

Companies are now supporting up to five different device platforms, making security policy enforcement difficult, says Ahmed Datoo, vice president of marketing at Fremont, Calif.-based mobile management company Zenprise.

"It's not out of the question to say a CFO could be using a WiFi network at café to check revenue numbers of his company for that quarter," Datoo says. "All of a sudden the enterprise no longer has control of its security model."

---

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


CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

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

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

## Recognition • Success • Growth

**June Exam Date:** 11 June 2011
**Early-Bird Registration Deadline:** 6 April 2011

ISACA®
*Trust in, and value from, information systems*

# The Fake Antivirus Scourge

by *Information Security* staff

Fake antivirus software is growing by leaping and bounds on the Internet and criminals are reaping profits, according to researchers at PandaLabs, the research arm of Panda Security. Rogue antivirus, which tricks users into believing their computers are at risk, emerged just four years ago but today makes up about 11.6% of all malware, they report. Forty percent of all fake antivirus programs were created in 2010 and Panda estimates that criminals are raking in $34 million a month from the stuff. Some examples of how criminals pushed rogue antivirus in 2010:

**Bogus Amazon messages** A fake Amazon email message about a Sony VAIO laptop order included an attached file of supposed tracking information that duped people into downloading a fake antivirus program last March, according to security researchers at Sophos.

**Spoofed warning pages** Criminals pushing rogue antivirus used a spoofed version of attack warning pages used by Firefox and Google Chrome to block users from visiting malicious websites, researchers at F-Secure and Websense reported in October. The fake attack page included what appeared to be a link for a browser update download but instead downloaded phony antivirus software.

**Twitter virus scam** In December, fake Twitter accounts tweeted messages touting an antivirus program with a shortened URL link that if opened appeared to be a Firefox security alert but was actually a fake antivirus popup, PandaLabs researchers said. The popup tries to fool users into thinking it's performing a virus scan and buying the rogue antivirus software.

**Ransomware scheme** PandaLabs in October uncovered a fake antivirus program that tried, after a computer was infected, to force a user to buy the bogus software before it would allow the user to access any files on the system. When a user tried to open a file, a message popped up claiming the application was blocked due to infection.

overheard

"In general, we're seeing the overall spend on information security remains somewhat slack…It's moving slightly upwards, but the fact is there is a lot more responsibility being put on security managers to use that spending efficiently."

–KHALID KARK, vice president and research director, Forrester Research


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

Earn ISACA's Certified in Risk and Information Systems Control™ (CRISC™) designation and gain the rewards of recognition and career advancement. Apply for grandfathering until March 2011.

***www.isaca.org/crisc-infosecmagazine***

**The right balance for your career.**

ISACA®
*Trust in, and value from, information systems*

# FACE-OFF

SECURITY EXPERTS **MARCUS RANUM & BRUCE SCHNEIER** OFFER THEIR OPPOSING POINTS OF VIEW

# Should network security be based on blacklisting or whitelisting?



## POINT: MARCUS RANUM

In 2007, I wrote an article on execution control in which I explained why antivirus was a dead-end idea, and predicted an eventual switchover from blacklisting to whitelisting. I couldn't have been more wrong so I periodically catch myself wondering if I'm one of a small percentage of the people who "get it," and if the entire security world has its collective head where the sun doesn't shine. Obviously, malware is a big problem and there's not going to be a silver bullet solution to it, but the industry's response to system integrity continues to be ineffective, expensive and a wasteful of time and energy.

**The effectiveness of blacklisting depends on the depth and accuracy of the blacklist, and the effectiveness of whitelisting depends on your ability to assess what should be allowed on the whitelist.**

**–Marcus Ranum**

To briefly recap: blacklisting is the oldest algorithm in computer security. Know what's bad, develop a pattern-matching system to detect it, and ring a bell when you detect the pattern. You can earn extra credit for detecting the bad thing just before it happens, and preventing it from happening. In a nutshell, that's what's behind many antivirus, intrusion prevention/detection systems, and spam filters. The whitelisting approach is the opposite—have a list of authorized/known good things, and permit only those. The effectiveness of blacklisting depends on the depth and accuracy of the blacklist, and the effectiveness of whitelisting depends on your ability to assess what should be allowed on the whitelist.

One of the standard complaints against whitelisting is that it's too difficult to manage the whitelist. That may be true, but it's also difficult to manage the occasional outbreaks of malware and targeted malware that slide past blacklisting systems. I don't think organizations make an effective assessment of the time spent managing their runtime environments—as the tax man says, "You can pay me now, or you can pay me later." When you

add the cost of data leaks and customer data leak notifications, it seems absurd to me that so many enterprises continue to treat their runtime environments as "anything goes."

In the real world, we see whitelisting effectively used for very huge, significant applications. Consider passports as an application of whitelisting at a national border: If you're on the authorized-citizens list, you have a passport for the country you want to enter, and if you're carrying an allied passport, you're on the greylist. And, of course, you could be on the blacklist/watchlist. Passports are not anywhere near as accurate as execution controls can be, because they're easier to forge, but obviously they can be managed in the large—the very large—with a bit of attention to detail. I think primarily what's lacking is the willpower to fight the political battle of convincing users that "this is a corporate asset, not your personal computer."

Consider another application of whitelisting: app stores. While enterprise IT has continued to blithely assert that taking control over its runtime environment is too difficult, smartphone users have bought into a number of "walled garden" software distribution models. I know there are still users who see that as a "jail," but the infrastructure is slowly getting put in place where maybe, just maybe, we'll see a shift from "trust whatever you run" to "run whatever you trust." If the model fails, it'll fail because a vendor gets greedy and goes for a market lock-out that encourages rampant jail-breaking to circumvent a software monopoly. As we've seen, however, people don't seem to mind a monopoly, as long as it lets them get what they want at a reasonable price with a minimum of effort.

**Rather than taking control of the desktop, IT managers wring their hands and say "It's too hard!"**

**–Marcus Ranum**

Willpower appears to be short in supply at the enterprise level. Rather than taking control of the desktop, IT managers wring their hands and say, "It's too hard!" At the same time, they complain it's difficult to get good employees if you don't let them keep up with Facebook and Twitter all day—which, if you think about it for a second, is nearly oxymoronic. A couple years ago, I worked on a project involving some massively expensive robotic devices that had been infected because one of the maintenance personnel had malware on his laptop, which he plugged into the robot's control network. Management at the company said it was difficult to control personal use of the laptops, but recognized the impact to its business was extremely expensive. The irony of the whole situation was that they only had six maintenance engineers in the first place—they had lost millions of dollars in order to save the cost of six locked-down netbooks that could have stayed in the toolbox with the other maintenance gear, instead of in the engineer's briefcase. I see this kind of failure over and over again in the industry: point-of-sale terminals unlocked get drive-by malware and require a customer data exposure notification, engineer carries Stuxnet into a SCADA network on laptop, etc.; penny wise and pound foolish, indeed.

What do I think is going to happen? We're going to see the divide between controlled and uncontrolled environments continue to deepen. There have already been many instances of malware in app stores; I'm betting we'll start seeing more interest by app store providers

in vetting the software better. Meanwhile, enterprise IT will keep getting owned, as antivirus technology falls further and further behind. The endgame may come in a few years, when—after a great deal of nail-biting—security technologists are in the unpleasant position of having to recommend executives use an iPad instead of a laptop—switch to an embedded device instead of a general-purpose operating system, and keep your e-mail "in the cloud" rather than on the device. In other words, the antithesis of everything many of us currently think makes sense. It could happen. And I'm sure Bruce (and plenty of you) will be happy to let me know I'm wrong.›

---

*Marcus Ranum is the CSO of Tenable Network Security and is a well-known security technology innovator, teacher and speaker. For more information, visit his website at www.ranum.com.*



## COUNTERPOINT: BRUCE SCHNEIER

The whitelist/blacklist debate is far older than computers, and it's instructive to recall what works where. Physical security works generally on a whitelist model: If you have a key, you can open the door; if you know the combination, you can open the lock. We do it this way not because it's easier—although it is generally much easier to make a list of people who should be allowed through your office door than a list of people who shouldn't–but because it's a security system that can be implemented automatically, without people.

To find blacklists in the real world, you have to start looking at environments where almost everyone is allowed. Casinos are a good example: Everyone can come in and gamble except those few specifically listed in the casino's black book or the more general Griffin book. Some retail stores have the same model—a Google search on "banned from Wal-Mart" results in 1.5 million hits, including Megan Fox—although you have to wonder about enforcement. Does Wal-Mart have the same sort of security manpower as casinos?

**Computer networks share characteristics with your office and Wal-Mart: Sometimes you only want a few people to have access, and sometimes you want almost everybody to have access.**

**–Bruce Schneier**

National borders certainly have that kind of manpower, and Marcus is correct to point to passport control as a system with both a whitelist and a blacklist. There are people who are allowed in with minimal fuss, people who are summarily arrested with as minimal a fuss as possible, and people in the middle who receive some amount of fussing. Airport security works the same way: The no-fly list is a blacklist, and people with redress numbers are on the whitelist.

Computer networks share characteristics with your office and Wal-Mart: Sometimes you only want a few people to have access, and sometimes you want almost everybody to have access. And you see whitelists and blacklists at work in computer networks. Access control is whitelisting: If you know the password, or have the token or biometric, you get

access. Antivirus is blacklisting: Everything coming into your computer from the Internet is assumed to be safe unless it appears on a list of bad stuff. On computers, unlike the real world, it takes no extra manpower to implement a blacklist—the software can do it largely for free.

Traditionally, execution control has been based on a blacklist. Computers are so complicated and applications so varied that it just doesn't make sense to limit users to a specific set of applications. The exception is constrained environments, such as computers in hotel lobbies and airline club lounges. On those, you're often limited to an Internet browser and a few common business applications.

Lately, we're seeing more whitelisting on closed computing platforms. The iPhone works on a whitelist: If you want a program to run on the phone, you need to get it approved by Apple and put in the iPhone store. Your Wii game machine works the same way. This is done primary because the manufacturers want to control the economic environment, but it's being sold partly as a security measure. But in this case, more security equals less liberty; do you really want your computing options limited by Apple, Microsoft, Google, Facebook, or whoever controls the particular system you're using?

Turns out that many people do. Apple's control over its apps hasn't seemed to hurt iPhone sales, and Facebook's control over its apps hasn't seemed to affect Facebook's user numbers. And honestly, quite a few of us would have had an easier time over the Christmas holidays if we could have implemented a whitelist on the computers of our less-technical relatives.

For these two reasons, I think the whitelist model will continue to make inroads into our general purpose computers. And those of us who want control over our own environments will fight back—perhaps with a whitelist we maintain personally, but more probably with a blacklist.›

---

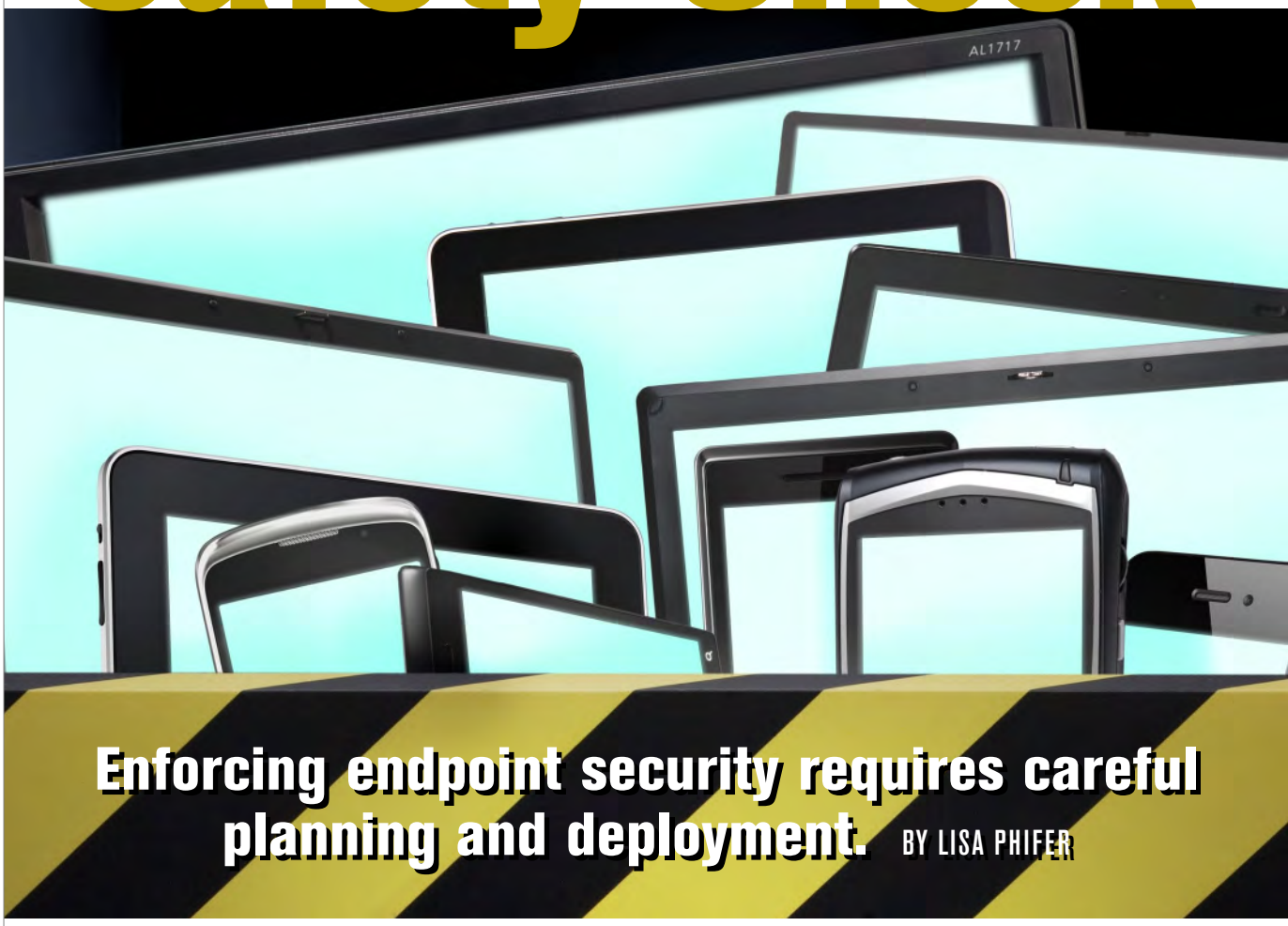
*Bruce Schneier is chief security technology officer of BT Global Services and the author of* Schneier on Security. *For more information, visit his website at www.schneier.com.*


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

**Trust no one except us at CDW.com/security**

CDW PEOPLE WHO GET IT

# Safety Check



## Enforcing endpoint security requires careful planning and deployment.

BY LISA PHIFER



**MALWARE-INFESTED**, non-compliant endpoints can bring even a well-secured network to its knees unless steps are taken to assess and prevent damage. Checking the health and posture of every IP-enabled device connected to a network then taking action to enforce compliance may be a simple concept, but deployment can be tricky.

According to Forrester Research, 40 percent of enterprises have started network access control (NAC) initiatives in which endpoint integrity can play a role, but only four percent have completed them. Many promising projects are abandoned, victims of overly-ambitious goals, ineffective implementations, or inter-organizational struggles.

So what does it take to plan, implement, and maintain a practical-yet-effective endpoint integrity enforcement program? We asked several adopters about their experiences to uncover the secrets to success and pitfalls to avoid. These diverse implementations served varied populations but all employed some essential best practices. *(See p. 22)*.

## THE FALL AND RISE OF INTEGRITY ENFORCEMENT

Endpoint integrity has never been more essential—or challenging to enforce. Between wireless mobility, bring-your-own phones, and a dizzying array of IP-enabled devices, everyone faces a daily influx of unknown, potentially risky endpoints. Enforcement through IT ownership is no longer feasible, and endpoint measures that do get deployed cannot disrupt business unless serious damage is imminent.

Many organizations that pursued NAC to enforce endpoint integrity backed off when users cried foul and help desks became overloaded. "In earlier deployments, NAC tended to be like an on/off switch, which proved too extreme in some cases—nobody wants to be the person who blocked the CEO," says John Sheedy, marketing manager for Bradford Network's Network Sentry appliances.

Soon, the primary goal for most new NAC deployments became guest access—basic friend-or-foe assessments that directed trustworthy insiders onto privileged segments while sending everything else to the Internet. Managed endpoints often received closer scrutiny, but guests did not. "Quarantine just involved way too many organizations and too much effort," says Mark Townsend, director of solutions management at Enterasys, and co-author of the Trusted Network Connect (TNC) Clientless Endpoint Support Profile.

But with BYO endpoints like iPads, Townsend is seeing growth in *guest-plus* access. In a nutshell, any device carried by a known user may be subjected to cursory assessment then granted better-than-Web access, followed by monitoring. "For cloud-based apps, you don't want to resort to screen-scraping to [detect] malware. This is giving rise to post-connect, continuous assessment, layer 7 flow analysis, and reputation-based rules," says Townsend.

### Best Practices

**Organizations offer nine tips for successful endpoint security enforcement initiatives.**

1. Build your business case and use it to define project goals.
2. Involve all stakeholders from the start (avoid silos).
3. Identify use cases, mapped to business goals.
4. Pick low-hanging fruit first.
5. Maximize transparency, minimize disruption.
6. Be realistic about assessment (no one size fits all).
7. Phase in enforcement: crawl, walk, run.
8. Leverage existing network/security investment through reuse.
9. Seek opportunities to integrate, share, and mine endpoint knowledge.

## BIGGER BANG FOR THE BUCK

In fact, every organization we interviewed had gone beyond malware to reap benefit from endpoint assessment. For example,

Miami Children's Hospital, a pediatric specialty facility, started endpoint integrity enforcement in 2004 to meet regulatory requirements.

"Our primary goal was to make sure we had proper controls over devices on our network," says IT Security Officer Alex Naveira. "We began with a rudimentary process, trying to leverage an old [port manager] that put machines on different networks, based on MAC. But that didn't give us the level of control we needed and wasn't very efficient."

When the hospital installed ForeScout CounterACT to enable out-of-band NAC, audit-mode reports were enlightening. "We expected about 3,000 devices, but discovered over 5,600," says Naveira. "That alone was a huge benefit. Plus, now we had the ability to quickly segregate those devices to better control traffic flows."

Today, the hospital maps endpoints onto VLANs by divvying them into three camps: guests (e.g., patients, families), personal (e.g., physicians, vendors), and hospital-owned (e.g., phones, clinical devices). Every endpoint discovered by CounterACT falls into an "other" bucket with Internet access. "A security engineer monitors that bucket to see whether any should be authorized and placed on a segregated VLAN," says Naveira.

All hospital-owned endpoints then receive ongoing scans. "We have structured requirements: Is antivirus installed and up-to-date, is the C: drive write-protected, are [critical] patches installed?" explains Naveira. Even checks applied in audit mode have proven valuable beyond expectations.

"The benefit of finding and fixing gaps is underestimated. About 20 percent of customers find [some endpoint measure] not working properly–as many as 50 percent of managed machines are not doing what is expected."

–JACK MARSHALL, director of marketing, Forescout

"In one case, we used a standard template to deploy multiple virtual servers. When we looked at reports, all were landing in non-compliant. Admins had forgotten to install antivirus before creating the template. That let us catch a big mistake quickly. CounterACT gives us eyes into our environment to make sure that other [measures] are being used effectively. This helps us close the gap on threats—be they caused by errors or viruses."

According to Forescout Director of Marketing Jack Marshall, Miami Children's Hospital experience is common. "The benefit of finding and fixing gaps is underestimated. About 20 percent of customers find [some endpoint measure] not working properly—as many as 50 percent of managed machines are not doing what is expected," says Marshall.

Pamela Chang, product manager for Symantec Network Access Control, sees enforcement as a complement to endpoint security. "Many customers used to just determine if laptops were corporate-issued," says Chang. "Now they look for whether [endpoint] software is actually running and current. With 20,000 to 35,000 new threats per day, a host that hasn't connected recently could be outdated." Enforcement is becoming popular to deal with this more efficiently, she says, by warning users and delivering access for safe self-remediation.

## FITTING INTO THE BIG PICTURE

Decisions can be enforced many ways. Security vendors like Symantec and Sophos emphasize host-resident agent enforcement. Network vendors like Cisco Systems, Juniper Networks, and Enterasys Networks prefer to leverage switch/access point/firewall capabilities. Drop-in appliances are sold by both camps and NAC specialists like ForeScout Technologies and Bradford Networks. Although users we interviewed had varied opinions about platforms, all stressed the importance of considering fit from the start. Essentially, organizations should pick a product that fits with their network, security platforms and processes instead of trying to work a deployment around whatever interfaces and workflows a product supports.

Pat Patterson, information security architect at Raymond James Financial, recommends a review of existing architecture and processes. "Look at how you're patching, how you're doing antivirus, and how those fit into any solution," he says. "We started with 802.1X but found that we couldn't [afford to] get that tightly coupled. We decided to integrate with DHCP because [combining] Sophos NAC with IP Source Guard made enforcement a lot easier."

"The first thing we validate is domain membership. The next thing to look at was whether antivirus was up to date, but rather than break a lot of connections right away, we moved forward an inch at a time."

–PAT PATTERSON, information security architect, Raymond James Financial

Today, Raymond James uses the Sophos NAC agent to assess LAN access by financial advisors and office staff. Remote users are assessed by Juniper's SSL VPN Host Checker. Together, these platforms govern access by 17,000 endpoints.

"The first thing we validate is domain membership," says Patterson. "The next thing to look at was whether antivirus was up to date, but rather than break a lot of connections right away, we moved forward an inch at a time. Stock traders have a tendency to get cranky if you don't let them onto the network during the trading day."

And so that policy was deployed in audit mode, floor by floor, building by building. "The most tedious part was identifying devices that couldn't play with our agent, like printers and Macs. We just had to go through switch tables to add exclusions, but it was labor-intensive," says Patterson.

"We already had systems to monitor security across our domain (like LANdesk patching), so we just make sure those agents were running on our expected domain population," he adds. Disk encryption is also checked to meet PCI Data Security Standard requirements.

Non-domain endpoints (including smartphones and iPads) get IPs on a guest VLAN, where SSL VPN can still be used for portal access. But Raymond James opted against auto-remediation. "When you boot your machine, if the NAC icon says you've been quarantined, call our helpdesk," says Patterson. Support then reinstalls certificates and agents to return broken domain machines to good health.

According to Scott Patterson, product specialist at Sophos, many Sophos NAC customers use NAC to prove lost laptop encryption. By finding a solution that leveraged what it already had (Sophos, Juniper, DHCP), Raymond James quickly checked off several compliance boxes, saving time so energy can be focused elsewhere, says Pat Patterson.

## CONTROLLING A DIVERSE ENVIRONMENT

Educational institutions were among the first to invest in endpoint assessment, because they cannot dictate endpoints. But diversity is no excuse; malware fires must still be extinguished. This challenge faced Bryant University when it first installed Bradford's Network Sentry back in 2004.

"We were coming off a homegrown system. At the time, [worms] like Blaster had decimated our network, so assessment was crucial."

–JON DOMEN, IT network analyst, Bryant University

"We were coming off a homegrown system. At the time, [worms] like Blaster had decimated our network, so assessment was crucial," explains IT network analyst Jon Domen. Bryant started with registration-time scans then moved to an agent for ongoing scans in 2007.

Later, as part of a green technology initiative, Bryant compressed most IT assets (including Bradford) into 80 virtual machines on five blade servers. Domen expects this to cut costs without impacting endpoint enforcement. "Our experience to date supports this assumption," he says.

All network entrance points are scrutinized, including 45 dorms, admin buildings, and classrooms. "We see everything from laptops, desktops, and PlayStations to eReaders and Netflix-compatible TVs. There was a time when each student had one computer, but most now have at least two. One kid came in with his own laptop, Mac, iPhone, Droid, Nokia, Palm, BlackBerry Torch, and Wii," says Domen. "As long as they adhere to our policies, we allow anything."

Bryant manages university-owned assets, but faculty can bring their own endpoints as well. "We use Bradford's Device Profiler to discover our infrastructure, and we have a program to supply students with laptops. But every device belonging to someone else must be registered; we want tracking back to users after incidents," says Domen.

For endpoints on the student network, Bryant requires nothing more than antivirus. "In 2007, we had outbreaks that left users scared. People were ready to accept persistent agents if that would prevent [downtime] again." Nonetheless, Bryant had to tackle Big Brother concerns; he found that communicating what scans looked for plays a critical role in user acceptance.

"We learned that we had to be flexible. So long as you have some antivirus—even free antivirus—we're happy," says Domen. "But it helps that we can do custom scans [to tighten controls during outbreaks]. That reactive piece lets us be more flexible on the proactive side. And, because users don't even know when they're getting scanned, I can step up frequency when something is going on."

Non-traditional devices like Wiis bypass antivirus checks, but don't pose the same threat. According to Bradford marketing manager Sheedy, Bradford's Device Profiler can associate new connections with historical data and use techniques like DHCP fingerprinting and port scans to auto-classify devices and deter MAC spoofing.

Bryant continues to find new uses for endpoint assessment. "After Virginia Tech, universities started to evaluate how they'd react. [Our agent] gives us a way to reach out to every machine on our network with just a few clicks," says Domen. "We've also been able to use audit mode to update machines running old Java. It's becoming the Swiss Army knife of our network."

## EASING ENFORCEMENT

"We connect everything from massively-parallel computing systems to vending machines. We see about 65,000 unique connections per day, including our residents, medical school, and dental school–the groups now in our assessment pilot."

–JIM GOGAN, network director, University of North Carolina at Chapel Hill

Like Bryant, University of North Carolina at Chapel Hill extended its NAC solution to mine endpoint data for other uses, including applications that let users, admins, and security officers do their jobs without having to send requests to the network group. "Our implementation of NAC is paramount to how we conduct business and manage the network on a daily basis," says network director Jim Gogan.

But UNC takes a very different approach to enforcement. A combination of agent-less and agent-based techniques are used to assess more than 10,000 endpoints—a number that is expected to grow to to 25,000 this summer. "We connect everything from massively-parallel computing systems to vending machines," says Gogan. "We see about 65,000 unique connections per day, including our residents, medical school, and dental school—the groups now in our assessment pilot."

"Our residential network is almost 100 percent user owned," says senior network engineer Ryan Turner. "In our dental school, the vast majority are state-owned, so compliance policies are very different. Our medical school is a mix, and across all areas we have unmanaged devices like printers, door controllers, and steam meters. If an authorized machine has an unsupported OS, it bypasses our endpoint integrity solution. We have tried to cover 95 percent of the machines out there."

However, UNC's Enterasys platform accomplishes "bypass" in a novel way. "Our quarantine policy doesn't flip machines into VLANs or apply ACLs. Edge user ports rewrite the Diff Serve control point in port 80 traffic—and only port 80 traffic—so that it gets forwarded to our assessment server," says Turner.

"Door controllers and such don't browse the Web, so their communication is largely unaffected. It may seem unusual to allow all but Web traffic, but it works. We didn't need to shut off email or

IM or anything else. Just preventing non-compliant machines from browsing the Web was enough of a carrot," he says.

But UNC also is concerned about peer-to-peer apps like BitTorrent and Limewire, as well as compliance mandates like HIPAA. "In the dental school, all machines were state-owned and enrolled in Active Directory, so a week before we turned on assessment, we used Group Policy Objects to push an agent to every machine," says Turner. This let UNC enforce school-specified policies like P2P bans and personal firewalls.

"When we expanded into the resnet [residential network], we had to change a lot. Not only were these machines not owned by us, but there's no paid support in dorms. We had to tread carefully to avoid isolating too many machines, and we had to use a captive portal to get our agent installed," says Turner.

UNC also needed a new result: a pop-up giving specific remediation instructions without blocking. "Our compliance rate was [significant] from that warning alone, without having to create a lot of angry customers or support tickets," says Turner. "Anything we can do to help users remediate themselves but let us verify they've done so turns out to be a win-win." UNC expects to use this same approach to promote compliance with Recording Industry Association of America intellectual property protections on the residential network.



## A VIEW INTO THE FUTURE

All of these organizations used some flavor of NAC to meet immediate needs, but none were stereotypical network NAC deployments. For example, many had interest in 802.1X, but none based their solution on this one method. All focused on endpoint needs, policies, and practices, matched to each user constituency they supported. This focus, combined with seeking out ways to make scans even more valuable, served these adopters well.

But the march towards network and system-integrated NAC continues. Analysts expect the NAC market to shrink as scanning and enforcement become widely available in endpoints and network elements. This means that the most pragmatic approaches for yesterday's deployments may not still be the easiest tomorrow.

For example, Juniper is making strides towards consolidation, using JunOS Pulse to implement access-network-independent policies, and not just for laptops, but for iPhones and Androids that roam between VPN and LAN. The Trusted Network Connect Working Group's IF-MAP is making it easier for any assessment engine to factor in real-time observations by third-party systems (e.g., IPS, DLP). Meanwhile, Cisco plans to use its TrustSec Security Group Access to bind endpoints to roles and resources, abstracted into tags that network elements can dynamically enforce without VLAN or ACL configuration.

Bottom line: Platform selection will continue to be important, but don't start there. Like these successful organizations, start from the top and think outside the box—literally.

---

*Lisa Phifer is president of Core Competence, a consulting firm focused on business use of emerging network and security technologies. Send comments on this article to feedback@infosecuritymag.com.*

## Don't Miss a Moment!

RSA® Conference 2011 begins February 14th! Thousands of security professionals will converge upon San Francisco for information security's largest conference. **Come for the day or stay for all five, there's a registration package option to meet your needs and schedule**.

- **Keynote Sessions** from top executives and industry luminaries
- **Over 200 track sessions** led by the best and the brightest in the industry
- **350 top security companies** will demo their latest products
- **Special Monday events** for Delegate Pass holders

Come for the full Conference, drop in for a day of sessions and events, or simply stop by the Expo. Don't miss out, register today.

# the adventures of alice & bob


Follow the Adventures of Alice & Bob at
**www.rsaconference.com/aliceandbob2011**

## RSA CONFERENCE 2011

20 YEARS

FEBRUARY 14-18 | MOSCONE CENTER | SAN FRANCISCO

**www.rsaconference.com/techtarg**

# Increasing Influence

*Information security managers are getting more of a say in enterprise cloud initiatives and mobile device projects.* BY MARCIA SAVAGE



**CLOUD COMPUTING** is too attractive for organizations to ignore and Caritas Christi Health Care System is no exception. The Boston-based health care organization, which provides health services to patients in eastern Massachusetts, southern New Hampshire and Rhode Island, is contemplating moving some data storage and possibly email to the cloud. Throughout the vendor evaluation process, Jim Murphy, information security officer at CCHC, is making sure critical security issues—such as encryption of data in transit and at rest—are addressed.

"I'm working closely with the systems engineering group to plug myself into those projects and conversations," he says. "Before we sign a contract, I'm trying to get security to have a seat at the table to address the risk."

In their rush to move IT services and applications to the cloud, organizations have often left security out of the decision process. But Murphy's work reflects a shifting tide, as more businesses are giving security management some degree of authority over cloud

initiatives. According to *Information Security*'s 2011 Priorities survey, 34 percent of 776 respondents said they have the ability to reject or delay cloud computing projects based on risk/threats. About 49 percent recommend or specify products and almost 29 percent have the ability to approve vendors based on security features and service level agreements.

"Businesses are savvy enough to involve security [in cloud evaluations] if they have compliance requirements or if there is sensitive data," says Khalid Kark, vice president and research director at Forrester Research.

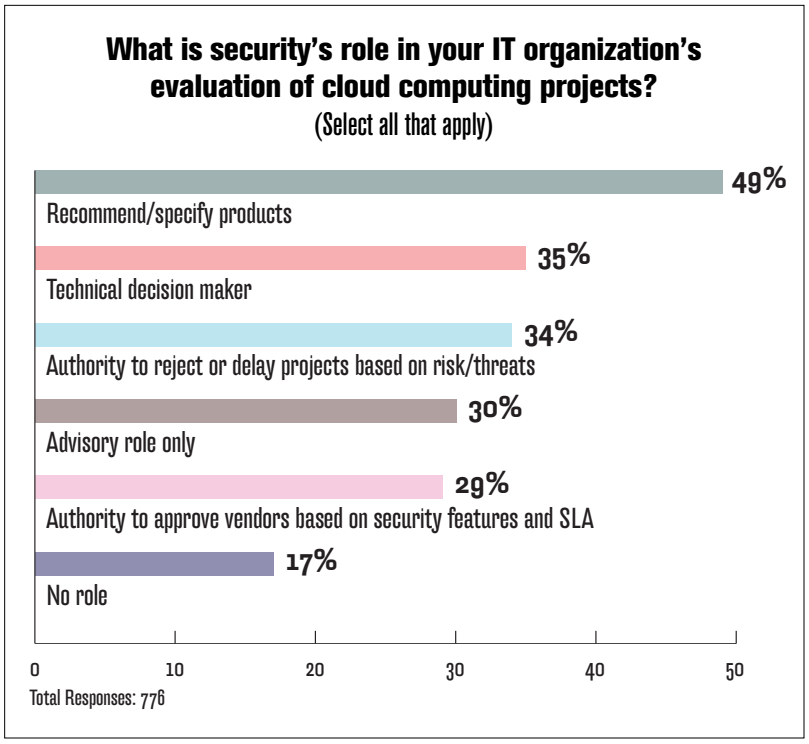
This year's Priorities survey also revealed that information security pros will be helping to evaluate enterprise mobile devices projects, spending more on network security monitoring, and ramping up disaster recovery planning. They'll also continue a shift from a technical role to a heavier focus on policy and regulations.

"Businesses are savvy enough to involve security [in cloud evaluations] if they have compliance requirements or if there is sensitive data."

–KHALID KARK, vice president and research director, Forrester Research

## ENSURING CLOUD SECURITY

Oftentimes with new technology, enterprises push ahead and security is an afterthought, says Lee Kushner, president of LJ Kushner and Associates, an information security recruitment firm, and co-founder of InfoSecLeaders.com. But information security job candidates are getting asked about their knowledge of cloud computing, indicating that companies are thinking about security at the architectural stage of cloud initiatives, he says.




Ron Woerner, a cybersecurity professor at Bellevue University and security analyst at a large architecture and engineering firm in the Midwest, says the role security plays in enterprise cloud initiatives depends on the relationship a security officer has with his or her business counterparts and whether the industry he or she is in is highly regulated.

"Those in high-risk areas or with good relationships will have more involvement in the decision-making process and thus have a greater ability to influence appropriate security controls for cloud infrastructure," he says.

In contrast to the 34 percent of survey participants who can put cloud projects on hold due to security concerns, 30 percent say they have an advisory role only.

Tony Meholic, CISO at Philadelphia-based Republic Bank, says an informal poll after a recent conference session he attended this fall showed that the size of a company has a lot of impact on security's role in cloud projects.

At smaller companies, where the information security manager wears a lot of different hats, the role was more passive than at a midsize company, where security managers tended to have more



# Full Steam Ahead

## Many organizations are making the shift to Windows 7 and its security features.


**THE MIGRATION** to Microsoft Windows 7 – and its enhanced security – appears to be in full swing this year. Sixty percent of respondents to Information Security's 2011 Priorities survey say their organization is either planning or in the middle of migrating to Windows 7.

Of the operating system's security features, 46 percent of readers said User Access Control was the most attractive to their organization. Thirty-six percent like the security isolation for services and applications that Windows 7 provides while 35 percent are impressed with the BitLocker encryption feature.

By sunsetting many of its older operating systems, Microsoft is basically forcing organizations to embrace Windows 7, says Ron Woerner, a cybersecurity professor at Bellevue University and security analyst at a large architecture and engineering firm in the Midwest. "That's not necessarily a bad thing, since Windows 7 has security features not available in Windows XP or Vista," he adds.

Microsoft UAC allows users to run with minimal privileges and only use admin or advanced privileges when necessary, Woerner says. "That will reduce one of the most common vulnerabilities: user error."

With Windows 7, Microsoft made BitLocker robust enough for the enterprise, he says, and easy to implement and support with minimal user interference. Plus, it's free with the operating system.

"For smaller companies that need some type of encryption solution, it's a bonus having this [BitLocker] built into the operating system rather than having to buy a solution," says Tony Meholic, CISO at Philadelphia-based Republic Bank.

However, Windows 7's hardware requirements are hefty, which could hold some companies back from migrating, he adds.

Due to the hardware requirements, some companies are looking to utilize desktop virtualization as a way to move to Windows 7.

The best way for us to get there is with desktop virtualization," says Lyndon Brown, IT director at pet supply retailer PETCO. "We're pretty integrated with virtualization technologies today, so it wouldn't be a huge investment to build that out."

–MARCIA SAVAGE

OS security

leverage to delay projects due to security issues. Infosecurity executives at large enterprises appeared to have the most influence on cloud projects, he says. None, however, could kill a project outright.

"Cloud computing is going to happen. It's not going to stop," Meholic says. "The best an information security professional can do is make sure you're part of the process as early as possible and participate as much as you can to make sure things go in the right direction."

Some organizations are planning to devote more resources to cloud security this year: 17 percent of survey respondents say their organization will spend more on securing the cloud in 2011.

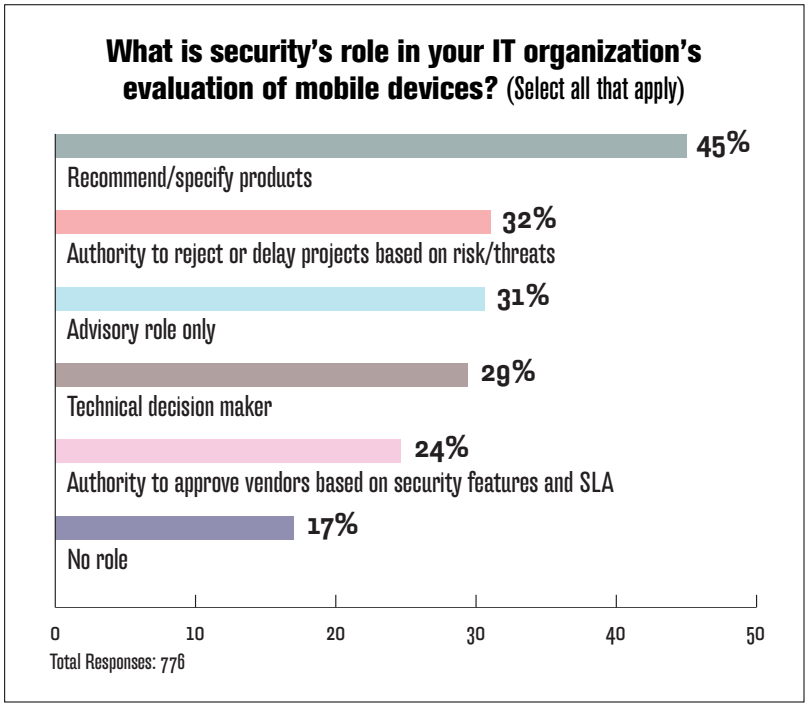
## CONTROLLING MOBILE DEVICES

While security professionals wrestle with the security implications of cloud computing projects, they also are contending with the proliferation of mobile devices in the enterprise. More and more employees are bringing their iPhones, iPads, and other devices into the workplace and senior executives are eager to use the latest technology.

> "Unlike many years ago, when security was an afterthought, it's an initial thought."
>
> –PHIL COX, principal consultant, SystemExperts

When it comes to their role in enterprise evaluation of mobile devices, 45 percent of survey respondents say they recommend or specify products. Thirty-two percent say they have the authority to reject or delay mobile device projects based risk/threats. Thirty-one percent have an advisory role only.

Senior executives are making security a priority in their adoption of mobile devices and telling security teams to figure out how the company can use the devices securely, says Phil Cox, principal consultant at security consulting firm SystemExperts. "Unlike many years ago, when security was an afterthought, it's an initial thought," he says.

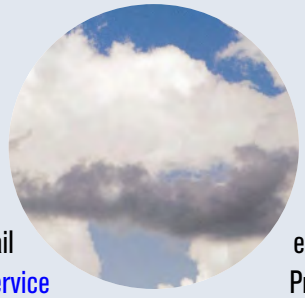



Indeed, Kark says he was having a conversation with a CISO when the CISO got a call from his company's CEO who said the board had decided to use iPads and wanted the CISO to figure out how to secure them.

However, Kark says he sees security being pushed more to the backseat on mobile device projects. The pressure from higher ups to support various devices is high while mobile

# Streamlined Security

**Retailer makes the switch to cloud-based email security to reduce costs and maintenance burden.**



**PETCO WAS LOOKING** to cut data center costs when its in-house email security supplier Proofpoint approached the company about its cloud-based service. The idea of switching from on-premise email security appliances to a software-as-a-service suite made a lot of sense, says Lyndon Brown, IT director at PETCO.

"If we can start moving to the cloud, we can shrink our footprint in our data centers and shrink the costs associated with that as well as maintenance costs," he says. Also, IT can better focus on serving core business needs, he adds.

So after taking a hard look at Proofpoint's SaaS offering, PETCO moved ahead and transitioned from its on-premise anti-spam and antivirus email protection systems, which were integrated with email encryption appliances, to the cloud-based Proofpoint Enterprise Protection and Proofpoint Encryption services. The services provide inbound email security and outbound email encryption for PETCO's email system at the network edge.

Proofpoint offered flexibility that other vendors couldn't, Brown says: "Because each business has its different needs, end user flexibility is key in these solutions."

SaaS-based email security isn't new, Brown says. He was familiar with the technology before cloud became the buzz word of the day. Email security is a natural fit for a cloud environment, he says.

"In my experience, it's one of the easier things to decide on moving to the cloud, especially if you're just trying to get your feet wet," he says. "It's a good opportunity to get used to how something works in a software-as-a-service model." ›

–MARCIA SAVAGE

use is so ubiquitous across an organization that it's hard to manage, he adds.

Mobile devices are tricky because many don't have adequate security protections as part of their basic infrastructure, Woerner notes.

"Mobile devices are just handheld computers that can access many of the same services that you do with a standard computer. The problem is that most users have admin privileges on these devices, so they can do what they want with them," he says. "Additionally, there's little malware protection or DLP available on mobile devices. On top of that, people are using their personal devices for work. This is a huge dilemma for security that will only become more prevalent in 2011."

At CCHC, a group uses iPod Touches to work with non-English speaking patients and Murphy says work is underway to figure out how to provide a secure wireless connection so the group can securely transfer information.

Also, the organization uses BlackBerry Enterprise Server but needs to be able to address unsupported devices like iPhones, Murphy says. The Massachusetts data protection law makes it especially critical that the organization secure mobile devices, he adds.

## NETWORK SECURITY MONITORING

Cloud computing and the explosion of mobile devices are pushing corporate boundaries far beyond the traditional network perimeter, but many companies plan to step up their network security vigilance in 2011. Almost a quarter of readers surveyed say their organization will increase spending

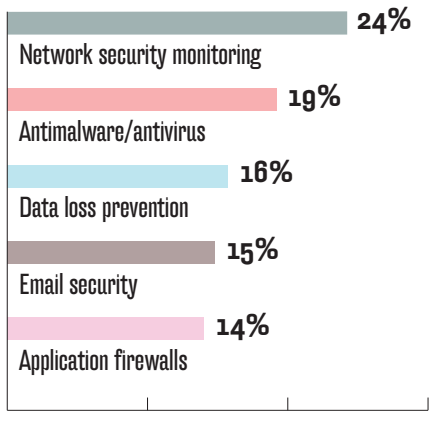
**True or False:**

**Over the last two years, my role has shifted from highly technical/implementation focused to a heavier focus and involvement on policy, regulations and legal issues.**

**55% True**
**45% False**

Total response: 777

**Over the 12 months, which of the following technologies/areas will see the largest percentage increase (year over year increase) in security spending across your entire organization?**




Total Responses: 765

on network security monitoring over the next year.

Rich Popson, information security manager at a health care organization, says traditional "block and tackle" firewall and intrusion prevention tools aren't cutting it. "There are too many false positives with traditional monitoring tools that cause headaches for us," he says. The organization recently bought a network security monitoring product from NetWitness to complement its security information management system and application-aware firewall.

Having additional visibility into network events enables the security team to focus on high-risk incidents, he says. "Visibility gives you the proof," Popson says. "You can say, 'This is exactly what happened'."

Forrester's Kark says the buzz around the advanced persistent threat (APT) and federal compliance requirements are driving companies to spend more on network security monitoring. Changes in Federal Information Security Management Act (FISMA) requirements emphasize the need for more frequent security reporting, leading to a continuous monitoring mantra, he says. That spawned off a subcategory in the security industry in which vendors tout network security monitoring and APT detection.

"Some of that [monitoring] is necessary, but if I'm a CISO, I wouldn't necessarily put a lot of my focus on the network," Kark says. "Much more risk lies in the application layer."

Beyond FISMA, other regulations are leading companies to spend more on network security monitoring, says Jonathan Gossels, president and CEO of SystemExperts. Most regulations like the PCI Data Security Standard and HIPAA include monitoring requirements, he says.

"It was one of those things that kept falling off the plate and now it can't fall off the plate," he says.

At the same time, some enterprises plan to spend more on antivirus and antimalware technology, a trend Gossels says makes perfect sense in an environment where threats are multiplying. Nineteen percent of survey respondents say they plan to spend more on such products in 2011.

Murphy says antimalware was a big priority for CCHC last year, when it replaced an underperforming system with Sophos Endpoint Security and Data Protection, which he says has been proactive in catching malware.

## DISASTER RECOVERY AND DATA SECURITY

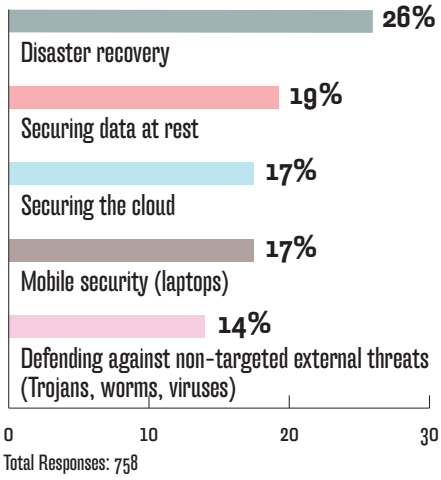
While compliance drives a lot of security initiatives, it's also is a major factor behind organizations' efforts to boost their disaster recovery planning this year, security experts said. Twenty-six percent of survey respondents said their organization would spend more on disaster recovery.

"Every regulation has a business continuity component to it," SystemExpert's Gossels says. "It's not that companies didn't have plans, but often they weren't formalized. Now it's required that they're formalized and practiced. It takes money to formalize things."

Meholic says disaster recovery planning is an onerous task that not a lot of people really enjoy but must be done. "There's a big push from regulatory agencies to have completed disaster recovery plans," he adds.

For CCHC, though, having a robust disaster recovery plan is more about best practices than compliance. "Since we are a hospital, we have to provide 24x7 availability to our applications," Murphy says.

**Over the next 12 months, which of the following priorities/business drivers will see the largest percentage increase (year over year increase) in security spending across your entire organization?**




Securing data at rest—in storage, databases, servers, and mainframes—was ranked as a priority by 19 percent of survey respondents. Meholic says securing data at rest is one of his top concerns. Some of the big security breaches have involved attackers accessing unsecured stored data, he notes.

"Whenever I do a security review, one of my first questions is about whether the data is secure at rest," he says.

Encrypting stored data costs money and business executives may be concerned about its impact on the user experience, but the time added is milliseconds, Meholic says. "If it's seven seconds instead of five, you're not going to notice," he says.

## ONGOING ROLE SHIFT

As information security professionals juggle multiple security initiatives and compliance mandates, their role in the enterprise continues to shift from technical operations to strategic, policy-oriented responsibilities.

Fifty-five percent of survey respondents say their role has shifted from a highly technical and implementation focused one to having a heavier focus on policy, regulations and legal issues. The role shift is a trend that's been ongoing for several years, security experts say.

"Instead of people being dedicated to hands-on security work, most security professionals are in charge of setting policy, evaluating technologies and dealing with regulations," Gossels says. "The day-to-day security operations have been increasingly rolled into other IT operations."

Woerner says he noted the need for security to focus on risk management and operate at the strategic level in *Information Security* five years ago.

"This trend continues today as more security professionals realize the necessity to understand and utilize risk management practices in their day-to-day activities… Security must collaborate with business partners in order to effectively manage risks and provide the appropriate levels of security controls," he says.

For many organizations, it's more cost effective to outsource the nuts and bolts of specific security implementations, such as an identity and access management project, instead of hiring the expertise in house, says Kushner.

"It's almost expected that security programs are dealing with more strategic, business, policy and legal types of problems," he says.

> "It's almost expected that security programs are dealing with more strategic, business, policy and legal types of problems."
>
> –LEE KUSHNER, president, LJ Kushner and Associates

When he started at CCHC 15 months ago, Murphy was focused on building a robust information security program and performed assessments and operational security. But he expects his role will change this year after a reorganization and a new CTO at the helm (CCHC was recently bought by Steward Health Care System, an affiliate of equity firm Cerberus Capital Management.) The organization has a lot of compliance requirements, including HIPAA, PCI and the Massachusetts data protection law, he notes.

"I will be working more on strategic, governance, and risk management issues rather than day-to-day operations," Murphy says.

---

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

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

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

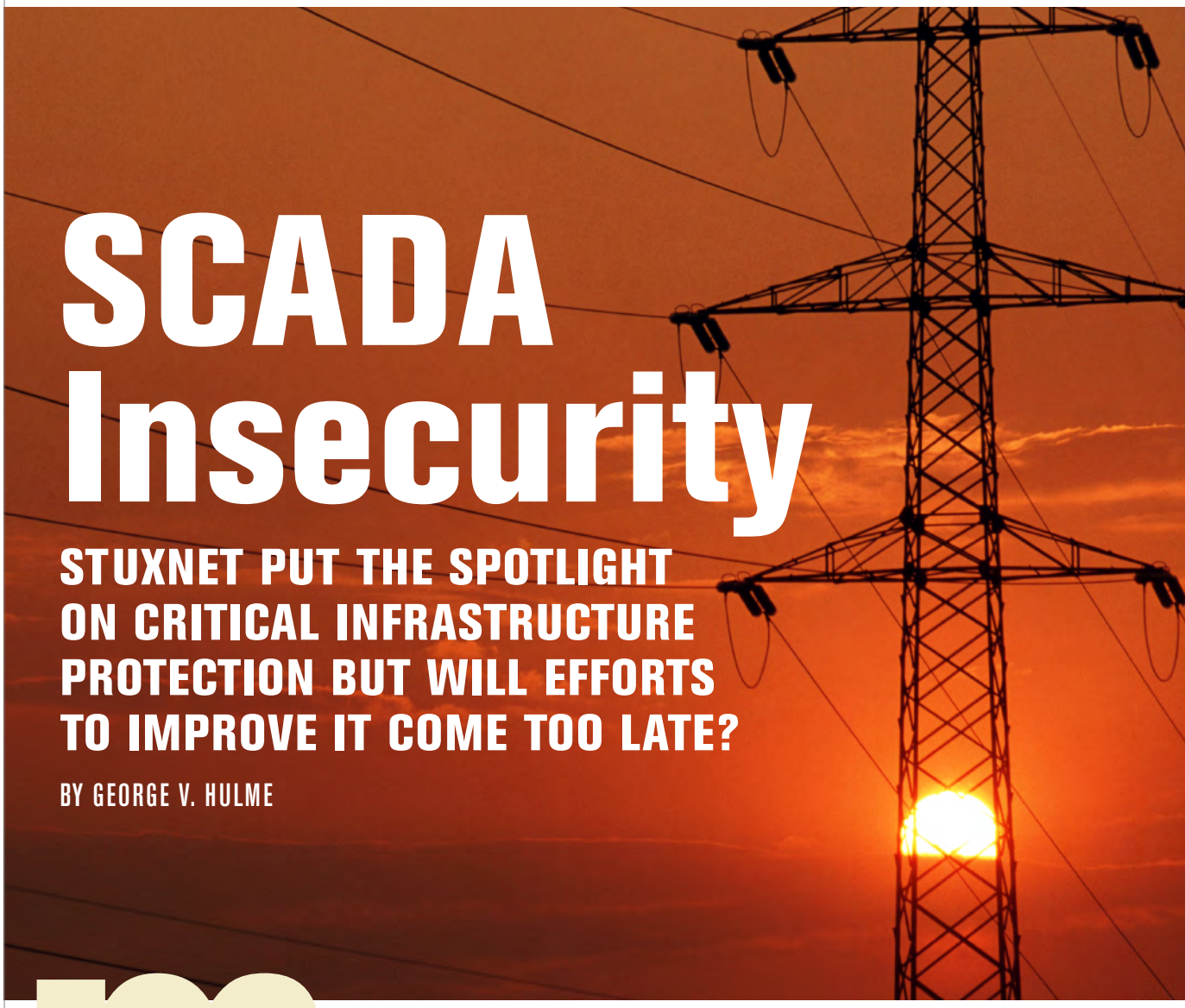
The Academy Pro allows information security professionals to learn about today's most important technologies on demand and at their own pace.

Check out The Academy Pro at
www.theacademypro.com

# the academy pro

Sponsored by:


# www.theacademypro.com



# SCADA Insecurity

## STUXNET PUT THE SPOTLIGHT ON CRITICAL INFRASTRUCTURE PROTECTION BUT WILL EFFORTS TO IMPROVE IT COME TOO LATE?

BY GEORGE V. HULME



**MARK WEATHERFORD** will likely not forget the week of July 12, 2010. He'd just started his job as vice president and chief security officer at the North American Electric Reliability Corporation (NERC) that week. And as chance would have it, security researchers had recently announced the discovery of Stuxnet, one of the most advanced worms on record and widely believed to be targeting Iranian nuclear facilities. With NERC's mission being to ensure the reliability of the North American bulk power system, it was a leap right into the fire for Weatherford.

The Windows-based worm, which contained a programmable logic controller (PLC) root kit, is the first known worm that can reprogram industrial systems, and was crafted to breach Supervisory Control And Data Acquisition (SCADA) systems. SCADA systems are often used to control and monitor industrial processes, including those that help to manage power grids.

Immediately, Weatherford put into place a "Malware Tiger Team" that could be leveraged to help NERC ensure that the information about Stuxnet that was shared among facilities was accurate and useful. The team was comprised of malware experts and representatives from a number of federal agencies. Once the initial commotion over Stuxnet subsided, the team's role faded, but not its ability to reconvene quickly should another threat against the power generation and distribution system materialize.

While the hope is that such a need never arises, the probabilities point to someday in the future when the Tiger Team is called back to work. The extremely sophisticated Stuxnet worm highlighted the vulnerability of the critical infrastructure the world relies on, and security experts worry it could be a harbinger of future attacks. That's especially true as nation-states increasingly invest in their offensive cyberattack capabilities. Just as concerning as the threat, experts say, is that efforts to secure the SCADA systems used to manage many of the critical systems for controlling electricity, water delivery and other essential services have been lax. The federal government and industry groups are taking steps to secure the grid and the SCADA systems that support it, but many worry time is running out before a significant attack hits.

The extremely sophisticated Stuxnet worm highlighted the vulnerability of the critical infrastructure the world relies on, and security experts worry it could be a harbinger of future attacks.

## RISING THREATS

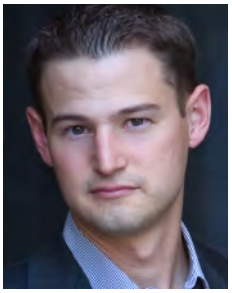
There's no question that concern over critical infrastructure security is growing. Consider the findings in a report released last year by the Center for Strategic and International Studies (CSIS), and funded by security firm McAfee, *In the Crossfire: Critical Infrastructure in the Age of Cyberwar*. Based on a survey of 600 IT security managers from critical infrastructure organizations, the report found that 37 percent believed the vulnerability of the sector they worked increased over the year prior, and two-fifths expect a significant security incident in their sector in the next year. Only one-fifth of respondents to the survey believe their sector to be safe from serious cyberattack in the next five years.

While there was no devastating attack that hit the IT systems that support the North American critical infrastructure, 2010 will nonetheless go down as a decisive year for malware and digital attacks. Cybercriminals (who themselves edged-out the hacker-hobbyist years ago) took a backseat to the state-sponsored attacker. These attackers are well trained, well-funded, and professional. They pose perhaps the greatest threat we've yet to see face the critical infrastructure. In fact, the CSIS survey found 60 percent of those surveyed believe foreign governments have been involved in past infrastructure infiltrations.

Researchers at Moscow, Russia-based Kaspersky Lab, where two of the four zero-day vulnerabilities the Stuxnet worm exploited were identified, reported that Stuxnet's mission was to infiltrate

a specific industrial control system that both monitors and controls industrial, infrastructure, and many on-site processes. It certainly wasn't considered an amateur job. "The inside knowledge of SCADA technology, the sophistication of the multi-layered attack, the use of multiple zero-day vulnerabilities and legitimate certificates bring us to an understanding that Stuxnet was created by a team of extremely skilled professionals who possessed vast resources and financial support," the company said in a bulletin.

"I view Stuxnet as a weapons delivery system, like the B-2 bomber," says Michael Assante, president and CEO at the National Board of Information Security Examiners, and former vice president and chief security officer at NERC and critical infrastructure protection strategist at Idaho National Lab. "The code was designed to be very modular, so that its attack payload could be changed to be able to attack different systems. It's clear to me that the resources available to the authors of the worm were substantial. They designed it with high confidence that the warhead would do exactly what it was designed to do," Assante says. "That takes skill and resources."



"I view Stuxnet as a weapons delivery system, like the B-2 bomber."

–MICHAEL ASSANTE, president and CEO, National Board of Information Security Examiners, and former vice president and chief security officer at NERC and critical infrastructure protection strategist at Idaho National Lab

That combination of well-heeled attackers and sophisticated malware means the stakes are much higher today than a few years ago when it comes to securing the critical infrastructure. This rise in the capabilities of cyber adversaries should be of concern to everyone. Civilization is dependent on the critical systems that control electricity, finances, communications, water delivery, food distribution, and manufacturing. And the management of many those systems themselves are largely dependent on SCADA systems. Years ago, however, when these SCADA systems were first developed, they weren't designed to be resilient to today's security threats or heavy reliance on common and commercially available software applications, operating systems or for communications over public networks such as the Internet.

## IGNORING THE RISKS

As SCADA systems have become increasingly networked, many believe that the industry and the federal government have not taken strong enough steps to ensure these systems are secure. "The industries that ignored cyber security, regardless of what the government said, are still doing just that," says Alan Paller, director of research at the SANS Institute. "It's a fundamental market failure. The industry said it would take care of things, and it didn't do the job it said it would do."

Others agree. "As long as there have not been any attacks [on their critical systems], it's hard for [insiders] to argue to make something more secure," says Richard Stiennon, chief research analyst at IT Harvest and author of *Surviving Cyberwar*. "There were no attacks last year, and there probably won't be attacks next year. So we're not spending on security because you say we should," is the

typical response security professionals hear from their management, Stiennon says.

"Following Stuxnet, one would think that there would had of been a surge of activity to protect the grid, but there wasn't," Paller says.

That apathy extends to the developers of industrial control systems, others say. "There is this climate where everyone understands the potential for mischief, but no one is talking openly about it. And the people who are finding vulnerabilities in SCADA systems and report them to the vendors find themselves in an adversarial situation," says Shawn Moyer, principal consultant at FishNet Security who co-presented a session on "Wardriving the Smart Grid" at BlackHat 2010. "What is going on in this industry today seems a lot like what was going on in the IT industry in the late 1990s when most software companies simply ignored security."

"Following Stuxnet, one would think that there would had of been a surge of activity to protect the grid, but there wasn't."

–ALAN PALLER, director of research at the SANS Institute

"When it comes to SCADA vendors, we are really early in the maturity curve," agrees Assante. For instance, he says, while security administrators at critical infrastructure organizations would like to know how to best harden those systems, the vendors don't always provide the necessary documentation that explains how to do so.

"The vendors understand that security matters, and they're starting to work security into their development processes. Generally, however, their security engineers probably aren't part of the developments teams," he says. "Security is not built into their processes. Over the next couple years, critical infrastructure vendors are going to have to more tightly integrate security into their design and product support initiatives," he says.

## REGULATIONS IN THE WORKS

The federal government and industry groups aren't standing still when it comes to securing the grid and SCADA dependent systems. And they're helping guide the way to more secure and sustainable power systems. Last June, the Department of Homeland Security (DHS) released its Catalog of Control Systems Security Recommendations for Standards Developers that aims to help facilitate the creation of security standards for SCADA, process control, distributed control, and other critical infrastructure systems. The standards help to detail everything from how such industries can screen personnel to establishing physical security and setting secure configuration management guidelines. NERC, for its part, maintains security standards and guidance to roughly 2,000 public and private firms involved in electricity production and distribution in North America.

NERC's Critical Infrastructure Protection (CIP) regulations were designed to help ensure the reliability of bulk power generation and delivery. NERC CIP regulations com-

prise eight mandatory requirements that establish the minimum acceptable level of risk, and include security log collection and analysis, access control, reporting, intrusion detection/prevention system, among others. "The standards have only been auditable for a couple of years, and we are light years improved from where we were a few years ago," says Weatherford. "Are we where we need to be? No. But neither was PCI DSS when it first came out. Today, PCI DSS is a fairly good standard."

Weatherford has a number of areas where he'd like to see improvement. For instance, he would like the CIP standards to move more rapidly and possibly be augmented with more agile ways for covered organizations to manage their risk. "It takes years for these standards to be agreed upon. That's way too long for cybersecurity," he says. Additionally, Weatherford says that a more dynamic risk management framework that can be used in conjunction with the CIP standards would help facilities more intelligently manage risk. "Just as all systems are not equally critical, the risk postures of different plants are not the same and can't be managed the same way," he says. "We've just begun work on developing a more agile way for organizations to



## Powering Up Security

### Utility company implements network encryptors to protect SCADA data and meet NERC requirements.

**WITH A HUGE POWER PLANT** built back in the 1940s that covers a lot of square footage, the North American Energy Alliance faced a compliance challenge. North American Electric Reliability (NERC) standards require that wiring between physical security perimeters be enclosed in conduit or the data must be encrypted. For the NAEA, that would have meant a lot of conduit so it opted to encrypt, says Dominick Birolin, network engineer at NAEA.

The company, which is based in Iselin, N.J., and owns a portfolio of 1,755 megawatts of electricity producing power stations in the Northeast, looked at a variety of encryption options, including point-to-point IPSec tunnels. But it determined that IPSec tunnels would result in latency problems, Birolin says.

"With CipherOptics, the latency was in microseconds as opposed to milliseconds. That was a big advantage, especially for SCADA systems."

–DOMINICK BIROLIN, network engineer, NAEA

NAEA ultimately chose network encryptors from CipherOptics (now Certes Networks) for securing its SCADA information. CipherEngine Enforcement Points from CipherOptics are FIPS 140-2 Level 2 validated encryption appliances.

"With CipherOptics, the latency was in microseconds as opposed to milliseconds. That was a big advantage, especially for SCADA systems," Birolin says.

The technology helps NAEA meet its compliance obligations, but data encryption is an overall good practice, he says. ›

–MARCIA SAVAGE

leverage the CIP standards."

Assante also agrees that critical infrastructure regulations should be risk based and more agile to help better prepare critical infrastructures and the security teams that protect them. "Legislation should include the need for more sharply defined federal authority to address specific and imminent cyber security threats to critical infrastructures in the form of emergency measures," Assante said in a hearing before the Senate committee on homeland security and government affairs in November.

## IMPROVING SECURITY OPERATIONS

When it comes to critical infrastructure protection, information sharing and collaboration has been called upon for years. Last year was the first year the industry has seen real information sharing begin to coalesce. In November, the Department of Homeland Security (DHS) launched a cyber security information sharing center designed to more efficiently share information about cyber threats to the critical infrastructure. Dubbed the Multi-State Information Sharing and Analysis Center (MS-ISAC) Cyber Security Operations Center, it's a 24-hour live watchdog that will, hopefully, provide state and local government officials the same details as those in the federal government.

> "Government and industry aren't standing still, but the question is are they doing enough, quickly enough."
>
> –RICHARD STIENNON, IT Harvest

According to DHS, The National Cybersecurity and Communications Integration Center (NCCIC) will head information sharing to the MS-ISAC Operations Center. States are expected to use the MS-ISAC Operations Center to cooperate to enhance IT security defense and response. The move is just one in a recent flurry of moves by the DHS to help bolster information sharing and incident response.

DHS also announced that the Information Technology Information Sharing and Analysis Center (IT-ISAC) will embed a full-time analyst and liaison to DHS at the NCCIC. The IT-ISAC consists of information technology representatives from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk mitigation strategies.

Also, this past fall, to test the nation's ability to withstand an advanced cyberattack, DHS and a number of international security and intelligence agencies engaged in a cyberwar game involving 1,500 security events designed to see how well federal agencies and more than 60 private sector companies in critical infrastructure responded to a cyberattack. Cyber Storm III was used to test the newly developed National Cyber Incident Response Plan (NCIRP), which is the government's current cybersecurity incident response playbook. A report detailing the results of the exercise is expected soon.

"Government and industry aren't standing still, but the question is are they doing enough, quickly enough," says IT Harvest's Stiennon.

## HELP WANTED

In the future, it may not be budget, technological, or regulatory hurdles that prove the most challenging when securing the critical infrastructure; it could be finding enough skilled security professionals. "It's not that there's a problem finding security superstars, there's a lack of people with basic security skills and knowledge," says Vincent Liu, managing partner at the application security firm Stach and Liu.

In its report, *A Human Capital Crisis in Cybersecurity*, the CSIS found that there are roughly 1,000 security professionals in the U.S. who have the specialized cybersecurity skills needed to protect the critical infrastructure. The report estimates the nation could need up to 30,000 similarly skilled people to get the job done. "There's no doubt that we need to invest more in the security workforce. We need better training, and regular reassessments of their skill level," Assante says.

> "It's not that there's a problem finding security superstars, there's a lack of people with basic security skills and knowledge."
>
> –VINCENT LIU, managing partner, Stach and Liu

NERC's Weatherford agrees: "There are not many qualified, technical, cybersecurity experts that have experience in the power industry." He says it's part of a troubling macro trend affecting the IT industry. "We've been talking about the retirement bubble for a couple years now. We studied the issue when I was CISO at the state of California, and we found so many technical staff eligible for retirement within next few years that it became obvious that if we didn't train and recruit enough people, we were really going to have a problem," he says.

Having the IT staff needed to keep operations running smooth is one thing, having enough professionals trained in the still obscure IT security profession is another—and experts warn we are running out of time. "These aren't always highly-skilled attackers or sophisticated malware that manage to get through. I've seen traditional worms like Conficker on hardened controllers," says Assante. "My greatest fear is that we are running out of time to learn our lessons. Stuxnet, although difficult to hijack or modify by others, may very well serve as a blueprint for similar but new attacks on control system technology," he adds.

---

*George V. Hulme is a business and technology journalist who often writes about security topics from his home in Minneapolis, Minnesota. Send comments on this article to feedback@infosecuritymag.com.*

# 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.

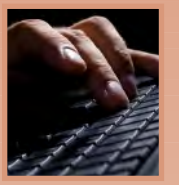
**If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.**

- 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

# COMING IN MARCH





## Virtualization Security

Visibility is the key to keeping virtual server environments secure. Virtual machines tend to grow unchecked, and this can lead to an unmanageable virtual environment. This feature will discuss key steps for virtualization security management, including cataloging virtual and physical assets, and practicing physical and logical segmentation.

## Risk Management Frameworks

The many security and risk management frameworks available to enterprises is vast and confusing. This article will look at popular frameworks such as OCTAVE, NIST and COSO/COBIT, and how enterprises can implement them to streamline risk management and compliance.

## Client-side Application Security

As widespread as Windows installations are, client-side applications such as Adobe Reader, Flash, Apple's QuickTime and others built on Java and AJAX code are more ubiquitous. This feature will look how enterprises can address these threats, manage security of client-side applications, and integrate fixes into existing vulnerability management programs.

**Don't miss our monthly columns and commentary.**

TechTarget
Where Serious Technology Buyers Decide

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.


*See ad page 20*

- Entrusting Endpoints
- Guarding the Gateway


*See ad page 7*

- CORE IMPACT Pro V11 Download
- Continuous Enterprise Risk Measurement White Paper


*See ad page 10*

- How 3 Cyber Threats Transform The Role of Incident Response: Targeted Attacks, System Exploits, Data Theft, and You
- Download Whitepaper: Countering Advanced Persistant Threats with Cyberforensics
- Respond Quickly to Security Incidents; Expose Advanced Malware Threats; Enforce Data Usage Policies


*See ad page 13, 15*

- **IT Professional Membership Benefits**
- **Get Certified in Risk and Information Systems Control**

SOPHOS

*See ad page 4*

- **Eight Threats Your Anti-Virus Won't Stop**
- **How Unauthorized Applications Impact Security and How You Can Take Back Control**