

# INFORMATION **SECURITY**<sup>®</sup>



JULY/AUGUST 2010

## Demystifying **APT**

Get the facts about this  
targeted threat activity

**PLUS**

**The Security SaaS Option**

**Building a Career Skill Matrix**





# TREND MICRO ENTERPRISE SECURITY

Maximum protection. Minimum complexity.

## UNLEASH COST SAVINGS

ESG Research quantifies the cost benefits  
of virtualized desktops.

[Get analyst report](#)

[Watch video](#)

[Contact Us: 877-252-2065](#)



You rely on enterprise security to safeguard your most valuable assets—your corporate data and reputation. And as the centerpiece of compliance policies, it also shields you from increasing regulatory and civil penalties. But the right security can also enable key business initiatives such as virtualization and cloud computing. Better yet, it can dramatically lower operating costs.

[facebook.com/fearlessweb](https://facebook.com/fearlessweb) • [twitter.com/trendmicro](https://twitter.com/trendmicro)

Trend Micro Enterprise Security will help you drive your business forward. It maximizes protection. It minimizes complexity. It supports your evolving business needs. **It's security that fits.**

## FEATURES

**20 What APT is (And What it Isn't)**

**CYBERSECURITY** Think you know all you need to know about the advanced persistent threat? We'll define APT and dispel a few myths. **BY RICHARD BEJTICH**

**26 Offloading the Security Burden**

**OUTSOURCING** Security software-as-a-service can help organizations reduce security headaches but also can present challenges. **BY SCOTT CRAWFORD**

**36 Do You Have the Intangibles?**

**SECURITY CAREERS** Your skill matrix—that connection between your tangible skills and personal qualities—is what separates you from your peers. **BY LEE KUSHNER AND MIKE MURRAY**

**10 PERSPECTIVES****Making the Grade**

Measure process maturity to illustrate how security supports the organization.

**BY CHRIS McCLEAN**



## ALSO

**5 EDITOR'S DESK****The Never-Ending Saga of Insecure Software**

Software security—or the lack thereof—has been a long-standing issue. More progress is sorely needed.

**BY MARCIA SAVAGE**

**13 SCAN****Security Response Teams Grapple With Cloud Computing**

No clear answers but experts urge organizations to proceed with caution. **BY ROBERT WESTERVELT**

**15 SNAPSHOT****Midyear Breach Report****17 INFOSEC LEADERS CAREER ADVICE****Planning Perils to Avoid**

Experts Lee Kushner and Mike Murray explain how building a career plan just might lead security professionals headfirst into some dubious challenges.

**BY LEE KUSHNER AND MIKE MURRAY**

**46 Advertising Index**



# WHO WILL YOU TRUST TO SECURE THE PRIVATE CLOUD?

Visit [www.rsa.com/virtualization](http://www.rsa.com/virtualization).



The Security Division of EMC

**EMC<sup>2</sup>**  
where information lives™

EMC<sup>2</sup>, EMC, and where information lives are registered trademarks or trademarks of EMC Corporation in the United States and other countries.  
RSA is a registered trademark of RSA Security, Inc. © Copyright 2010 EMC Corporation. All rights reserved. 1990



# The Never-Ending Saga of Insecure Software

*Software security—or the lack thereof—has been a long-standing issue. More progress is sorely needed.*

BY MARCIA SAVAGE

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

**AH, SUMMER.** Time to kick back a little and enjoy the long days and warm weather. Uh, well not so much if you're an information security professional. There's never any respite from the seemingly endless stream of new software vulnerabilities and patches to apply.

Already in June, we had a bumper crop of [patches from Microsoft](#), which coincided with a flaw in [Adobe's Flash Player](#), Reader, and Acrobat products. Plus, attackers quickly exploited a zero-day [vulnerability in the Windows XP Help and Support Center](#) component, which was disclosed by a Google engineer (and unleashed a renewed debate over responsible disclosure, a whole other topic we won't rehash here). Of course, the bad news wasn't limited to commercial software. AT&T made headlines for all the wrong reasons with its poor Web application security that was uncovered by a small security research firm and exposed the email of thousands of iPad 3G users.

The industry has preached the need for software security and secure coding for several years now. After all, if software is designed securely from the start, it means a lot less problems down the road. In the commercial software realm, Microsoft certainly has made strides in improving the security of its software, and Adobe has seen the light with its implementation of a [secure software development process](#). However, Microsoft's monthly security bulletins combined with quarterly security patches from Oracle and Adobe continue to require labor and expense in the enterprise.

At an (ISC)<sup>2</sup> conference on software security last month in Fremont, Calif., attendees were asked how insecure software has impacted their organization. Twenty-six percent ranked staff hours spent on installing patches or remediation as the top impact. Interestingly, the majority (56 percent) ranked reputation damage due to breaches as having the biggest impact.

During a panel discussion, participants raised—and quickly dumped—the notion of

**Twenty-six percent ranked staff hours spent on installing patches or remediation as the top impact. Interestingly, the majority (56 percent) ranked reputation damage due to breaches as having the biggest impact.**



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

a something like a Good Housekeeping Seal for software. The general consensus: A lab can certify a toaster oven, but issuing a safety seal for software that's used in so many different ways and in multiple environments is impossible.

A big part of the problem, says Max Rayner, former CTO at travel deal publisher Travelzoo and a panelist at the (ISC)<sup>2</sup> conference, is the lack of security training for programmers. "For decades, we've taught people how to code, but not necessarily how to code securely," he says.

The industry continues to tackle the problem of insecure software with several initiatives, including the [Building Security in Maturity Model \(BSIMM\)](#), which offers a model drawn on security practices of 30 firms, and the Software Assurance Forum for Excellence in Code ([SAFECode](#)), which aims to advance software assurance methods. SAFECode, which has a membership that includes Microsoft, Adobe and Symantec, recently released [a paper that provides guidance for reducing risks in the software supply chain](#). (ISC)<sup>2</sup>, provider of the CISSP program, now offers a certification in software security.

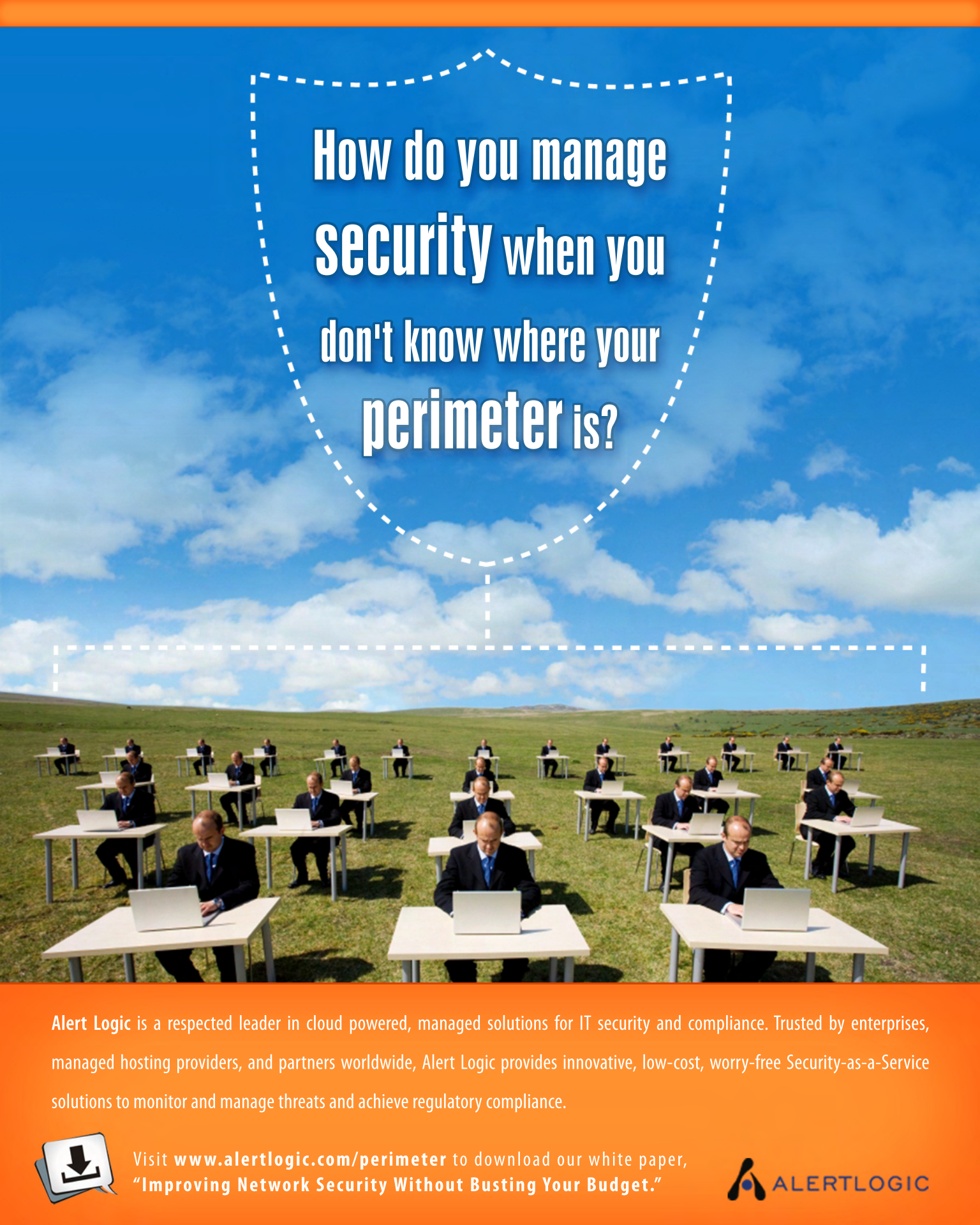
Hewlett-Packard says it's developed a methodology for reducing the risk of security flaws in software, which it's used in-house for more than six years and recently made commercially available. The idea is to perform a threat analysis of an application's architecture, before a single line of code is written, and save money on corrections required by penetration tests and other security reviews.

The need for secure software becomes only more critical with cloud computing, says Chris Whitener, chief security strategist for HP Secure Advantage. "If we can't trust some of the foundations that the cloud is built on, the whole thing starts to fall apart," he says.

Of course, flaw-free software isn't possible. But with cloud computing drawing intense interest in the enterprise and financially-motivated attackers always on the hunt for holes to exploit, we need a laser-like focus on software security. We can't afford to take our eyes off the ball even during the dog days of summer. •

---

*Marcia Savage is editor of Information Security. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*



# How do you manage security when you don't know where your perimeter is?

Alert Logic is a respected leader in cloud powered, managed solutions for IT security and compliance. Trusted by enterprises, managed hosting providers, and partners worldwide, Alert Logic provides innovative, low-cost, worry-free Security-as-a-Service solutions to monitor and manage threats and achieve regulatory compliance.



Visit [www.alertlogic.com/perimeter](http://www.alertlogic.com/perimeter) to download our white paper,  
"Improving Network Security Without Busting Your Budget."



# VIEWPOINT

Readers respond to our commentary and articles. We welcome your comments at [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).

## Puzzling Formula

In the May 2010 article, “[The Real Risk Equation](#),” Ron Woerner describes the real risk equation mathematically as Risk = Impact X Probability / Cost. Maybe I am misunderstanding his point, but this would indicate risk is inversely proportional to cost, i.e., the greater the cost the lower the risk (if he is dividing by a larger number the risk rating will be lower/smaller). On the contrary, for most programs or program managers, risk is directly proportional to cost: If a particular risk is going to cost the company a lot of money if it occurs, it will probably be given a higher risk rating than a risk that will not cost the company a lot of money if it occurs—other things being equal.

—JEFF OWEN, director, Air Force medical information systems test bed,  
Sentel Corp.



Ron Woerner replies:

*Thanks for the feedback. Your thoughts are correct. Risk should be weighed against the mitigation cost. While risk can be inversely proportional to cost, it's not always the case.*

*Although I've seen some organizations think they can spend their way to lower risk, spending on risk reduction follows the law of diminishing returns. That's the problem I've seen with trying to quantify something like risk. There's no way to do it without finding an exception that breaks the rule. The equation I propose (based on historical references) is a*

*tool to be considered for understanding your risks and the costs of mitigation. I admit it's not perfect, but it has worked well for me.*

### TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

## COMING IN SEPTEMBER

### 2010 READERS' CHOICE AWARDS

*Information Security and SearchSecurity.com surveyed our readers to determine which products are best at protecting data and networks. Readers only voted on products they had deployed in their company so this listing may help you plan and simplify your information security product buying decisions.*

### PCI REFRESH

The Payment Card Industry Data Security Standard is the most controversial and prescriptive information security regulation—and it's due for an update in early October. This article will take a deep dive into PCI and what is lacking in the standard, such as virtualization and cloud security guidance, direction on end-to-end encryption and how companies can use tokeniza-

tion as either a compensating control or as a means to comply with the standard's encryption and data protection directives.

### MITIGATING WEB 2.0 THREATS

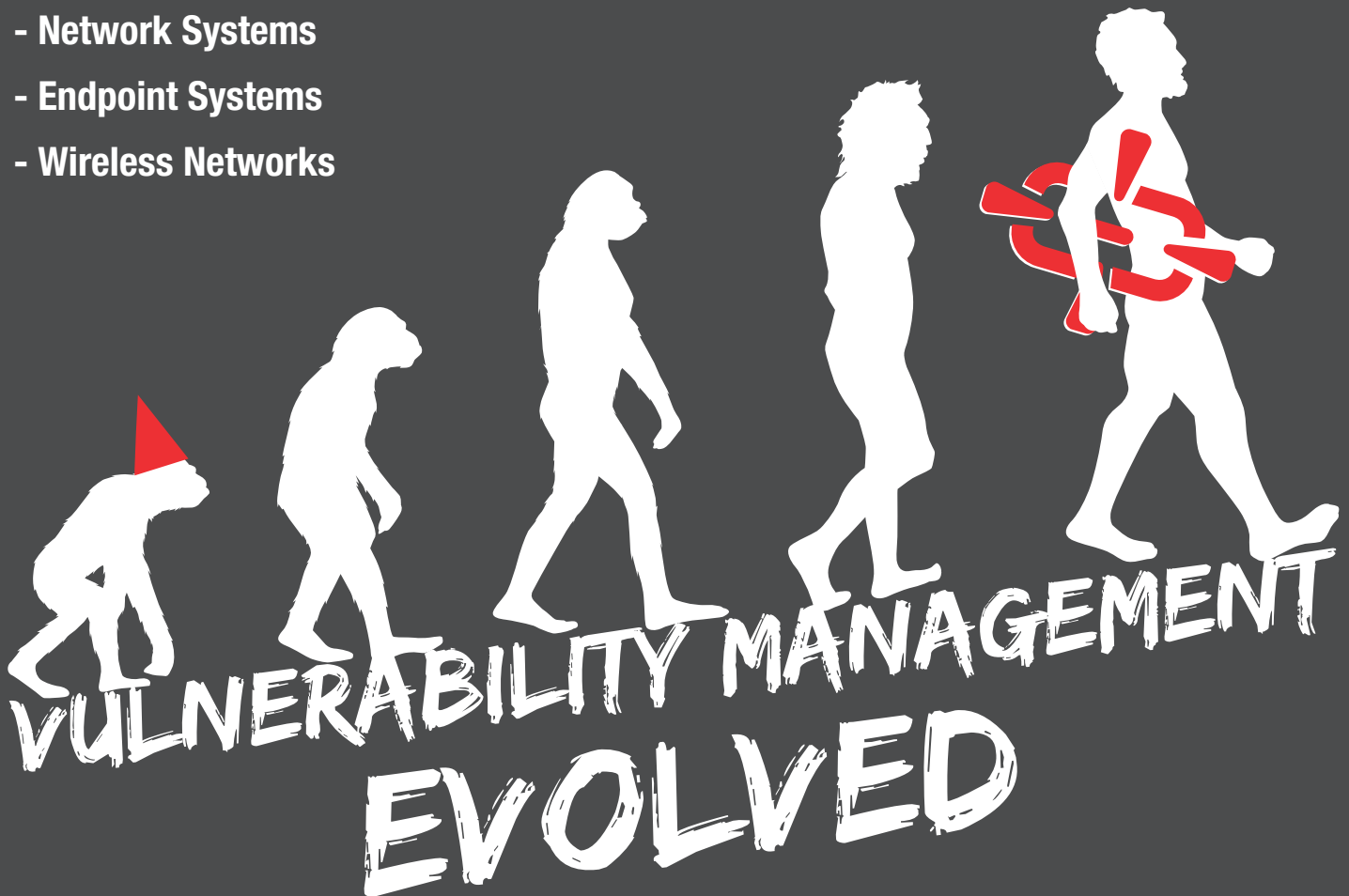
The collaborative nature of Web 2.0 has great appeal for business from a marketing and productivity point of view. Companies are taking advantage of social networking sites such as Facebook

and Twitter to connect with colleagues and customers, or free online services such as webmail, Google Docs, and other collaborative platforms to share information. CISOs must find the balance between security and the business need for these tools and enable their use in such a way that reduces risk. This article will look at necessary policies and technologies that will help you keep Web 2.0 threats at bay.



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

**Learn more:**

Visit [www.coresecurity.com](http://www.coresecurity.com)  
or call us at (617) 399-6980

# Making the Grade

BY CHRIS MCGLEAN

*Measure process maturity to illustrate how security supports the organization.*

## TABLE OF CONTENTS

## EDITOR'S DESK

## PERSPECTIVES

## SCAN

## SNAPSHOT

## CAREER ADVICE

## APT

## SECURITY SAAS

## CAREERS

SPONSOR  
RESOURCES

**HOW WELL DO** your colleagues in other departments understand what security does? If executives had to grade how well you're doing as a function supporting the business, would they know what questions to ask?

Last year, Forrester Research found that roughly half of all CISO or equivalent roles reported directly to C-level executives, yet we still see a significant number of these individuals struggling to articulate how security supports the broad organization. Operational metrics and compliance reports reflect performance to some extent, although the scope of these measures is limited, and they rarely address the interests of the business.

To meet these challenges, security professionals should use a framework to evaluate the process maturity of all functions for which the security organization is responsible. Measuring process maturity takes the conversation out of the technology world and presents an assessment of how well you approach your different responsibilities.

For example, using **COBIT** maturity levels, you can assess whether your incident response process is 0—non-existent; 1—ad hoc; 2—repeatable; 3—defined; 4—measured; and 5—optimized. The details behind the score will be different for each function, but they will all have similar characteristics. That is, to reach a level 3 you will look for clearly defined policies and procedures, and to reach a level 4 you will need to show that you consistently use metrics to guide decision making. It takes time to develop the unique characteristics for each function (i.e. deciding what metrics to use for log monitoring versus remote access controls) but it allows you to compare otherwise dissimilar areas of security using the same scale.

To make this work, your score explanations need to be:

- **Prescriptive:** The characteristics required to achieve the next-higher level of maturity should be clear and objective. An assessment should yield similar results

Measuring process maturity takes the conversation out of the technology world and presents an assessment of how well you approach your different responsibilities.

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

#### SCAN

#### SNAPSHOT

### CAREER ADVICE

#### APT

### SECURITY SAAS

#### CAREERS

#### SPONSOR RESOURCES

regardless of who conducts it.

- **Process-oriented:** Even for security functions that primarily rely on technology, you should be evaluating the process you take to choose, deploy, and monitor that technology. Focusing too much on the products or tools used is likely to make the assessment irrelevant in a few years' time.

- **Uncomplicated:** Security organizations must constantly respond to auditors, regulators, business partners, and other stakeholders to support different types of assessments. A maturity assessment should not require an extremely large amount of background data or evidence. The evaluation should be made based on high-level discussions and observations.

When building the framework for this model, it's helpful to consider functions described in standards and regulations that are core to your organization's control framework, although it should not get down to the level of control assessments. In addition, it's important to consider the governance and oversight functions of the security organization, which often don't show up in industry standards. Those functions include strategic planning, budgeting, capacity planning, skills management, and performance management. Also, evaluate how well the security organization works with other relevant functions, such as compliance, audit, legal, and lines of business.

The objective of a maturity assessment like this is to provide a platform for discussing and demonstrating what the security department does, help plan your security roadmap, and show that security investments are leading toward measurable progress. This approach will not help you measure whether or not you are secure, and it does not take into account key aspects of building a roadmap, such as risk exposure and available budget. However, security professionals looking for a straightforward way to baseline their approach to security (and benchmark their program against historical assessments and/or peers) should find this a valuable and worthwhile exercise. •

The objective of a maturity assessment like this is to provide a platform for discussing and demonstrating what the security department does, help plan your security roadmap, and show that security investments are leading toward measurable progress.

---

*Chris McClean is an analyst at Forrester Research. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com). He will be speaking at [Forrester's Security Forum](#) September 16-17 in Boston.*



# Check Point Abra

Put your office in your pocket.



- Instantly turns any PC into your own corporate desktop
- Provides virtual workspace that keeps mobile data secure
- Delivers ideal solutions for mobile workers, contractors and disaster recovery



Secure  
virtualization



Secured connection  
solutions



Portable, plug-and-play  
solutions

Get the **FREE** technical white paper to learn more about Abra at:  
[www.checkpoint.com/abra\\_whitepaper](http://www.checkpoint.com/abra_whitepaper)



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

Analysis | CLOUD SECURITY

## Security Response Teams Grapple with Cloud Computing

*No clear answers but experts urge organizations to proceed with caution.*

BY ROBERT WESTERVELT



**UDO SCHWEIGERT**, a security analyst who runs the computer emergency readiness team at Siemens AG, says his company is well-versed in dealing with cloud providers but that work remains.

The German-based technology giant has more than 450,000 employees in 180 countries. So it wasn't surprising that a division in Japan contracted with one software-as-a-service provider while the company's sales offices in Russia chose another to suit their needs, Schweigert says.

Siemens moved quickly to develop policies and educate business users about the importance of data security when choosing a cloud provider. The company's work isn't done, however. More policies are needed to address cloud-based infrastructure and platform providers, he says.

"We were lacking risk management with many of these projects," Schweigert says. "That's why we've made it part of our corporate risk management strategy."

Cloud computing was a hot topic at June's Forum of Incident Response and Security Teams (FIRST) Conference 2010, where Schweigert spoke on a panel. FIRST attendees—many of them members of security response teams—are wrestling with cloud computing concepts and trying to understand how cloud computing might change the way first responders address security threats. They didn't get any clear-cut answers from cloud and security experts at the conference, but one message was clear: tread carefully when moving into the cloud.

Fundamental security technologies work like they always have, but certainly enterprises shouldn't rely on the service provider to maintain data security, experts say. Consequently, security professionals need to approach cloud computing matters delicately, says Chris Hoff, director of cloud and virtualization solutions at Cisco

### TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

SNAPSHOT

CAREER ADVICE

APT

SECURITY SAAS

CAREERS

SPONSOR  
RESOURCES

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

Systems and a well-known speaker and blogger on cloud computing issues. Business units see the cost savings associated with moving to the cloud, but can easily overlook or even ignore the risk assessment, Hoff says.

"Our ability to influence those decisions and have a rational conversation can be very difficult sometimes," Hoff says. "We can't run around and say the sky is falling because we're not going to be taken seriously."

Setting an appropriate risk posture by knowing the kind of data that can reside at cloud providers and the intellectual property and other data types that need to be fully safeguarded from cybercriminals is a good first step, says Dave Aitel, a noted security expert and chief technology officer of Miami-based assessment and penetration vendor Immunity. Aitel adds that the assumptions people make with cloud computing—cost benefits and increased efficiencies—are often different than the results they get.

"Attackers are always looking for opportunities to exploit that gap between the assumptions you're making and the reality," Aitel says.

Jose Nazario, a botnet expert and senior security researcher at Arbor Networks, calls cloud-based services the inevitable next stage for enterprises. However, he says security experts are still learning about the threats posed by the cloud.

"We can't fully understand and quantify the risks and we've been doing this stuff for the past 20 years," Nazario says. •

**"Our ability to influence those decisions and have a rational conversation can be very difficult sometimes. We can't run around and say the sky is falling because we're not going to be taken seriously."**

—CHRIS HOFF, director of cloud and virtualization solutions, Cisco Systems

*Robert Westervelt is the news editor of [SearchSecurity.com](http://SearchSecurity.com). Send comments on this article to [feedback@inforsecuritmag.com](mailto:feedback@inforsecuritmag.com).*



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

## Midyear Breach Report

By Information Security staff

So far this year there's been no report of a massive data breach like the Heartland Payments Systems 2008 hack in which about 130 million credit and debit cards were stolen, but there's been no shortage of breaches in 2010. The Privacy Rights Clearinghouse has tallied more than 100 breach reports so far this year, ranging from lost laptops and stolen hard drives to hack attacks. Here are some of the bigger breaches from the nonprofit's list, with the estimated number of records exposed:

**1.2 million** Lincoln National Corp. in January notified state authorities of a vulnerability uncovered within its portfolio management system: Users were sharing passwords and thereby exposing the personal information of about 1.2 million customers.

**1 million** BlueCross BlueShield of Tennessee reported that the theft of 57 hard drives from a training facility last October exposed the private information of one million customers in multiple states. The hard drives contained customers' personal data and protected health information, which was encoded but not encrypted.

**208,000** AvMed Health Plans announced in February that the theft of two company laptops from its corporate offices may have compromised the personal information of some current and former subscribers.

**3.3 million** Educational Credit Management Corporation, a guarantor of federal student loans, reported in March that portable media with personally identifiable information on 3.3 million borrowers was stolen from its headquarters.

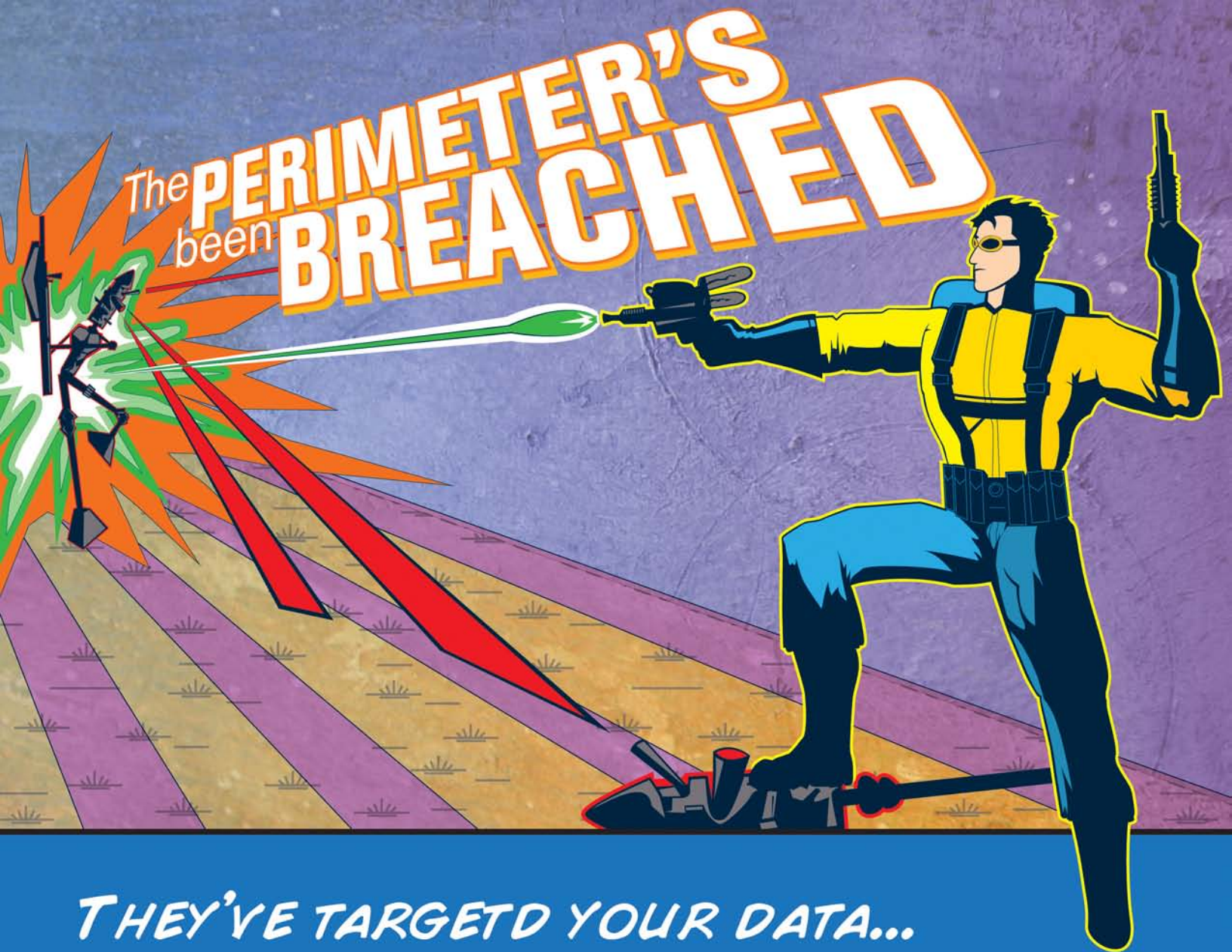
**409,262** Affinity Health Plan, a New York managed care service, in April notified more than 400,000 current and former employees and others that their personal data might have been exposed through the loss of a digital copier hard drive that hadn't been erased.

OVER-  
HEARD



“It would be a mistake to say one OS is more secure than another.”

—JOSH CORMAN, research director at The 451 Group, commenting on a report that Google is phasing out the Windows operating system for internal use due to security concerns.



## *THEY'VE TARGETED YOUR DATA... NOW WHAT?*

- CONCERNED ABOUT ADVANCED THREATS EVADING PERIMETER DEFENSES?*
- NEED TO PREVENT DATA THEFT?*
- DO YOU HAVE DIFFICULT RESPONDING TO MALWARE SUCH AS THE ZEUS TROJAN?*

*IF YOU ANSWERED YES TO ANY OF THESE QUESTIONS, VISIT [WWW.GUIDANCESOFTWARE.COM](http://WWW.GUIDANCESOFTWARE.COM) TO LEARN HOW ENCASE CYBERSECURITY EXPOSES AND ELIMINATES UNKNOWN RISKS AND THREATS TO DATA SECURITY.*







# Planning Perils to Avoid

BY LEE KUSHNER AND MIKE MURRAY

*Building a career plan just might lead security professionals headfirst into some dubious challenges.*

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

**AS YOU DEVELOP** your [information security career plan](#), you are going to be challenged to honestly assess your skills and figure out ways to develop your weak points. As you do so, you are going to be forced to make decisions that may accelerate or hinder your pursuit. It's important to make sure that you avoid some potential planning hazards that could divert you from achieving your desired career goal. Let's look at three.

## FOCUSING ON THE WRONG ELEMENTS OF A NEW ROLE

In order to achieve your career goal you are most likely going to have to pursue opportunities outside your current work environment to gain valuable experience or build new skills. When you refer back to your career plan, you should already have an idea of [what skills are important to develop](#). Keep in mind, the primary goal of switching positions is the skills, not the other things that many information security professionals expect to come with a new position: more money and a flashier title. Many fail to recognize the opportunity for skill development a new position will provide, or decide to accept an inferior position that diverts them from their initial purpose for switching roles.

It's true that additional money will make your life easier, and having a flashier title will impress your mother-in-law, but at the end of the day these are irrelevant to long-term goals. For example, in many cases when a company offers pay that is outside of the market for your skills, there is likely an urgency to complete a specific task. They are hiring you exclusively for your current skills, and may not have an interest in enabling you to build skills that are important to you.

If you are entertaining such an opportunity, it is critical to ask the new employer questions about your career path and personal development during the interview process to help you determine if your expectations align with your new employers'.

Titles are generally more important internally because they are not standardized across industries. Titles could be significant if you are changing positions within the same industry, such as financial services. Many financial services firms have standard titles, and have similar skill requirements associated with them. For example if you were a vice president of information security at one firm, you would not want to accept a role in another financial services firm as an associate. Conversely, you should not have any issue in accepting a position in a non-financial services firm that has a title of manager, director, or senior director.

Always keep in mind when you are looking for your next role that your future manager is more likely to care more about what you accomplished than your title.

## EXPECTING IMMEDIATE IMPACT FROM CAREER INVESTMENTS

In addition to developing information security skills within our work environments, we have to select meaningful career investments to augment our professional development, such as advanced degrees, certifications and technical and non-technical career development. Any meaningful career investment traditionally costs a good amount of money and requires a great deal of time.



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

It's natural to want a quick return on our investments and our expectation is that our employer will place a value on a credential and recognize the achievement with either a promotion or an increase in responsibility. Unfortunately, many organizations do not recognize the value in a way that aligns with the information security professional's expectations. In these cases, job satisfaction will most likely decrease and it may cause you to begin looking for another position. This is a huge mistake.

It is important to think logically about the situation and gain perspective. When you make the decision to pursue a major career investment, the purpose should be for your long-term benefit, not the immediate impact.

A significant career investment (such as a master's degree) is something you will carry throughout your career, and the benefit that you will receive from this knowledge will show up in your daily performance. It would be logical for your company to evaluate your performance and measure your impact to the information security function after you have achieved this credential. Hopefully, you will be able to demonstrate to your employer specific aspects of your professional development that will inspire them to advance your career and provide you with the type of responsibility that you want in order to get you closer to your career goal.

Keep in mind that it's not wrong to expect a return, however it is critical to manage the expectation of the time it takes to create this impact.

## REMAINING IN YOUR COMFORT ZONE

In assessing current skills and abilities, it is very easy to figure out what we are good at and what comes naturally to us. It is equally difficult to come to grips with our weaknesses. However, when determining your strategies for planning your information security career, it is more important to face our deficiencies so that we can eliminate obstacles.

One key strategy is to attempt to leave your comfort zone and place yourself in situations that will force you to develop new skills. Granted, this is much more challenging than sticking to what you do best; however in order to achieve great things, you have to be prepared to accept great challenges.

For example, if I knew that my skills are in technical areas and I struggled with presentations and public communications, I would find opportunities within the context of my position to develop presentation skills. One step you could take would be to start a lunch-and-learn program to present information security topics to your technical team on topics in an informal setting with your peers. After you felt comfortable with this, as part of a security awareness program you could volunteer to speak in front of internal diverse groups in a more formal matter. If you continued to improve and felt comfortable, you could apply to present on a similar topic at a local chapter meeting at ISSA, OWASP or ISACA.

Depending on your commitment and aggressiveness, this process may last between six and 18 months. However, at the end you will have addressed this deficiency, and hopefully transformed it into a personal strength.

## STAY TRUE TO YOURSELF

Your written career plan should be utilized as a valuable guide as you make decisions regarding the direction of your career. Keep in mind that when you are called upon to make these decisions, you are not going to be correct all the time. In making these decisions, you should not expect perfection, and you should not second guess yourself if these decisions do not turn out the way that you plan. As you are faced with these choices, utilize your internal compass as a guide and focus on your desired outcome. Whatever decisions you make, right or wrong, maximize the impact that they will have on your career. If you do so, you should avoid any pitfall or hazard that could come your way. •

*Lee Kushner is the president of LJ Kushner and Associates, an information security recruitment firm, and co-founder of [InfoSecLeaders.com](http://InfoSecLeaders.com), an information security career content website.*

*Mike Murray has spent his entire career in information security and currently leads the delivery arm of [MAD Security](http://MAD Security). He is co-founder of [InfoSecLeaders.com](http://InfoSecLeaders.com), where he writes and talks about the skills and strategies for building a long-term career in information security.*

*Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com)*

# GOOD FORTUNE

## Can Be Yours



### BREAK INTO IT.

Register for an ISACA certification exam.

**Exam Date:** 11 December 2010

**Registration Deadline:** 6 October 2010



[www.isaca.org/infosecmag](http://www.isaca.org/infosecmag)

*Introducing ISACA's newest certification:*



*Grandfathering is now open.*



## TABLE OF CONTENTS

## EDITOR'S DESK

## PERSPECTIVES

## SCAN

## SNAPSHOT

## CAREER ADVICE

## APT

## SECURITY SAAS

## CAREERS

SPONSOR  
RESOURCES

# What APT is (AND WHAT IT ISN'T)

Think you know all you need to know about the advanced persistent threat? We'll define APT and dispel a few myths. BY RICHARD BEJTICH

**THE TERM** advanced persistent threat, or APT, joined the common vocabulary of the information security profession in mid-January, when [Google announced its intellectual property had been the victim of a targeted attack originating from China](#). Google wasn't alone; more than 30 other technology firms, defense contractors and large enterprises had been penetrated by hackers using an array of social engineering, targeted malware and monitoring technologies to quietly access reams of sensitive corporate data.

[Google's public admission](#) put a high-profile face on targeted attacks and the lengths attackers would go to gain access to proprietary corporate and military information. It also kicked off a spate of vendor marketing that promised counter-APT products and services that have only served to cloud the issue for security managers and operations people.

In this article, we'll define APT, dispel some myths and explain what you can do about this adversary.



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

## WHAT IS THE ADVANCED PERSISTENT THREAT?

The United States Air Force coined the phrase advanced persistent threat in 2006 because teams working within the service needed a way to communicate with counterparts in the unclassified public world. Department of Defense and intelligence community members typically assign classified names to specific threat actors, and use the term intrusion set to describe activities by those threat actors. If the USAF wanted to talk about a certain intrusion set with uncleared personnel, they could not use the classified threat actor name. Therefore, the USAF developed the term APT as an unclassified moniker.

It is crucial to this discussion to recognize that APT is a proper noun. APT refers to specific threat actors; APT does not refer to vaguely unknown and shadowy Internet forces. The term is most frequently applied to distinct groups operating from the Asia-Pacific region. Those knowledgeable about APT activities can conduct an honest debate as to whether the term should be used to refer ONLY to certain Asia-Pacific actors, or if it can be expanded as a general classifier. In other words, if adversaries in Eastern Europe operate using the same tools, tactics, and procedures as traditional APT, should these actors also bear the APT label?

The answer to this question depends on the person asking it. An information security practitioner in a private organization will typically not care if the threat actors attacking an enterprise originate in the Asia-Pacific or Eastern European regions. The reason is that the practitioner will likely take the same defensive actions regardless of the location or nationality of the adversary.

However, someone with the legal and/or national security authority to apply diplomatic, intelligence, military or economic (DIME) pressure would certainly want to identify the origin of an attack. For the purposes of this article, aimed at information security practitioners, it is not necessary to answer the “who” question definitively. However, those who do have elements of DIME power should take attribution statements by Google and other victims seriously.

Most of those actively countering APT activity describe the adversary in the following manner:

**A****dvanced** means the adversary can operate in the full spectrum of computer intrusion. They can use the most pedestrian publicly available exploit against a well-known vulnerability, or they can elevate their game to research new vulnerabilities and develop custom exploits, depending on the target's posture.

**P****ersistent** means the adversary is formally tasked to accomplish a mission. They are not opportunistic intruders. Like an intelligence unit, they receive directives and work to satisfy their masters. Persistent does not necessarily mean they need to constantly execute malicious code on victim computers. Rather, they maintain the level of interaction needed to execute their objectives.

**T****hreat** means the adversary is not a piece of mindless code. The opposition is a threat because it is organized and funded and motivated. Some people speak of multiple “groups” consisting of dedicated “crews” with various missions.

In brief, APT is an adversary who conducts offensive digital operations (called computer network operations or perhaps computer network exploitation) to support various

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

state-related objectives. APT is characterized by devotion to maintaining some degree of control of a target's computer infrastructure, acting persistently to preserve or regain control and access. Unclassified briefings by counter-intelligence and military analysts use the term "aggressive" to emphasize the degree to which APT pursues these objectives against a variety of government, military, and private targets.

## WHY IS ADVANCED PERSISTENT THREAT MISUNDERSTOOD?

Beginning in January and peaking in February and March, many elements of the digital security community focused their attention on APT. Unfortunately, some of those speaking about the problem quickly found themselves echoing statements and questionable research offered by parties who were not familiar with APT. Several factors contributed to an overall sense of confusion, with some of the more trustworthy voices competing with parties who would have been better advised to stay in the background.

Several factors caused this phenomenon:

- Besides Google's public statement, and subsequent secondhand reporting about allegedly affected peer companies, very little original data was available. Without details to discuss, the security community turned to almost anyone willing to talk about the incident. In too many cases, the speakers turned out to be vendors who saw APT as a marketing angle to rejuvenate slumping security spending. [RSA Conference 2010](#) featured many companies selling counter-APT products, hoping to capitalize on the new hot topic of 2010.

- McAfee reported it was analyzing malware that it claimed to be associated with the Google incident, independently assigning the name "[Aurora](#)" to the affair thanks to a path found in the malware. In late March, McAfee blamed "the fog of war" for mistakenly confusing a Vietnamese-targeted botnet with Google incident malware. Unfortunately, by associating this false lead with the Google incident, McAfee prompted a variety of security researchers to direct their efforts on code that likely had nothing to do with the Google incident.

- Many analysts too narrowly focused on the elements of the incident that they could best understand, regardless of the real nature of the event. For example, companies specializing in botnet research assumed botnets were involved, and talked about the Google incident in those terms. Others who focus on identifying vulnerabilities and developing exploits, concentrated on a flaw in Internet Explorer (patched by [MS10-002](#)) presumably leveraged by intruders to gain access to Google resources. Unfortunately, botnets have nothing to do with APT, and vulnerabilities, exploits, and malware are only elements of APT incidents—not the core feature of them.

## IS APT NEW?

When the Google attack entered the public arena, many people wondered if APT was something new. The answer to this question depends on one's perspective, plus understanding some history. As mentioned earlier, the term APT is approximately 4 years old. It entered the common lexicon in early 2010 with the [publicity garnered by Google's bold proclamation](#). However, consulting companies, particularly Mandiant have been conducting public webcasts and presentations discussing APT by name since 2008.

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

Prior to the 2006 invention of the APT term, news stories of Chinese intruders attacking military and government organizations bore the label “Titan Rain.” For example, a 2005 *Time* magazine article by Nathan Thornburgh titled “[The Invasion of the Chinese Cyber-spies](#)” described battles fought by Shawn Carpenter, then defending Sandia National Laboratories. That story mentioned Carpenter’s experience with similar intruders dating back to late 2003. Even in 1998, when I served as a captain in the Air Force Computer Emergency Response Team, we encountered adversaries that many would now label APT.

Some would even argue that nothing about APT is new. To the extent that espionage is as old as warfare itself, some claim APT activity is just spying another form—and not even a new medium, given the [history of computer espionage dating from Cliff Stoll’s work](#) in the 1980s.

I argue that APT is new if those asking the question move beyond two-dimensional thinking. Considering APT activity in terms of offender, defender, means, motive, and opportunity, APT is clearly new. Points for the “old” camp include the identity of the offender (nation-states) and the motive (espionage). Points for the “new” camp make a stronger argument:

**Defender:** I break APT targets into four phases: 1) late 1990s - military victims; 2) 2000-2004 - non-military government victims; 3) 2005-2009 - defense industrial base; 4) 2009-present - intellectual property-rich targets and software companies. (Unfortunately there are clear examples of earlier victims, but these dates roughly cover most known cases.) The assault conducted during phases 3 and 4 is unprecedented, meaning entirely new classes of defenders must protect themselves from attackers previously a concern for the military.

**Means:** Too many critics focus on malware, ignoring (or being unaware) of the

## OBJECTIVES

# APT Impact

**Analysts currently assess APT activities as supporting four main goals.**

- **Political** objectives such as maintaining internal stability.
- **Economic** objectives that rely on stealing intellectual property from victims. Such IP can be cloned and sold, studied and underbid in competitive dealings, or fused with local research to produce new products and services more cheaply than the victims.
- **Technical** objectives that further their ability to accomplish their mission. These include gaining access to source code for further exploit development, or learning how defenses work in order to better evade or disrupt them. Most worryingly is the thought that intruders could make changes to improve their position and weaken the victim.
- **Military** objectives that include identifying weaknesses that allow inferior military forces to defeat superior military forces.

—RICHARD BEJTICH



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

impressive management and administration applied to repeatedly attempting to access, or preserving access to target organizations. APT incidents are not hit-and-run, smash-and-grab affairs.

**Opportunity:** The explosion of Internet connectivity in the last decade and the extreme distribution of sensitive data to end points provides cheap, low-risk, remote access options for intruders, unlike anything available to human spies.

On balance, I argue APT is new, at least when considered from the perspective of non-military targets, and remembering that phase 3 APT activity began in 2003 and became a significant problem in 2005.

## WHAT SHOULD DEFENDERS DO TO COUNTER APT?

The majority of this article has focused on describing APT and its history, because battling this adversary does not require a technical solution. The most effective counter-APT weapon is a trained and knowledgeable information security analyst. Many security vendors have adopted APT in their marketing literature. Some offer to find APT on a potential victim's network. Others have even registered APT-themed domain names.

Tools are always helpful, but the best advice I can provide is to educate business leaders about the threat so that they support organizational security programs conducted by competent and informed staff.

A second question one is likely to ask follows: How do I know if I am an APT target? Contact your local Federal Bureau of Investigation office. One of the biggest game-changers in counter-APT awareness developed during the last several years is taking the form of visits by FBI and military or counter-intelligence specialists to potential victims. It's difficult to deny a security breach when representatives from a national security agency reveal excerpts from proprietary data or intellectual property and ask "does this data belong to you?" If you have not already engaged your organization's leaders in a counter-APT conversation, requesting a threat briefing from the local FBI office is an excellent way to promote managerial attention.

On a technical level, building visibility in to one's organization will provide the situational awareness to have a chance to discover and hopefully frustrate APT activities. Without information from the network, hosts, logs, and other sources, even the most skilled analyst is helpless. Thankfully, obtaining such information is not a new challenge, and most security shops should be pursuing such programs already. The goal of counter-APT operations should be to make it as difficult as possible for the adversary to steal intellectual property; "increasing the cost per megabyte," to quote the NSA's Tony Sager, is the goal. •

---

*Richard Bejtlich is director of incident response for General Electric, and serves as principal technologist for GE's Global Infrastructure Services division. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

Everything  
you want  
in an AV  
solution.



Internet Security

**NEW**  
Remote Administrator 4  
features:

- Intelligent group manager
- Firewall rules merge wizard
- Improved policy manager
- Simplified remote administration
- Cross-platform management



# Protection, speed and flexibility.

## ESET NOD32 Antivirus 4 + Remote Administrator

ESET NOD32® Antivirus 4 Business Edition is more than simply powerful Internet security. It's a comprehensive network-wide solution. And, when paired with ESET Remote Administrator, it takes the headaches out of IT management. Light on client resource consumption and easy to manage, ESET NOD32 + Remote Administrator (RA) saves money that might otherwise be wasted upgrading computers running sluggish AV. And because it's so easy to manage, your IT department gets back what it values most — hours in the day.

### Proactive protection

We scan all incoming and outbound network traffic, email attachments and removable media — but that's not enough. We compare unknown code to millions of database signatures — but that's not enough either. We even have frequent ultra-small updates that incorporate signatures from threats encountered across ESET's 100-million user network — but you still need more.

Superior protection doesn't depend on updates at all. In comparative testing using outdated signatures, ESET consistently outperforms other AV solutions. "ESET offers the highest proactive threat detection," independent AV-Comparatives May 2009.

The difference? Advanced heuristics. Proactive protection that doesn't just passively look for existing features of malware — it actively predicts strains that haven't been written yet and sandboxes them in a controlled disk environment where they can do no harm. And when a block of code seems suspicious — it is immediately repaired or quarantined. Smoothly. Efficiently. Seamlessly.

### Unmatched speed

On the user end, ESET runs just two processes — the scanning kernel and the user interface — and together sip just about 44 MB of RAM. Typically, that's less than an instance of Word, Communicator, Excel, Explorer or Firefox. And with minimal interruptions or pop-ups and no scanning slowdown at file open or startup, your users won't even notice its running. But they will notice they no longer need to phone IT for lagging startups or malware infections.

On the server side, mirrored downloads and small signature updates mean your network traffic will never lag because of your antivirus solution. Mail scanning happens in the blink of an eye and compatibility with a variety of protocols and systems, from Cisco NAC to Microsoft Exchange means that you'll never have to deal with multiple antivirus solutions for your mixed network.

### Flexible management

For mixed networks, ESET NOD32 delivers comprehensive protection — working natively in Windows XP, Vista and 7; Linux / BSD / Solaris; Mail Server; Exchange; and soon Linux Desktop and Apple Mac OS X.

Vast multiplatform protection doesn't have to be a management nightmare. ESET Remote Administrator allows for simple push-installation of preconfigured NOD32 packages to client computers and now with RA4 — allows Active Directory management of dynamic networks.

The combination of ESET NOD32 + Remote Administrator means simple, powerful management of a network of 10 computers or 10,000 with protection for every system and every platform. Each computer is an attack surface — and you need the best available protection on all of them.

Solutions to fit all  
your business needs

- File server security
- Mail server security
- Gateway server security
- Mobile phone security

[www.eset.com/business/products](http://www.eset.com/business/products)

Request your free trial at [www.eset.com/business-trial](http://www.eset.com/business-trial)



# OFFLOADING THE SECURITY BURDEN

Security software-as-a-service can help organizations reduce security headaches but also can present challenges.

BY SCOTT CRAWFORD

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

**SECURITY THREATS** and vulnerabilities have exploded in recent years. Attackers are more sophisticated and focused on information that has tangible value. The result for many organizations worldwide is an outpouring of time and money on security that never seems to slow down.

Sound familiar? If so, you're not alone. Organizations everywhere have gotten caught up in what many see as a security arms race. An ongoing investment in security technologies means constant maintenance and upgrades across multiple tools to stay current with the threat landscape—regardless whether or not this supports the strategic priorities of the business. More than a few wonder if there isn't a better way to manage this investment more intelligently.

For many, the answer is the increasingly popular alternative of security software-as-a-service (SaaS). Software hosted by a third-party service provider has become well established for business applications, but security SaaS is different. While any [SaaS](#) offering may offer functionality to enhance security such as access control or secure connectivity, security SaaS exists primarily to support security. Examples include hosted message security and filtration (the expansion of "anti-spam" to include antivirus, anti-malware, and other capabilities such as anti-phishing), vulnerability assessment, Web browsing security, identity management delivered as SaaS for other SaaS services—and the list keeps growing.

There's something else that stands out about security SaaS: Some organizations have long been reluctant to outsource one of the most sensitive functions in IT, but today many are embracing security SaaS. What are the benefits that are leading enterprises as well as small- to medium-sized businesses (SMBs) to turn to hosted security technology?



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

And what are the factors organizations should weigh before making security SaaS a part of their strategy? We'll examine these issues and provide strategic guidance for organizations considering the SaaS option for security.

## The SaaS Advantage

If the primary value of security SaaS could be reduced to a single word, it would be "relief." With a SaaS approach, a third-party service provider takes on responsibility for the maintenance of the technology investment. In exchange for a regular, recurring fee, the customer gains readily adopted access to technology that is kept up-to-date with little or no customer action required. For the enterprise, it means expanding the reach of security management and outsourcing many of its complexities that free up resources for more strategic priorities. For small- to medium-sized businesses (SMBs), it puts a higher level of capability within their grasp.

## Ease of Adoption

In Enterprise Management Associates' 2010 survey of security SaaS users, large enterprises and SMBs alike saw improved access to capability with easy adoption as the greatest benefit. In many cases, there is little or nothing for the customer to deploy; they simply enable the service. For message filtration, service activation amounts to adding another relay to the mail system. The same is largely true for adding inline Web proxies for safe browsing services. For vulnerability assessment, the capability can be used on-demand. The relatively straightforward adoption of offerings like message filtration has led to more than a few comparisons with utilities that are simply "switched on"—and a revival of some of the old arguments in favor of what was once called "utility computing." Those considering security SaaS should, however, note that not all hosted security services are created equal in this respect. Readily externalized services such as message filtration may be more easily adopted than the outsourcing of deeply integrated technology on which the business has a critical dependency, such as access management for internal resources. User accounts still have to be provisioned, and may require synchronization with existing accounts.

## Shifting the Maintenance Burden

Once the service is activated, ongoing maintenance becomes the responsibility of the service provider. This shifts the burden of capital investment and maintenance costs to a third party under contract. Capital investments in security products that in the past may have been unpredictable and sometimes challenging to justify in light of their initial costs are shifted over to the operations side of the balance sheet. Barriers to acquiring new security technologies are sharply reduced or eliminated at the cost of a regular and more predictable subscription.

The transparency of technology maintenance enabled by the SaaS model has high appeal. Says one customer of a vulnerability assessment SaaS offering from Qualys: "We began with this provider at version three of their service. Today, we're at version seven, and we didn't have to do a thing. We also got PCI capability added to this service without having to lift a finger—it just showed up. You can't imagine how happy we are."

# Advice from the Frontlines

## Service providers and their customers say a phased approach is best when adopting security SaaS.

AS TODAY'S PROVIDERS and customers hammer out the answers to the challenges presented by security SaaS, they are defining how to make the most of the hosted opportunity. What do these early participants in this still-emerging domain recommend to those considering security SaaS?

SaaS providers and customers alike recommend adopting security SaaS in stages wherever it makes sense to do so; they often suggest beginning with services that are most readily adopted. In the enterprise, initial deployments should be contained if possible, limiting impact on critical business applications or risks of exposing the most sensitive information where able. This allows the customer to become familiar with how the provider approaches such issues as SLAs, performance expectations, data confidentiality, and divisions of responsibilities between the provider and the customer.

Such an approach is not always possible when the need outweighs adoption risks. This may be particularly true among SMBs, who may need to outsource a wider scope of functionality. If starting with a limited approach is not feasible, reference customers can help the new client develop a feel for how the service may impact its users, as well as the vital resources or processes it touches. They can also help new customers learn how to make the most of the service, and share experience in working with the provider.

Having a broader potential use case in mind is another way to approach a phased adoption of security SaaS. Terry Wyatt, corporate security officer at a leading health care technology company, says the organization had the eventual integration of vulnerability remediation in view when it first considered Hewlett-Packard's vulnerability assessment SaaS for Web applications. In phase one of the adoption, the service was used only by the security team to become familiar with its use and its impact on the organization. In phase two, the outcomes of assessments were first made available to development teams to familiarize them with the new tool for identifying security issues requiring remediation.

By phase three, developers had become sufficiently familiar with the service to initiate assessments themselves, freeing the security team for other important priorities. According to Wyatt, this not only made the most strategic use of limited resources, it also achieved an important objective by breaking down silos of technology and culture to foster a more effective approach to security management. »

—SCOTT CRAWFORD

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

#### SNAPSHOT

#### CAREER ADVICE

#### APT

#### SECURITY SAAS

#### CAREERS

#### SPONSOR RESOURCES

## Enterprise Benefits

Scalability and rapid adaptability are other advantages of security SaaS for large or highly distributed organizations. "Adding capability without having to add a dozen or more security engineers just to use it is a definite benefit for us," says Ed Bellis, CISO for an online travel company that uses a hosted email security service from Postini (now owned by Google) and hosted vulnerability assessment services from Qualys and WhiteHat Security. When the service provider adapts to new or emerging issues such as newly disclosed vulnerabilities or threats, it is that much less for enterprise security teams to manage.

Another enterprise benefit of the SaaS model is that some hosted tools can be accessed from virtually anywhere, by any aspect of the customer's organization. Hosted message filtration services can centralize email security across a global organization, improving consistency in accounting as well as defense while providing universal access to the service regardless of location. Vulnerability assessment SaaS enables a global business to cover a wider scope of applications worldwide. One major technology vendor uses this approach to identify issues that require further investigation with onsite tools and expertise, allowing it to better allocate precious security resources where most needed. The scalability essential to

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

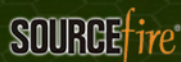
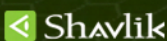
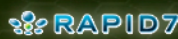
Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a firehose'.

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](http://www.theacademypro.com)

## the academy pro

Sponsored by:



# [www.theacademypro.com](http://www.theacademypro.com)

The Academy Pro © Owned by Black Omega Media Group Incorporated



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

a successful SaaS offering further enhances the value of this approach to the enterprise. In effect, the customer “rents” not just the provider’s technology, but the capabilities of its data centers as well.

The wide accessibility of a hosted service has been particularly valuable to Terry Wyatt, corporate security officer at a leading health care technology company that uses Hewlett-Packard’s vulnerability assessment SaaS for Web applications. “We don’t have to engineer some complex architecture in order to enable access to findings from an internal tool across all our development teams,” Wyatt says. “Each team gets its own portal to the hosted service, where they can find the results they need. Simply outputting results in a PDF report meant for auditors just doesn’t cut it for remediation.” This approach has played a key role in helping this organization foster more efficient and effective processes for vulnerability management.

## SMB Opportunities

Because the provider can distribute its costs across tens, hundreds or thousands of customers, a SaaS model can offer “enterprise-class” security capability to the smallest organization—and it can do so at the predictable cost of a subscription. For SMBs, this does more than relieve prohibitive initial investment costs and ongoing maintenance burdens; it gives them access to technologies that might otherwise be beyond their reach.

The SaaS model has helped smaller organizations embrace technologies such as single-sign-on for third-party services—something typically seen as an enterprise-level technology project. Lincoln Cannon, director of Web systems for Merit Medical Systems, a 1,500-employee medical device company, was able to use identity management SaaS from Symplified to extend internal single-sign-on to other third-party SaaS resources for office productivity applications and training.

“I knew that traditional approaches to single-sign-on were likely to be too expensive and involved to consider. Using a readily deployed SaaS offering enabled us not only to roll out single-sign-on to third party services, it also allows us to mash up authenticated services at the browser,” Cannon says. “Now, when we make changes to documents in our SaaS office suite, they are reflected automatically in our SaaS training service through single-sign-on, relieving us of the need to create documents in one service and upload them to another in separate steps.”

Not surprisingly, security SaaS adoption is growing substantially among SMBs. In EMA’s 2010 survey of security SaaS customers, responses from organizations having fewer than 2,500 employees were compared to those from larger organizations. While a

“I knew that traditional approaches to single-sign-on were likely to be too expensive and involved to consider. Using a readily deployed SaaS offering enabled us not only to roll out single-sign-on to third party services, it also allows us to mash up authenticated services at the browser.”

—LINCOLN CANNON, Web systems director, Merit Medical

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

majority of all respondents (57 percent) indicated their use of SaaS would expand this year, the percentage of SMBs saying their use would grow significantly was five times greater than that of large enterprises (25 percent versus 5 percent).

## The Challenges

With all these positive values, why isn't security SaaS transforming security management wholesale? For starters, the broader security SaaS landscape is still taking shape, with a mix of technologies and players both old and new.

This means that vendors and early adopters alike are still defining the optimal balance between what providers offer and what customers demand. Prospective users will want to consider these factors carefully, since the more they ask of their providers, the greater the likelihood that providers will pass the added costs along to the customer, which may put the cost advantages of SaaS at risk. This is no small concern: In EMA's survey of current and former security SaaS users, unmet expectations of cost reduction was the number one reason for dropping a service: 63 percent of those who either quit or reduced their use of SaaS did so because it didn't reduce costs or in some cases, actually increased costs.

## Growing Pains

The youth of the security SaaS market is itself a factor: Some offerings such as message filtration have been around for years; others are just emerging. Well-proven services may be adopted with higher confidence than those whose impact may not yet be fully known. "We have yet to apply the service to a wider scope of our sites, because we want to make sure it won't tip over critical applications," says one user of vulnerability assessment SaaS who, though pleased with the service so far, is taking a cautious approach to developing a thorough understanding of its impact.

The youth of some SaaS offerings is also evident in the service provider's approach to issues such as sensitive data protection. "Some service provider contracts declare values for loss or exposure that are substantially lower than the actual value of the data," says Randall Gamby, an enterprise security architect for a Fortune 500 insurance and finance company. "They don't understand that if they have an incident, we may not recoup our damages."

**"Some service provider contracts declare values for loss or exposure that are substantially lower than the actual value of the data. They don't understand that if they have an incident, we may not recoup our damages."**

—RANDALL GAMBY, enterprise security architect

If the service fills a gap better than anything else, these factors may matter little to the business with a keenly felt need. Regardless, prospective customers will want to learn as much as they can about how service providers address the risks of new services. If the provider has relatively few customers, how significant is the customer's need in light of the provider's capability and its stability as a business? How flexible is an emerging provider willing to be to win business? If it has an established customer base, what do others say about the service? Does it have any key partnerships with other preferred suppliers? How

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

do these factors influence the provider's long-term prospects?

## Adoption Complications

While some security SaaS offerings like message filtration and vulnerability assessment are readily externalized and have limited impact on internal resources and infrastructure, others are not. Security services that are more deeply integrated with internal resources, or those where the service becomes critical to the customer's business, are more complicated to implement. Providers must offer adequate assurance of availability and performance in these cases. The security of the service itself may be a factor, but in some cases this can be addressed with approaches such as those that blend an on-premises interface with external services to give the customer greater control.

Identity management delivered as SaaS, such as the Symplified service Merit Medical Systems uses to extend single-sign-on, offers one such example. Providers in this space are aware that many organizations will be reluctant to expose sensitive internal access credentials to public networks. To solve this problem, they may place an interface (either software or an appliance) at the boundary between the customer's premises and access to the SaaS offering. This helps to abstract credentials and secure the customer's link with the service, thereby enhancing protection. Some may refer to this as a "hybrid" approach but that term has potential for abuse, particularly among vendors who simply add capabilities such as remote management to on-premises products in order to capitalize on the "security as a service" trend.

And there are other considerations where adoption may be less straightforward than simply flipping a switch. For example, does the provider require customers to maintain separate user accounts just for the service, or can they be synchronized with existing accounts? Would a service interruption be "business critical," or can outages or other disruptions be tolerated? SaaS providers know their customers have these concerns, and some are prepared to answer—where they can. Regardless, those exploring security SaaS will need to understand the various ways in which moving to SaaS can affect their organization.

## Service Level Agreements

This brings up the subject of the service level agreement (SLA). Adopters must remember that in exchange for the advantages of outsourcing technology management, the customer gives up a measure of direct control. Should the service be interrupted, compromised, or otherwise fail to deliver as expected, who has responsibility for what?

Providers recognize that customers need assurance that the service will fulfill expectations, but customers need to be clear on what really matters in an agreement. For example, if the customer has compliance or policy obligations to secure sensitive data or make information available in response to an e-discovery demand, how does this affect the service provider? What standards or regulatory requirements does the customer adhere to and are they compatible with the provider's existing practices? How much visibility does the customer have—or want—into how the service provider meets expectations? What about disaster recovery and business continuity? And what assurances can the provider offer to make good on its commitments?

Other SLA factors may enter into play should the customer choose to leave the service. Can the customer take any relevant configuration data, activity logs, or other meaningful

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

management information to a competitor? When data sensitivity is a factor, does the provider commit to secure erasure after service ends—or for that matter, whenever the data is no longer needed? If so, to what extent (if any) can the customer verify? Does the service offer any alternatives that would relieve or eliminate the need for secure erasure in such cases, such as helping the customer to mask, tokenize or encrypt sensitive information?

Prospective customers should remember that just because a SaaS application is designed to meet the needs of a wide variety of users, that doesn't necessarily mean that the service can't be tailored to meet specific requirements. But they should also remember that this likely comes at a cost. Providers who offer affordable yet realistic assurances against the risks of outsourcing will likely be recognized by customers as being more responsive to their needs, giving the provider an edge in an emerging field where many already see high value.

## Looking Ahead

Where will the security SaaS trend lead?

Will it transform IT security technology

as we know it today? In some cases, it's easy to imagine where vendors may go next. Antivirus vendors already offer products as well as hosted services that provide inline protection for email and messaging systems. They also provide signature updates to their antivirus products as a service. Not surprisingly, some AV vendors have recently moved to extend their services even further, with antivirus and anti-malware coverage for endpoints delivered as SaaS. Data loss prevention (DLP) effectively complements inbound message filtration with outbound control, so its deployment as SaaS may not be far off. Encryption services could complement hosted DLP, broadening the scope of data security offered as a service.

In other cases, it may be difficult to imagine outsourcing more sensitive functionality to a third party, but consider where security services have already made inroads. Deeply integrated technologies such as security information and event management (SIEM) take input from security tools throughout the enterprise, but event management and incident response are already part of the managed security services (MSS) landscape. Can the deployment of the underlying technology as a service in its own right be far behind?

This illustrates how security SaaS is itself part of a larger spectrum of "security as a service." In a certain light, SaaS could be seen as a form of a managed service, since the customer effectively outsources the maintenance of the technology to the service provider. This is something to consider when SaaS may not yet be the right answer for a certain need today. Outsourcing deeply integrated security infrastructure

**Providers who offer affordable yet realistic assurances against the risks of outsourcing will likely be recognized by customers as being more responsive to their needs, giving the provider an edge in an emerging field where many already see high value.**



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

may not yet lend itself to a SaaS model but that may change if or when trends such as cloud computing take hold. Until then, prospective customers should bear in mind that managed security services can help fill the gap between the outsourcing of technology and the outsourcing of the expertise needed to optimize on-premises efforts.

As the value of security SaaS continues to emerge, and answers to customer questions and concerns unfold, its true potential will become clearer. A number of both established and emerging vendors—and more than a few customers—already see it as playing a decisive role in shaping the future of IT security. In the EMA survey, the majority of today's adopters (59 percent) see security SaaS as more strategic than tactical. They see it as expanding capability and shaping their strategy rather than simply filling operational gaps.

The promise security SaaS offers for eliminating some of the most onerous headaches of security management and freeing customers to tackle more strategic priorities is not lost on these early adopters—nor is it lost on vendors staking their future on its potential. •

---

*Scott Crawford, CISSP, CISM, is managing research director of the security and risk management practice at Enterprise Management Associates (EMA), an IT industry analyst and consulting firm. Send comments on this article to [feedback@infosecuritymag.com](mailto: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](http://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

## TABLE OF CONTENTS

## EDITOR'S DESK

## PERSPECTIVES

## SCAN

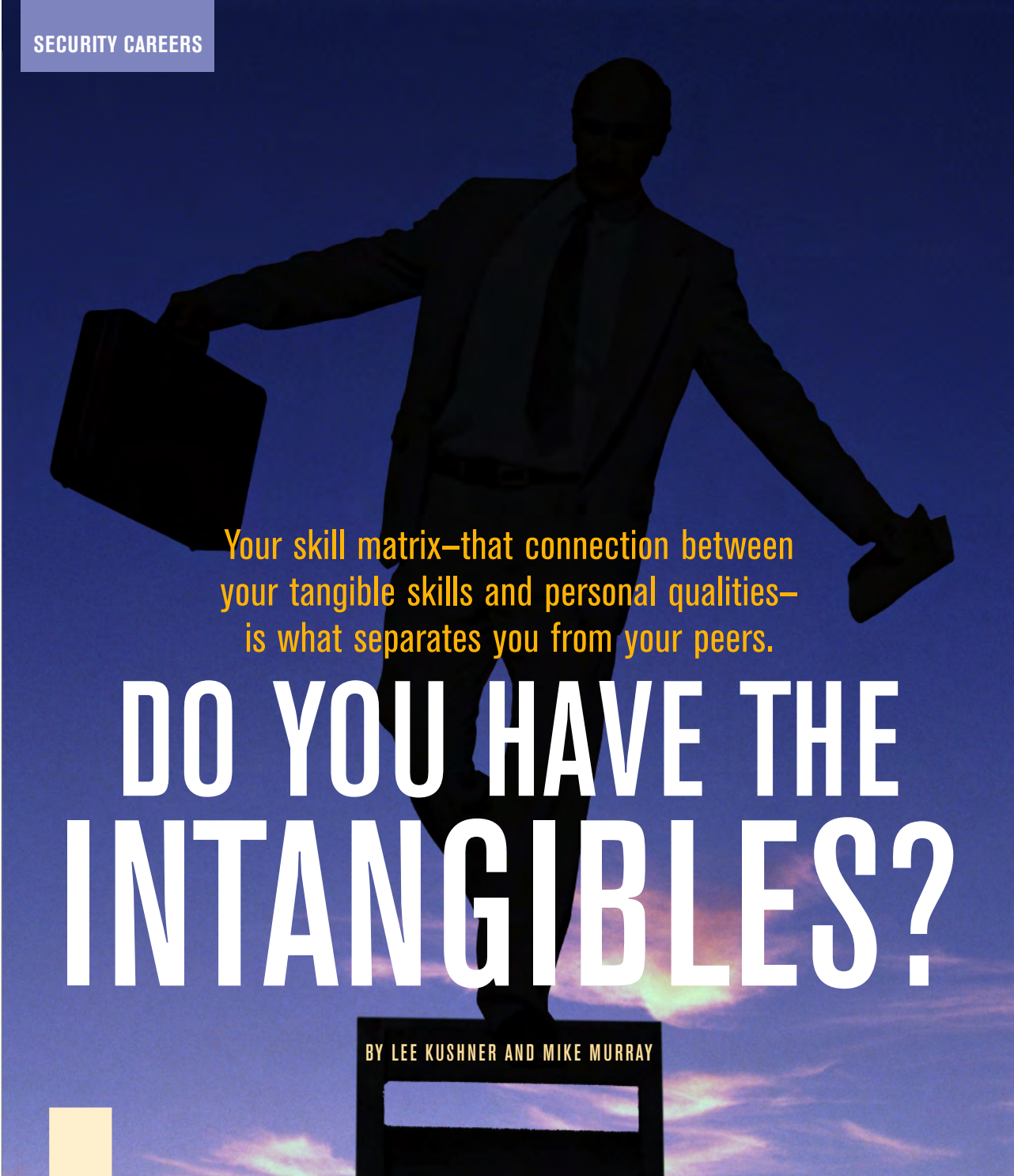
## SNAPSHOT

## CAREER ADVICE

## APT

## SECURITY SAAS

## CAREERS

SPONSOR  
RESOURCES

Your skill matrix—that connection between your tangible skills and personal qualities—is what separates you from your peers.

# DO YOU HAVE THE INTANGIBLES?

BY LEE KUSHNER AND MIKE MURRAY

**TRADITIONALLY, WHEN A** company begins to search for an information security leader such as a CISO, they generally create a job description. Most standard job descriptions contain a detailed list of skills, experiences and certifications needed to be considered for a specific role. The more advanced the position, the more detailed the list. At face value, the resumes of many senior information security professionals are able to match job requirements that are outlined in standard CISO or information security leader positions. However, while it may be easy for many experienced information security professionals to believe they have the credentials to qualify for senior roles, many fall short.

The primary reason is not due to experience or certifications, but due to a blend of tangible and intangible skills that cannot exclusively be found on resumes.

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

As we look into the future and enterprises ingrain security into the corporate culture, competition for these positions will be increasingly difficult. Information security professionals are going to have to spend more time differentiating themselves from their peers. Instead of being concerned with building their resumes, information security professionals are going to have to focus on the development of their personal skill matrix to provide them with a better chance to be chosen for these roles.

## WHAT IS AN SECURITY CAREER SKILL MATRIX?

An information security professional's skill matrix is defined as the connection and correlation between skills, experience, education and personal qualities that are utilized in his or her career. While it is true that many information security professionals have had similar work experiences (that often result in indistinguishable resumes), a skill matrix is personal and unique.

As it relates to one's skill matrix, your professional success as information security professionals is predicated by two factors: First is the ability to connect and correlate these elements to equal a sum greater than the separate parts. The ability to effectively link these experiences and credentials will generally enable information security professionals to separate themselves from others who share similar experiences, but have not figured out how to maximize and leverage their value.

A good example of this would be information security professionals who go back to school to get an advanced degree, and expect to have their career accelerated on the basis of attaining the certification alone. The knowledge received in the advanced degree is one element of the equation, but the real impact lies in the application of this new knowledge. The real value is in the utilization of these new learned skills to make the information security program more efficient and effective. It is these specific results that would create more professional opportunity and warrant a promotion.

The second would be the ability to articulate and communicate the value and application of your information security skill matrix to others who may be in a position to accelerate your career. These can consist of your current employer, future employers, your peers and your social networks. For example, no one could argue that a CISSP is a meaningful information security certification, however its value increases substantially when you can articulate how you utilize the specific knowledge regularly either in the course of your current position or when interviewing for a new one. The certification may have value to some people just because you have it—for them, it signals your interest and commitment to the profession and your desire to obtain a base level of knowledge within the certification. However,

**An information security professional's skill matrix is defined as the connection and correlation between skills, experience, education and personal qualities that are utilized in his or her career.**



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

the true value of the certification to your employers (or potential employers) is a direct reflection of what you are able to do for them. Your ability to communicate that value is one of the fundamental differentiators that you have.

## FOUR SKILL CATEGORIES FOR YOUR MATRIX

From the inception of the industry, it has been commonly stated that effective information security leaders can be successful if they have an understanding of people, process and technology. Without question, this is a solid foundation for information security professionals to build their career, however as the industry has developed over time, we have a responsibility to evolve with it.

Today's information security leaders are faced with many of the same issues as past leaders, however there is no question that there is increased intensity, scrutiny and visibility on their actions and performance.

The internal and external threats facing corporate information security organizations are much more diverse, the standards and regulations are more complex, the media has made the impact of a security incident much more severe, and executive management is less patient and much less tolerant. As we look to the future, these factors will continue to intensify, making it necessary for information security leaders of the future to develop a greater arsenal of skills that will enable them to effectively lead their organizations as they address the information security and information risk management issues facing them.

These skills will fall into four primary categories:

1. A greater knowledge of technology's impact on the organization
2. Better business acumen specifically as it relates to the business operations that they are attempting to secure
3. Leadership in all forms (team leadership, organizational leadership and industry leadership)
4. A consistent commitment to their professional development that will enable them to maximize their talents.

There are many information security professionals who believe that the only way to be effective in the role of information security leader is to be respected by senior executive management (the C-suite) and to be viewed as equal team member. While a statement like this holds a great deal of merit, it could be applied to any other member of the executive team as well. At all levels of an organization, respect among one's peer group is earned and is not an entitlement. As you move closer to the top of the organization, this becomes a greater challenge.

One of the primary reasons information security professionals have fallen short of earning the respect they would like, is because they have been benchmarking their skills against the wrong group of people. Many information security leaders believe that since they are recognized and respected among their security peers, they would automatically be respected by leaders in other corporate functions. But because information security is relatively new and viewed as a cost center and sometimes a business inhibitor, many are reluctant to welcome security leaders as

WE'LL GET  
YOUR IT SYSTEMS  
TO TALK...



ARE YOUR NETWORK DEVICES HOLDING YOUR LOGS HOSTAGE?  
WHAT YOU DON'T KNOW CAN HURT YOU.

OPTICS FOR SECURITY INFORMATION MANAGEMENT IS AN AFFORDABLE AUTOMATED LOG MANAGEMENT SERVICE THAT CENTRALIZES, ANALYZES AND RETAINS LOG DATA AND HELPS YOU USE IT TO SUPPORT BUSINESS FUNCTIONS. SCALABLE TO 100% OF YOUR LOG DATA, SO YOU CAN REST EASY, GLASSHOUSE HAS GOT YOU COVERED.

FOR MORE INFORMATION CONTACT: [SECURITY@GLASSHOUSE.COM](mailto:SECURITY@GLASSHOUSE.COM)

[WWW.GLASSHOUSE.COM](http://WWW.GLASSHOUSE.COM)

 **GLASSHOUSE**

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

peers. Also, many other executives do not believe that the information security leader has had to go through the same professional gauntlet they had to endure to rise to the top of their profession.

If information security professionals hope to be effective at the C-level, they are going to have to demonstrate the same mastery of these skills and display the same level of competence as their peers on the executive team. The best way to convince them that you, the information security leader, deserves the respect and attention will be to develop the technical skills of a CIO, the business acumen of a COO, the leadership skills of a CEO, and underscore it with a demonstrated commitment to professional development that is consistent with the new peer group.

## KEEP THOSE TECHNOLOGY CHOPS

Many information security professionals enter their careers with a strong foundation in technology. Whether this talent is gleaned from their home-grown computer labs or from computer science curricula at universities, this level of core understanding has long been a building block for a successful career. As technology has evolved over the past decade, it has created the need for information security professionals to acquire a broader understanding of networks, applications, wireless technologies, operating systems and software development. Many information security professionals have utilized these experiences to learn more about integrated information security concepts, including identity and access management, securing the software development lifecycle, data protection, security event management and many others. Although these skills enable information security professionals to display their knowledge of the security ecosystem, they are limiting when you compare them to security concerns affecting the business.

Information security leaders of the future are going to be entering their roles at a crossroads, where the workforce will be much more computer savvy and have higher expectations for availability, flexibility and access.

Information security professionals are going to have to be able to exhibit to their employers their understanding of broader technological trends that could have an increasing impact on the company's ability to do business and reach their customers in a secure manner. For example, in today's business environment, many organizations view cloud computing as a viable technology strategy, however the security implications have limited its acceptance and adaptation.

The information security leader of the future is going to be required to have a deeper understanding of these technologies and also be able to help foreshadow their impact on the enterprises that he or she is chartered to secure. It will be important

**Information security leaders of the future are going to be entering their roles at a crossroads, where the workforce will be much more computer savvy and have higher expectations for availability, flexibility and access.**

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

for information security leaders to leverage their knowledge of these broader technologies in order to inspire the necessary confidence in leading their organizations into the future.

## UNDERSTANDING SECURITY'S ROLE IN THE BUSINESS

If you were to define the core responsibility of an information security leader in one catchphrase, the response would be “to secure the business.” Although this is the correct answer to the question, the answer becomes quite broad and only proves to be effective when the information security leader has the requisite knowledge of the company’s products, services, and industry in order to do so.

Most information security leaders of today believe that they do this well, however many business executives would disagree with that statement. The reason is that business leaders have such intricate knowledge of how their company operates, that information security leaders generally do not measure up to their expectations. This presents the biggest challenge for information security leaders of the future. As a group, you are going to have to become more atuned to the company’s business. If we work in financial services, we are going to have to think like bankers. If we work in health care, we are going to have to think like doctors.

We will ultimately need to become better educated on the business issues that our organizations face, and be better prepared to address them within the context of our role and the solutions that we offer. We will need to read the same articles, attend the same conferences and join the same social networks as the business leaders. As we do this, we will become more knowledgeable of the business that we are trying to secure. This knowledge will provide us with the necessary confidence to have more meaningful conversations and make more impactful suggestions to our counterparts. As we demonstrate our effectiveness, our peers will include us more in key business decisions and our opinions will become more valued.

Through this new developed trust, we will be able to become more effective in our information security leadership roles. We will gain better knowledge on specific threats facing our businesses and understanding of the impact of regulations facing our industry. We will increasingly learn more about our business ecosystem (partners, suppliers and customers) and the security concerns that are associated with these relationships. In addition, as our companies begin to increasingly integrate technology into their sales and marketing strategies, we will become a resident expert in understanding the security and privacy implications of deploying these tactics.

In the future, we will no longer be able to think like information security professionals who understand business, but we will have to think like business people who understand security.

**We will ultimately need to become better educated on the business issues that our organizations face, and be better prepared to address them within the context of our role and the solutions that we offer.**



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

## EFFECTIVE LEADERSHIP IN ALL FORMS

While many people refer to the highest ranking information security professional in an organization as either the CISO or CSO, this is not necessarily accurate. The “officer” title in a traditional corporate function comes with inherent duties, responsibilities and obligations. Although many information security professionals have elected to assume a title that ends with the word officer, their positions may not be recognized in the same fashion as others who hold this similar title.

Independent of the official title that accompanies the highest ranking information security professional, the one thing that remains constant is the fact that they are the leader of the information security function, and the success of the company’s information security program can be directly correlated to their effectiveness as a leader. For this reason, information security professionals are going to have to develop their leadership skills and demonstrate them on a regular basis to all that they encounter.

When information security professionals begin to look at their leadership skills, they are going to be evaluated on how they assemble their organization and create a culture that attracts high caliber professionals to their team.

Once this group is in place, they will then be judged on how effective they can be in the management of their teams and the development of their talent. In doing this, information security leaders are going to have to make a more conscious effort in learning well established management and team building techniques that will create an information security team that is viewed similarly to the more effective business units within the company.

In addition to refining their internal leadership skills, information security leaders are going to have to strive to be effective leaders outside their own business unit. This will require that they learn to communicate their successes and their wins to the other leaders within the business.

If this sounds like the dreaded “politics,” it’s because it is. All non-trivial projects require that we interact with others, and politics is the word we give to that interaction. Information security leaders need to understand how to work with others, work with organizational structures and gain momentum within the organization due to the successes of their projects and the way that they communicate them. In essence, the information security leader of the future will be an effective marketer, simultaneously building consensus and momentum that will spur the acceptance of his or her information security program throughout the corporate enterprise.

In addition to refining their internal leadership skills, information security leaders are going to have to strive to be effective leaders outside their own business unit. Considering the visibility the profession demands, it will be a key that information security professionals become better at business communication in all of its forms. Information security leaders will need to hone their public speaking, writing and

**In addition to refining their internal leadership skills, information security leaders are going to have to strive to be effective leaders outside their own business unit.**

presentation skills, in order to effectively create the internal brand of their information security program.

## DEMONSTRATED COMMITMENT TO PROFESSIONAL DEVELOPMENT

When many information security professionals think about their own professional development, the first things that come to mind are industry certifications and member organizations. While attaining a CISSP, CISM or a SANS certification are notable accomplishments, they alone do not serve as effective differentiators when it comes to being an information security leader. These certifications hold a great deal of weight within the industry, but once you move into the levels of senior management, they do not hold much relevance. Information security leaders of the future are going to need to strive to attain similar levels of education and credentials that are held by their peers at the C level. Among corporate leaders, many have elected to continue their professional development by gaining advanced degrees from top flight academic institutions, as either full time students or as part of executive MBA programs.

Information security professionals are going to need to seek out these programs and take similar courses of study. For example, if you were to make an investment in an advanced degree, it would be much more valuable and practical to attain a degree in a subject matter associated with broader business skills than to attain a master's degree in information security.

When you think of the business leaders in your organization, many have MBAs but very few have a master's of information security. Achieving a master's degree that is similar to your corporate peers will automatically place you in the same alumni networks and these recognized credentials should enable you to garner immediate respect when interacting with other business leaders within your organization.

Although degrees are important, they are only one component of professional development. Just as with other executives, information security leaders are going to need to make regular investments in their career that will enable them to refine their strengths and develop their weaknesses. Making annual investments in their careers will enable them to develop skills that will help build confidence in their overall ability to lead the security organization. In many cases, it is this confidence that will provide information security leaders with the necessary mental toughness to manage through difficult situations, inspire others and drive change throughout their organizations and their teams.

The information security profession is challenging in its own right. Combine the challenge of the profession with the responsibilities that encompass effective leadership and it becomes more daunting. However, the greater the challenge, the greater the reward. The information security profession attracts people from many

Information security leaders of the future are going to need to strive to attain similar levels of education and credentials that are held by their peers at the C level.

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

#### SNAPSHOT

#### CAREER ADVICE

#### APT

#### SECURITY SAAS

#### CAREERS

#### SPONSOR RESOURCES

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES

different disciplines and backgrounds. Independent of their evolution, most information security professionals aspire to positions of leadership, and the responsibilities and rewards that accompany them. Due to this increasing competition, attaining information security leadership roles will become increasingly more difficult.

In the future, it will become ever more important for information security professionals to make regular investments in their professional development. These investments will be critical in helping them to build a skill matrix that will differentiate them from their information security peers, gain acceptance with other executive team members, and elevate the information security profession to the place that it rightfully deserves in the corporate pecking order. •

---

*Lee Kushner is the president of LJ Kushner and Associates an information security recruitment firm and co-founder of [InfoSecLeaders.com](http://InfoSecLeaders.com), an information security career content website.*

*Mike Murray has spent his entire career in information security and currently leads the delivery arm of MAD Security. He is co-founder of [InfoSecLeaders.com](http://InfoSecLeaders.com) where he writes and talks about the skills and strategies for building a long-term career in information security.*

*Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

# Your One Stop Shop for All Things Security

## Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. **Free.**

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.



[www.SearchSecurity.com](http://www.SearchSecurity.com)

Breaking news, technical tips, security schools and more for enterprise IT professionals.



[www.SearchSecurity.com](http://www.SearchSecurity.com)

Learning materials geared towards ensuring security in high-risk financial environments.



[www.SearchFinancialSecurity.com](http://www.SearchFinancialSecurity.com)

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.



[www.SearchSecurity.co.UK](http://www.SearchSecurity.co.UK)

Information Security strategies for the Midmarket IT professional.



[www.SearchMidmarketSecurity.com](http://www.SearchMidmarketSecurity.com)

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.



[www.SearchSecurityChannel.com](http://www.SearchSecurityChannel.com)



## ADVERTISING INDEX

**Alert Logic** ..... 7  
[www.alertlogic.com](http://www.alertlogic.com)

- Improve Network Security Without Busting Your Budget white paper
- Alert Logic Demo Center - watch how easy we make it to be secure and compliant

**Check Point Software Technologies Ltd.** ..... 12  
<http://www.checkpoint.com>

- White Paper: Check Point Abra - A Secure Virtual Workspace
- Turn any PC into a corporate desktop

**Core Security Technologies** ..... 9  
<http://www.coresecurity.com/>

**ESET** ..... 25  
<http://www.eset.com/>

- ESET NOD32 Antivirus 4 Trial
- Ten Ways to Dodge CyberBullets

**Guidance Software, Inc.** ..... 16  
[www.guidancesoftware.com](http://www.guidancesoftware.com)

- Tackling the Causes of Data Leakage and Data Loss
- Understanding Data Location is Imperative for Data Loss Prevention

**ISACA** ..... 19  
<http://www.isaca.org/>

- Downloads
- Certification

**RSA, The Security Division of EMC** . . 4  
[www.rsa.com](http://www.rsa.com)

- Securing the Administration of Virtualization
- Build a Solid Foundation for Secure Virtualization

**Trend Micro, Inc.** ..... 2  
<http://us.trendmicro.com/us/home/>

- Cloud security meets VMware Ready Virtual Appliance: Read Infonetic's Hybrid SaaS report here.
- OfficeScan 10.5: Unleash the power and performance of physical and virtual desktops. Click here to try now.

**The Academy Pro** ..... 29  
[www.theacademypro.com](http://www.theacademypro.com)

- Free infosec videos for the information security community.

**SystemExperts** ..... 35  
[www.systemexperts.com](http://www.systemexperts.com)

**Glasshouse Technologies** ..... 39  
<http://www.glasshouse.com/>

## TECHTARGET SECURITY MEDIA GROUP



**EDITORIAL DIRECTOR** Michael S. Mimoso

**EDITOR** Marcia Savage

### ART & DESIGN

**CREATIVE DIRECTOR** Maureen Joyce

### COLUMNISTS

Marcus Ranum, Bruce Schneier, Lee Kushner, Mike Murray

### CONTRIBUTING EDITORS

Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

### TECHNICAL EDITORS

Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

### USER ADVISORY BOARD

Edward Amoroso, AT&T  
 Anish Bhimani, JPMorgan Chase  
 Larry L. Brock, DuPont  
 Dave Dittrich  
 Ernie Hayden  
 Patrick Heim, Kaiser Permanente  
 Dan Houser, Cardinal Health  
 Patricia Myers, Williams-Sonoma  
 Ron Woerner, TD Ameritrade

### SEARCHSECURITY.COM

**SENIOR SITE EDITOR** Eric Parizo

**NEWS DIRECTOR** Robert Westervelt

**SITE EDITOR** William Hurley

**ASSISTANT EDITOR** Maggie Wright

**ASSOCIATE EDITOR** Carolyn Gibney

### INFORMATION SECURITY DECISIONS

**GENERAL MANAGER OF EVENTS** Amy Cleary

**EDITORIAL EVENTS MANAGER** Karen Bagley

**VICE PRESIDENT/GROUP PUBLISHER**  
 Doug Olender

**PUBLISHER** Josh Garland

**DIRECTOR OF PRODUCT MANAGEMENT**  
 Susan Shaver

**DIRECTOR OF MARKETING** Josh Garland

**SALES DIRECTOR** Dara Such

**CIRCULATION MANAGER** Kate Sullivan

**ASSOCIATE PROJECT MANAGER**  
 Suzanne Jackson

**PRODUCT MANAGEMENT & MARKETING**  
 Corey Strader, Andrew McHugh, Karina Rousseau

### SALES REPRESENTATIVES

Eric Belcher [ebelcher@techtarg.com](mailto:ebelcher@techtarg.com)

Patrick Eichmann [peichmann@techtarg.com](mailto:peichmann@techtarg.com)

Jason Olson [jolson@techtarg.com](mailto:jolson@techtarg.com)

Jeff Tonello [jtonello@techtarg.com](mailto:jtonello@techtarg.com)

Nikki Wise [nwise@techtarg.com](mailto:nwise@techtarg.com)

### TECHTARGET INC.

**CHIEF EXECUTIVE OFFICER** Greg Strakosch

**PRESIDENT** Don Hawk

**EXECUTIVE VICE PRESIDENT** Kevin Beam

**CHIEF FINANCIAL OFFICER** Jeff Wakely

### EUROPEAN DISTRIBUTION

Parkway Gordon Phone 44-1491-875-386  
[www.parkway.co.uk](http://www.parkway.co.uk)

### LIST RENTAL SERVICES

Julie Brown  
 Phone 781-657-1336 Fax 781-657-1100



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.

All rights reserved. Entire contents, Copyright © 2010 TechTarget. No part of this publication may be transmitted or reproduced in any form, or by any means without permission in writing from the publisher, TechTarget or INFORMATION SECURITY.

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### SNAPSHOT

### CAREER ADVICE

### APT

### SECURITY SAAS

### CAREERS

### SPONSOR RESOURCES