APRIL 2012 • WWW.SCMAGAZINE.COM

SC MAGAZINE

FOR CANADIAN IT SECURITY PROS

REVIEWED IN GROUP TESTS

LogRhythm P38
A highly customizable SIEM with a number of pre-built policies

NetIQ P44
Sentinel is a SIEM solution that is easy to deploy and use

AccessData P48
FTK 4.0 is a serious advance in computer forensic tools

FEATURES:

THE BIG PICTURE

Tools now can sort through "Big Data," so security pros can connect the dots, says Preston Wood, CSO, Zions Bancorporation **P20**

Plugging in privacy

Ontario's privacy commissioner is ensuring that electricity firms protect data as they roll out smart grid technology **PC1**

The next Cold War

Instead of military assaults, today's adversaries hire coders to create attacks that can run for years **P30**

VOLUME 23 NO. 4 • April 2012 • WEBSITE WWW.SCMAGAZINE.COM • EMAIL SCFEEDBACKUS@HAYMARKETMEDIA.COM

SC MAGAZINE
FOR CANADIAN IT SECURITY PROS

REGULARS

Tina Stewart P12

Chester Wisniewski P26

Preston Wood, CSO at Zions Bancorporation P20

FEATURES

Cover photo by Bob Adler

PRODUCT REVIEWS

AccessData FTK 4.0 P49

McAfee ESM P39

SC Magazine™ (ISSN No. 1096-7974) is published 12 times a year on a monthly basis by Haymarket Media Inc., 114 West 26th Street, 4th Floor, New York, NY 10001 U.S.A.; phone 646-638-6000; fax 646-638-6110. Periodicals postage paid at New York, NY 10001 and additional mailing offices. POSTMASTER: Send address changes to SC Magazine, P.O. Box 316, Congers, NY 10920-0316. © 2012 by Haymarket Media Inc. All rights reserved. Annual subscription rates: United States: $98; Canada and Mexico: $110; other foreign distribution: $208 (air service). Two-year subscription: United States: $175; Canada and Mexico: $195; other foreign distribution: $375 (air service). Single copy price: United States: $20; Canada, Mexico, other foreign: $30. Website: www.scmagazine.com.

BPA WORLDWIDE haymarket®

www.facebook.com/SCMag

www.twitter.com/scmagazine

Evolutionary conundrums...

This year's RSA Conference seemed a bit more energized than in recent years. The floor was bustling. Meetings seemed fruitful for many. Press conferences and vendor parties were happening everywhere you looked. And our own SC Awards U.S. Gala was packed.

As I await final official attendee numbers from conference organizers, it was clear that thousands of information security pros turned out (unofficial, pre-audit numbers said more than 21,000 people attended compared to 18,500 the previous year, according to one RSA Conference staffer). All the major vendors were on site, as were government officials, executive leaders, analysts, consultants and more.

To many, it seemed as if larger crowds were hitting classes and were more engaged with speakers and the information presented. As well, questions being bandied about on the show floor were more detailed – attendees really wanted to hear from vendors how their solutions worked and in what ways these offerings actually might help them.

This is an interesting observation and sort of reflects one that was voiced in an online editorial webcast we held mid-March. During that event, "Evolve and Survive," Gene Fredriksen, CISO of Tyco International, said there were a whole host of things driving budget, resources and tweaks to security/risk management programs. Some of these include regulatory mandates, pernicious attacks, like APT, and certainly the success of many of today's infrastructure assaults. Just as many pros believe, he warned that companies and government entities likely already have malcontents roaming their networks, which has brought into existence two groups of exes: those who have been breached and those who have no clue.

Now, what is *not* driving budgets is the fear, uncertainty and doubt (FUD) argument. Fredriksen said that even if some less farsighted practitioners are relying on such methods, more knowledgeable C-level cats just aren't buying.

FUD simply doesn't fly any longer. Strategic moves made to safeguard critical data and harden systems, as opposed to sometimes haphazard tactical ones, are what is necessary for the long-run success of any business and government agency. And so, too, are traits like agility and vision.

Fredriksen said to move methodically and quickly is a necessity these days. Failing that, organizations, their leaders and, most assuredly, their CISOs/CSOs will simply transform into today's dinosaurs. And, well, we all know what happened to those guys.

Illena Armstrong is VP, editorial director of SC Magazine.

> "Fear, uncertainty and doubt simply doesn't fly any longer."

WHAT IS SCWC 24/7?

SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

THIS MONTH

SC WORLD CONGRESS 24/7 eSymposium

April 24
eSymposium: Cyber espionage

Those engaging in cyber espionage to steal various classified and/or proprietary documents from U.S. agencies and other organizations are riding high. The theft of this critical information shows that attackers are enlisting whatever weaknesses in systems they can to siphon corporate and government data, often going unnoticed for months. Experts share background on the types of attacks to watch out for and what you can do to thwart them.

ON DEMAND

PCI compliance

Unlike other rules mandating technology usage, the PCI Data Security Standard is far more specific and not open to "user interpretation." But, when it comes to implementing precautions, such as those outlined in PCI DSS, many companies balk because they fear the added costs. Experts provide some pointers to how they are reaching a PCI-compliant state, and staying within budget.

Mobile security

To safeguard handhelds used by business execs is a constant trial – one that rarely is satisfactorily remedied. But companies must find a way to manage and protect these endpoints. We offer solutions.

FOR MORE INFO

For information on SCWC 24/7 events, contact Natasha Mulla at natasha.mulla@haymarketmedia.com.

For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazineus.com/scwc247.

SC WORLD CONGRESS 24/7

WHO'S WHO AT SC MAGAZINE

EDITORIAL
VP, EDITORIAL DIRECTOR Illena Armstrong
illena.armstrong@haymarketmedia.com
EXECUTIVE EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DIGITAL CONTENT COORDINATOR Marcos Colón
marcos.colon@haymarketmedia.com
TECHNOLOGY EDITOR Peter Stephenson
peter.stephenson@haymarketmedia.com
SC LAB MANAGER Mike Stephenson
mike.stephenson@haymarketmedia.com
DIRECTOR OF SC LAB OPERATIONS John Aitken
john.aitken@haymarketmedia.com
SC LAB EDITORIAL ASSISTANT Judy Traub
judy.traub@haymarketmedia.com
PROGRAM DIRECTOR, SC CONGRESS
Eric Green *eric.green@haymarketmedia.com*

CONTRIBUTORS
Stephen Lawton, Deb Radcliff, Jim Romeo

DESIGN AND PRODUCTION
ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com
VP OF PRODUCTION & MANUFACTURING
John Crewe
john.crewe@haymarketmedia.com
PRODUCTION MANAGER
Krassi Varbanov
krassi.varbanov@haymarketmedia.com

SC EVENTS
EVENTS DIRECTOR Natasha Mulla
natasha.mulla@haymarketmedia.com
SENIOR EVENTS COORDINATOR Anthony Curry
anthony.curry@haymarketmedia.com
EVENTS COORDINATOR Maggie Keller
maggie.keller@haymarketmedia.com

U.S. SALES
VP, SALES DIRECTOR David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST BUSINESS MANAGER
Matthew Allington (415) 346-6460
matthew.allington@haymarketmedia.com
NATIONAL ACCOUNT MANAGER - EVENT SALES
Mike Alessie (646) 638-6002
mike.alessie@haymarketmedia.com
ACCOUNT EXECUTIVE Dennis Koster
(646) 638-6019 *dennis.koster@haymarketmedia.com*
SALES/EDITORIAL ASSISTANT Roo Howar
(646) 638-6104 *roo.howar@haymarketmedia.com*

LICENSE & REPRINTS ACCOUNT EXECUTIVE
Malika Touré (646) 638-6101
malika.toure@haymarketmedia.com

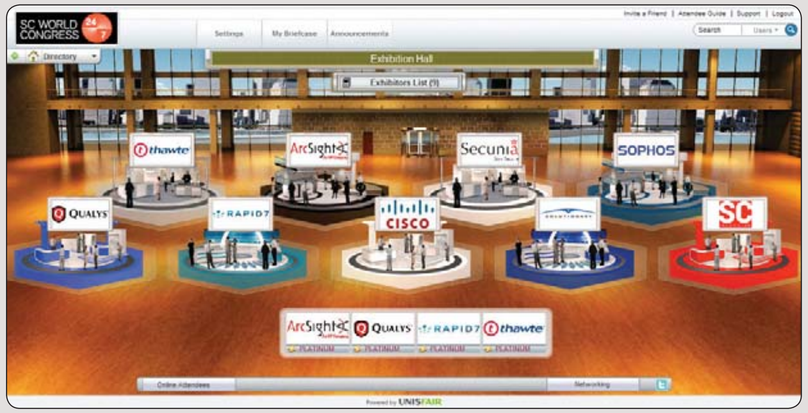
EMAIL LIST RENTAL
EMAIL SENIOR ACCOUNT MANAGER
Frank Cipolla, Edith Roman Associates
(845) 731-3832 *frank.cipolla@epostdirect.com*

CIRCULATION
AUDIENCE DEVELOPMENT DIRECTOR
Sherry Oommen (646) 638-6003
sherry.oommen@haymarketmedia.com
CUSTOMER DATA MANAGER
Joshua Blair (646) 638-6048
joshua.blair@haymarketmedia.com

SUBSCRIPTION INQUIRIES
CUSTOMER SERVICE: (800) 558-1703
EMAIL: Haymarket@cambeywest.com
WEB: www.scmagazine.com/subscribe

MANAGEMENT
CEO OF HAYMARKET MEDIA Lee Maniscalco
EXECUTIVE VICE PRESIDENT Tony Keefe

SC WORLD CONGRESS 24/7



The always-on resource for IT professionals

As a complement to our annual SC Congress Conference and Expo events, *SC Magazine* has launched a permanent website environment that will be open to our readers around the clock all year long. Each month we host an event on the site focused around a pertinent subject that you as an IT security pro face on a regular basis. This is a completely FREE offering to keep you informed of the newest developments in the industry. Participants can earn up to eight CPE credits for an eConference & Expo, and two CPE credits for a Virtual Symposium.

Join us for our next virtual events

SC WORLD CONGRESS 24/7 eSymposium

April 24 – Cyber espionage:
Hacktivist groups have made it clear that no computer network are immune from penetration. Perhaps today's top challenge facing senior IT personnel is to get the C-suite to sign off on implementing a 24/7 security system before the enterprise suffers a breach.

SC WORLD CONGRESS 24/7 eSymposium

May 17 – Advanced monitoring and forensics:
Hacktivist groups have made it clear that no computer network are immune from penetration. Perhaps today's top challenge facing senior IT personnel is to get the C-suite to sign off on implementing a 24/7 security system before the enterprise suffers a breach.

For a complete schedule and to register, visit our 24/7 site: scmagazine.com/scwc247

SC WORLD CONGRESS 24/7

Upcoming events

May 24
eSymposium:
Privacy and security

June 7
Canadian eSymposium

June 21
eConference: Auditing and compliance

July 12
eSymposium: Database security

July 24
eConference: Securing the cloud

Aug. 23
eSymposium: Social networking security

Sept. 6
eSymposium: Mobile security

Sept. 18
eConference: Data security

Oct. 9
eConference: PCI

Oct. 25
eSymposium:
Advanced persistent threats

Nov. 15
eSymposium: Vulnerability management

Dec. 4
Canadian eSymposium

For more information

SALES
Mike Alessie
National accounts manager
(646) 638-6002
mike.alessie@haymarketmedia.com

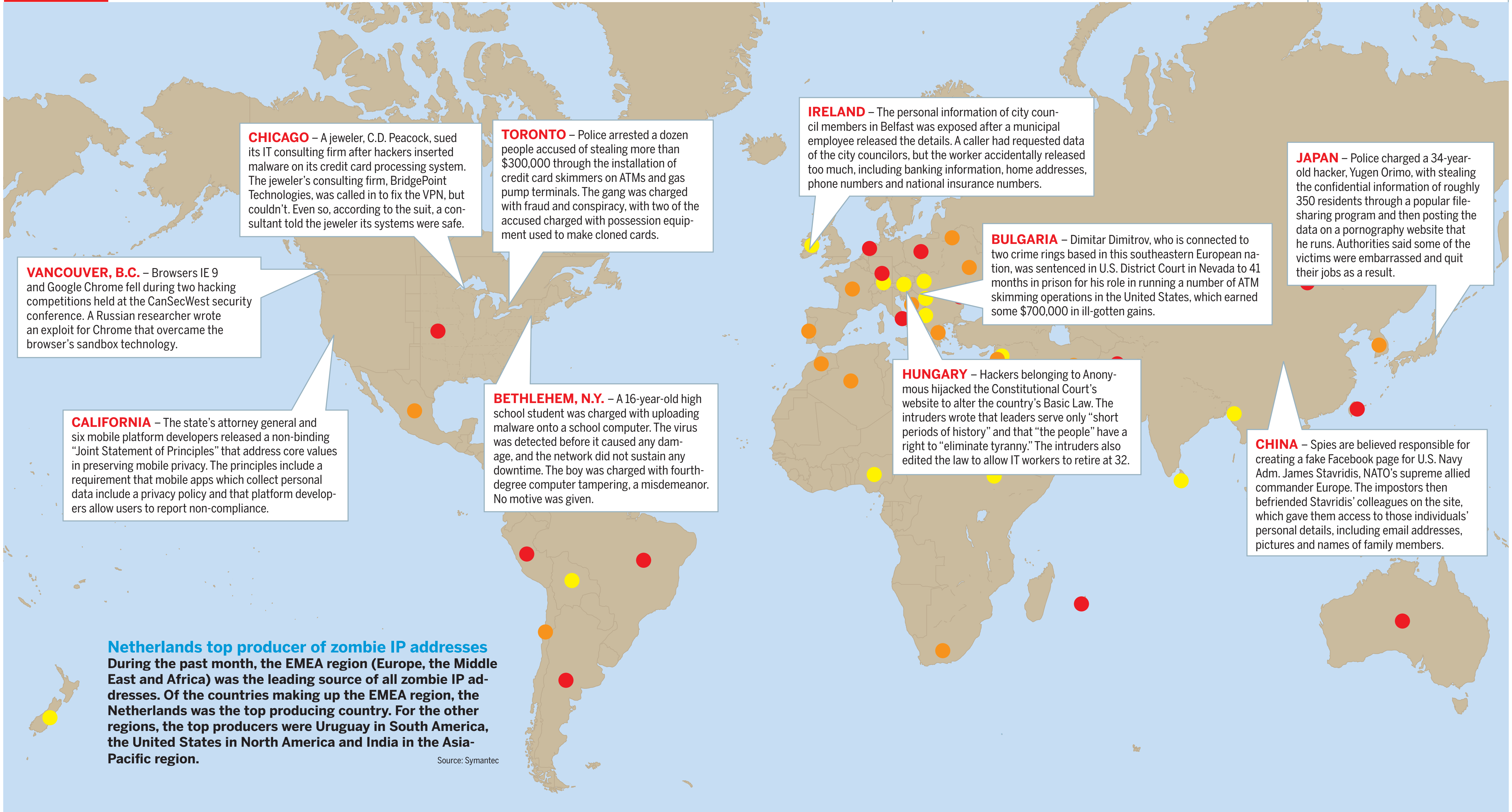
EVENTS
Anthony Curry
Senior events coordinator
(646) 638-6009
anthony.curry@haymarketmedia.com

SC MAGAZINE ThreatReport

Cyber criminal activity across the globe, plus a roundup of security-related news

Colored dots on the map show levels of spam delivered via compromised computers (spam zombies). Activity is based on the frequency with which spam messaging corresponding with IP addresses are received by Symantec's network of two million probes with a statistical reach of more than 300 million mailboxes worldwide.

🟥 HIGH-LEVEL ACTIVITIES
🟧 MEDIUM-LEVEL ACTIVITIES
🟨 LOW-LEVEL ACTIVITIES



CHICAGO – A jeweler, C.D. Peacock, sued its IT consulting firm after hackers inserted malware on its credit card processing system. The jeweler's consulting firm, BridgePoint Technologies, was called in to fix the VPN, but couldn't. Even so, according to the suit, a consultant told the jeweler its systems were safe.

TORONTO – Police arrested a dozen people accused of stealing more than $300,000 through the installation of credit card skimmers on ATMs and gas pump terminals. The gang was charged with fraud and conspiracy, with two of the accused charged with possession equipment used to make cloned cards.

VANCOUVER, B.C. – Browsers IE 9 and Google Chrome fell during two hacking competitions held at the CanSecWest security conference. A Russian researcher wrote an exploit for Chrome that overcame the browser's sandbox technology.

CALIFORNIA – The state's attorney general and six mobile platform developers released a non-binding "Joint Statement of Principles" that address core values in preserving mobile privacy. The principles include a requirement that mobile apps which collect personal data include a privacy policy and that platform developers allow users to report non-compliance.

BETHLEHEM, N.Y. – A 16-year-old high school student was charged with uploading malware onto a school computer. The virus was detected before it caused any damage, and the network did not sustain any downtime. The boy was charged with fourth-degree computer tampering, a misdemeanor. No motive was given.

IRELAND – The personal information of city council members in Belfast was exposed after a municipal employee released the details. A caller had requested data of the city councilors, but the worker accidentally released too much, including banking information, home addresses, phone numbers and national insurance numbers.

BULGARIA – Dimitar Dimitrov, who is connected to two crime rings based in this southeastern European nation, was sentenced in U.S. District Court in Nevada to 41 months in prison for his role in running a number of ATM skimming operations in the United States, which earned some $700,000 in ill-gotten gains.

HUNGARY – Hackers belonging to Anonymous hijacked the Constitutional Court's website to alter the country's Basic Law. The intruders wrote that leaders serve only "short periods of history" and that "the people" have a right to "eliminate tyranny." The intruders also edited the law to allow IT workers to retire at 32.

JAPAN – Police charged a 34-year-old hacker, Yugen Orimo, with stealing the confidential information of roughly 350 residents through a popular file-sharing program and then posting the data on a pornography website that he runs. Authorities said some of the victims were embarrassed and quit their jobs as a result.

CHINA – Spies are believed responsible for creating a fake Facebook page for U.S. Navy Adm. James Stavridis, NATO's supreme allied commander Europe. The impostors then befriended Stavridis' colleagues on the site, which gave them access to those individuals' personal details, including email addresses, pictures and names of family members.

Netherlands top producer of zombie IP addresses

During the past month, the EMEA region (Europe, the Middle East and Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA region, the Netherlands was the top producing country. For the other regions, the top producers were Uruguay in South America, the United States in North America and India in the Asia-Pacific region.

Source: Symantec

ThreatStats

The biggest increases in month-over-month zombie activity occurred in Vietnam

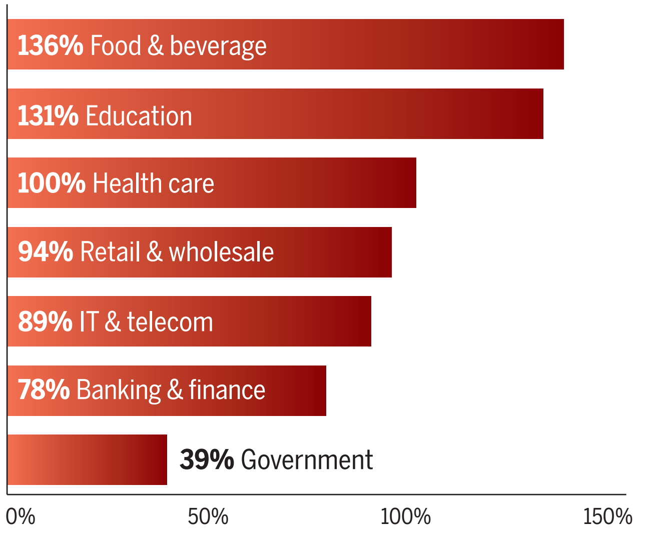
Spam The world's worst spam-support ISPs

Position	ISP	Number of current known spam issues
1	chinanet-zj	58
2	ovh.net	57
3	telefonica.com.ar	50
4	chinanet-fj	49
5	unicom-cn	46
6	iliad.fr	45
7	unicom-hl	45
8	hostnoc.net	44
9	telefonica.com.br	43
10	chinanet-gd	43

The networks listed knowingly provide service to criminal spam gangs and ignore alerts from anti-spam systems and internet users.

Source: The Spamhaus Project

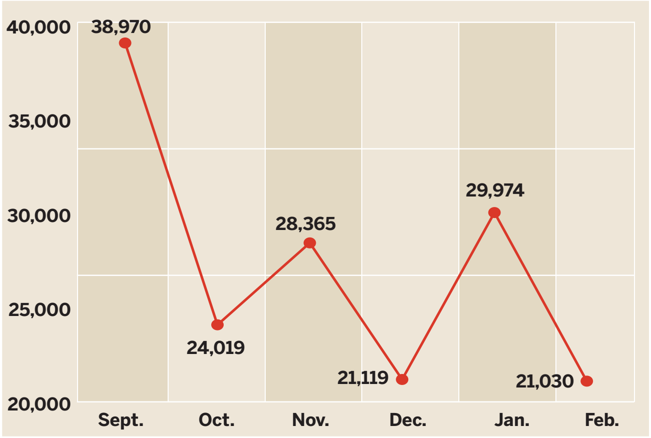
Malware Vertical encounter rate



The chart above reflects the encounter rate of web malware across a selection of industry verticals. Rates above 100 percent reflect a higher-than-median rate of encounter and rates below 100 percent reflect a lower-than-median rate.

Source: Cisco ScanSafe

Phishing A 30 percent drop in February



February marked a 30 percent drop in worldwide phishing volume. The U.S. finally overtook the U.K. as the country that endured the highest phishing volume. Canada landed in a surprising second place in terms of global volume in February.

Source: RSA Anti-Fraud Command Center

Top breaches of the month Data loss

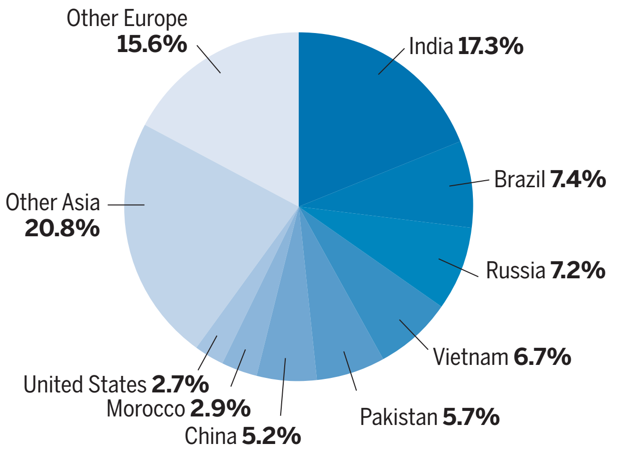
Name	Type of breach	Number of records
Piedmont Behavioral Healthcare (Concord, N.C.)	An Alamance County employee mistakenly changed a lock on the facility that housed data servers with personal health information.	50,000
St. Joseph Health System (Calif.)	Protected patient information from several California hospitals may have been available on the internet for one year.	31,800
Central Conn. State Univ. (New Britain, Conn.)	A malware infestation exposed the information of current and former faculty, staff and student workers.	18.763

Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005:

544,669,041 (as of March 9)

Source: Privacy Rights Clearinghouse (data from a service provided by DataLossDB.org, hosted by the Open Security Foundation)

Zompie IPs Global distribution



The biggest increases in month-over-month zombie activity occurred in Vietnam and China, while the largest decreases occurred in India and Pakistan.

Source: Commtouch Software Online Labs

Top 5 attacks used by U.S. hackers

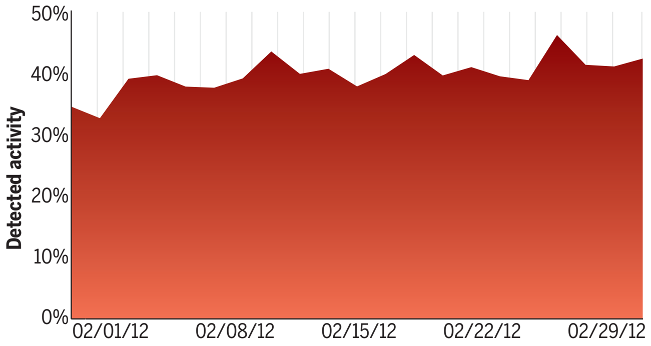
1. Butterfly bot
2. ZeuS trojan
3. ZeroAccess trojan
4. Downloader trojan
5. Sinowal trojan

Top 5 attacks used by foreign hackers

1. Butterfly bot
2. ZeroAccess trojan
3. ZeuS trojan
4. Sinowal trojan
5. Downloader trojan

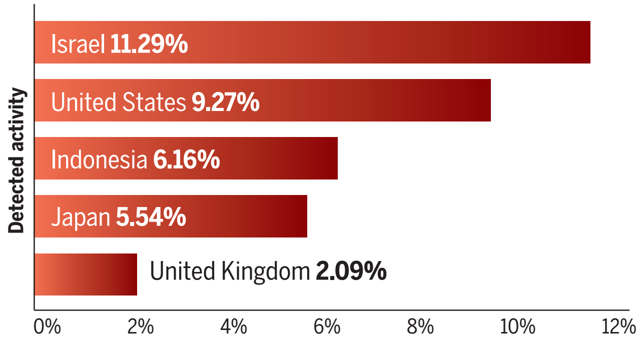
There were 6,748,788 attacks in the U.S., primarily originating from Chicago; Los Angeles; Dallas; New York; and San Rafael, Calif. There were 814,385 foreign attacks, primarily originating from Beijing; Chisinau, Moldova; Buenos Aires, Argentina; Caracas, Venezuela; and Sanitago, Chile. Source: Dell SecureWorks

Spam rate Compared to global email



Spam rate indicates the accumulated emails tagged as unsolicited.

Received spam Top five regions



Source: Fortinet Threatscape Report

Internet dangers Top 10 threats

	Name	Movement	Date first observed	Type	Last week	Weeks on list
1	Sality.AU	▲	12/06/10	Worm	0	0
2	Winwebsec	▲	09/22/10	Scareware	6	2
3	Zbot.gen!AF	▼	12/16/10	PasswordStealer	2	1
4	VBInject.UG	▲	01/29/12	MalwarePackage	12	1
5	Zbot.gen!Y	▲	09/21/10	PasswordStealer	8	1
6	Rebhip.A	▲	09/21/10	Worm	18	14
7	VBInject.RT	▲	07/22/11	MalwarePackage	0	0
8	Sinowal.gen!Y	▲	06/10/11	PasswordStealer	0	0
9	Alureon.G	▲	12/16/10	Virus	0	0
10	Expiro.AF	▲	05/26/11	Virus	0	0

Source: Kindsight Security Labs

Update

2 minutes on... A new way to net phish is in the works P14

Me and my job Computer forensic and litigation support P15

Skills in demand Virtualization security architects are needed P15

NEWS BRIEFS

»A **malicious attacker** deliberately attempted to interfere with a crucial **party leadership vote** in **Canada** last month, according to a company commissioned to run the online voting system used.

Scytl Canada, which provides online balloting services, confirmed that a deliberate distributed denial-of-service attack (DDoS) was launched in an attempt to disrupt the federal **NDP** leadership vote on March 24.

More than 10,000 separate computers were used in the DDoS attack, which began during the second round of balloting. Reports of timeouts on the system caused operators to examine the logs, from which they identified an external attack.

Scytl increased system throughput and blocked malevolent IP addresses, and managed to keep the system running at a slower speed.

The attackers used a **botnet** with compromised machines located mainly in Canada, the company said.

The NDP leadership election was held following the death of former leader **Jack Layton** in August.

The motive for the attack is unclear. But according to research firm Environics, the NDP and its bitter rival, the **Conservative Party**, tied in popularity in March, with the latter's approval rate dropping 10 points. The last time that the NDP was in first place – tied or otherwise – was in 1987.

A leading hacktivist lived in this housing project in Manhattan's East Village.

AP Photo/Mary Altaffer

Hacker snitch

Following his arrest in June for a number of high-profile attacks, Hector Monsegur, aka Sabu, continued to urge on his fellow hacktivists...while apparently in cahoots with the FBI to rat them out. When he was picked up by authorities, Monsegur was helping to lead LulzSec, an offshoot of Anonymous. According to the FBI, his statements helped law enforcement charge five other people with roles in hacks.

THE QUOTE

"Unless you have visibility into where your data is going, how do you manage risk?"

— Dave Cullinane, CISO of eBay, on a panel at February's RSA Conference expressing concern about cloud implementations

»The investigation into fraudulent **robocalls** in Canada escalated this month, as **Elections Canada**, an independent agency that oversees voting, said that 7,000 calls had gone out across the country.

In February, complaints emerged about fraudulent calls to voters in the Ontario riding of Guelph, misdirecting them to non-existent polling stations during the national election. Since then, voters in ridings across the country have come forward.

Marc Mayrand, chief electoral officer at **Elections Canada**, has now opened 250 case files on 800 individual complaints, covering 10 provinces and one territory.

The calls have been traced to **RackNine**, an Edmonton-based web-hosting company that operates an automated calling service. It was hired by the **Conservative Party** of Canada for its national election campaign.

"It's absolutely outrageous," said Maynard. "It should not be tolerated It should be sanctioned severely."

Maynard was called to testify to a parliamentary committee about the matter, but many Canadian media were involved in a lock-up interview with Finance Minister **Jim Flaherty**, who was announcing the Canadian budget.

Canada's **CBC** found in an investigation this month that many voters who had received robocalls had previously been contacted by the Conservative Party and had told it that they would not be voting for it. Some claim to have received misleading calls attempting to redirect them to incorrect voting locations, which they then tracked to Conservative Party offices.

Prime Minister Stephen Harper continues to deny Conservative Party involvement in the robocalls affair.

Debate» Anti-virus is essential.

FOR

David Hartley
ESET senior research fellow

Malware is no imaginary problem, especially on Windows PCs: Anti-virus labs see tens and even hundreds of thousands of new samples daily, and infections are all too common. It's better to ask, are there instances where anti-virus is not necessary? Perhaps. For instance, if your system can't trade data or applications with other systems; if it runs an operating system for which there is no known malware and no possibility of a zero-day attack against the OS or applications; if there is no way of installing any application that hasn't been screened proactively and with 100 percent effectiveness by system and connectivity providers; if you're a techie with the time, knowledge and skills to avoid any situation that poses any risk whatsoever; and, if you can, properly administer alternative and multilayered security approaches, such as whitelisting and log analysis.

But those are scenarios that fit a small proportion of computer users, and even in some of those cases, anti-virus remains a helpful supplementary precaution.

AGAINST

Jeremiah Grossman
founder and CTO of WhiteHat Security

Let's make one thing clear: It's not a question of using anti-virus software or not, it's a question of how much should be spent on it.

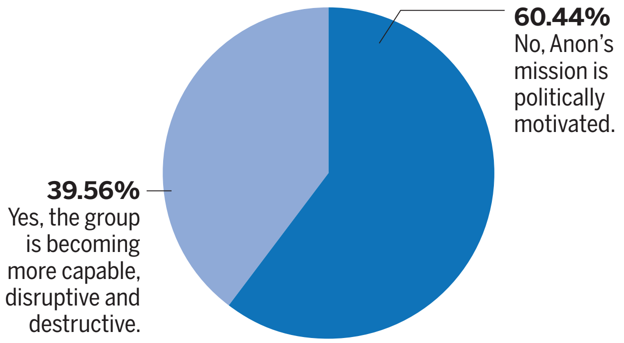
As Gartner reports, consumers will spend nearly $5 billion this year on AV software. This is far too much money for something with such a poor track record, and one the bad guys evade almost at will. It is far too much, especially when free alternatives, like Microsoft Security Essentials, give consumers the bulk of what they need and allows them to spend money on things that actually protect their data.

Computers crash, people get hacked, bad guys steal personal data – victims suffer the consequences with or without AV software. Consumers, and businesses too, must not view AV as a primary defense. A better way for consumers to protect themselves is to take three steps that will save them money and protect their digital assets:

First, install "free" AV software. Next, invest in a good backup solution. And finally, upgrade the web browser.

THE SC MAGAZINE POLL

Does Anonymous pose a threat to the U.S. power grid?



To take our latest weekly poll, visit **www.scmagazine.com**

THE STATS

$46m

a year is the average spent on computer security by 21 energy companies surveyed by Bloomberg

69% of known cyber strikes against their systems are thwarted by the utility companies polled

Source: Bloomberg Government/ Ponemon Institute, Feb. 2012

THREAT OF THE MONTH

Ukash ransomware

What is it?
What makes this threat unique is the effective use of localization and the impersonation of a law enforcement body. It highjacks the computer and holds it hostage for payment.

How does it work?
The malware is a PE file distributed via email or downloaded by other malware. It replaces the Explorer.exe file on the system and blocks GUI access to the file system and taskbar. A graphic is presented claiming the computer has been used to commit an act of terrorism. A demand for payment is levied in the form of a fine.

Should I be worried?
This attack vector is working throughout Europe. The bug removes the original Explorer.exe file, but doesn't target data. Recovery is possible by restoring the original Explorer.exe file via the command line and deleting the malware executable.

How can I prevent it?
Awareness goes a long way. Plus, performing regular backups will limit the impact if data is targeted.

Source: Donald DeBolt, director of threat research, Total Defense

2 MINUTES ON…

A new way to net phish

Some 300 billion emails circulate each day, but they still can't escape a fundamental flaw – that users who receive these messages can't be certain who sent them. This underlying weakness has led to phishing and spam being persistent threats on the web for many years.

But the age-old quest for accountability in digital communication has a new champion: Domain-Based Message Authentication, Reporting and Conformance (DMARC), a new specification whose creators hope soon will be adopted by the Internet Engineering Task Force (IETF).

DMARC has a few things working in its favor that past authentication attempts didn't. For one, it is not a standalone protocol, but one that works in concert with popular security methods already adopted: DomainKeys Identified Mail (DKIM), a technique that associates a domain name to an email message, and Sender Policy Framework (SPF), which detects spoofing.

"DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms," according to the group. "This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo and any other email receiver implementing DMARC."

Second, DMARC has some muscle behind it. Not only are the major email providers behind the system, but so are some of the most digitally abused brands, such as PayPal. And third, DMARC gets away from the traditional approach of blacklisting.

"DMARC gives us an ability not just to guess if that message is good or bad, but to actually know whether it came from a legitimate organization," said Patrick Peterson, founding member of DMARC and CEO of email security firm Agari.

DMARC uses DKIM and SPF to vet, at the domain level, the trustworthiness of emails. Email providers can then, through their own policy and through user preferences, get as granular as they wish. That may mean simply monitoring unauthenticated messages all the way to outright blocking them.

The specification also allows senders to publicize their email handling practices, while receivers can offer feedback.

Critics of DMARC argue that as long as people are involved in the process, users still will fall for phishing and spam.

"Humans don't work the way technology works, they work the way humans work," said Joseph Steinberg, CEO at Green Armor Solutions, an authentication vendor.

– Marcos Colón

72% of all inbound email is spam

Source: M86 Security Labs

JOBS MARKET

Me and my job

Douglas Vitale
information assurance and forensic expert for a major utility company

How do you describe your job to average people?
My main responsibilities are computer forensics and litigation support. On the forensic side, I assist our investigators by collecting electronic data from hard drives, servers and email to find evidence they can use in their investigation. On the litigation side, I am responsible for collecting electronically stored information (ESI) for individuals involved in lawsuits. This is done by collecting the ESI from hard drives, servers and email, and processing the data so our legal team can review and produce the relevant files.

Why did you get into IT security?
With a bachelor's degree in criminal justice, my background is in investigations and physical security, but I've always had a passion for computers, so I wanted to find a way to integrate both. I went back to school for my master's in computer science and while in school began searching for a career that I would enjoy and be able to integrate with my knowledge and experience. Once I found out about computer forensics, I knew that was the field I wanted to go into after I graduated. I was fortunate enough to find a forensic position immediately after graduation.

What was one of your biggest challenges?
One of the biggest challenges that I'm constantly faced with is the new technologies that are introduced on a daily basis. As a computer investigator, I need to stay ahead and be knowledgeable of what is coming out.

What keeps you up at night?
Unlike other fields, computer forensics/litigation support is a new and evolving field. Every day, I spend an hour or more reading blogs and forums to familiarize myself with the new advancements in computer hardware and software. I also stay abreast of recent court opinions and case studies to see how the legal side of computer forensics/litigation support is progressing.

Skills in demand

As more organizations move into the cloud, the demand for virtualization security architects is growing. Vendors want to drive offerings, services firms need customer-facing solutions architects, and end-users seek help with strategy and migration.

What it takes

Experience and knowledge of SaaS development, multi-tiered application environments, database and storage technologies, virtualization platforms, ID management and authentication, and regulatory requirements are needed.

Compensation

Base compensation ranges from $130k to $200k, plus incentives.

Source: Jeff Combs, director of recruiting at Acumin - US

Briefs Company news

»**Vormetric**, provider of encryption and key management for enterprise systems, has appointed **Tina Stewart** vice president of marketing. She will oversee the company's global marketing activities and will report directly to company CEO, Richard Gorman. Previously Stewart held marketing, branding and communication roles at **Juniper Networks**, **Arbor Networks** and **Network Associations**, which since has been acquired by **McAfee**.
www.vormetric.com

Tina Stewart, vice president of marketing, Vormetric

»**AlienVault**, provider of open-source security information and event management solutions, has appointed **Barmak Meftah** as president and CEO, and **Roger Thornton** as chief technology officer. Meftah recently served as VP of the software security division at **HP** and before that as chief products officer of **Fortify Software**, which HP acquired. Thornton founded **Fortify**.
www.alienvault.com

»**Joey Tyson**, a former security engineer at consultant **Gemini Security Solutions**, has joined the security team at **Facebook**. He will focus on privacy, and will be tasked with reviewing and influencing policy, as well as engaging the site's hundreds of millions of members.
www.facebook.com

»**Solera Networks**, provider of network security analytics, has won $20 million in funding from **Intel Capital** to be used to expand global sales, marketing and product development initiatives around its threat response products, which enable deep packet inspection of real-time traffic.
www.soleranetworks.com

»Anti-virus firm **Trend Micro** has hired **Tom Kellerman** as the company's first-ever U.S. vice president of cyber security. Kellerman, the former chief technology expert of wireless security provider **Air Patrol** and vice president of security awareness at **Core Security**, will act as an adviser to government customers. In addition, Kellerman is a member of the Commission on Cybersecurity for the 44th President, which aims to guide federal policy making.
www.trendmicro.com

Tom Kellerman, U.S. vice president of cyber security, Trend Micro

» **NIST** has established the **National Cyber Center of Excellence**. The Maryland-headquartered center seeks to accelerate the mass adoption of security tools and technologies that can be used to secure e-government and e-commerce. Funded for $10 million, the center will work to develop new security approaches that can meet real-world demands.
www.nist.gov

» **CrowdStrike**, a company created to help organizations protect intellectual property and national security information, has launched. Co-founded by **George Kurtz**, the former CTO of **McAfee**, CrowdStrike will focus on determining who is behind attacks, which it believes is the most critical piece in protecting assets. **Dmitri Alperovitch** and **Gregg Marston** are the other founders.
www.crowdstrike.com

PCI: Five years older and wiser

Mike Mitchell
VP, global network operations, American Express

Over the past few years, adoption of and compliance with PCI standards has made it more challenging for criminals to steal large volumes of credit card data. Some of the improvements in the evolution of the standards, like log monitoring and other steps – a result of industry feedback and involvement in standards development – have increased the likelihood that an organization can identify anomalies indicative of breaches, and hopefully stop them before the criminals abscond with payment data.

So, where do we take it from here? Our mission at the council remains the same: protecting cardholder data must be at the center of our efforts. The PCI standards offer the best protection of payment card data across all payment channels. We must continue to increase awareness, and provide the education and resources for security and business professionals alike to secure their organizations' data.

At the council, we are going to apply continued focus on understanding technologies that offer Payment Card Industry Data Security Standard (PCI DSS) scope reduction for merchants, including point-to-point encryption (P2PE) and tokenization. While there's no silver bullet, we believe that through these technologies we can make it simpler, faster and more efficient for smaller merchants to adopt the PCI standards.

We will continue to engage all PCI stakeholders with new opportunities for participation, and provide a dedicated period for collecting and sharing feedback. This, in turn, will not only result in additional supplementary guidance, but also in strong revisions to the next iteration of the PCI standards, to be released in 2013. We believe that through this feedback loop we are gathering the input of the widest collection of payment and security experts around the world in an effort to reduce payment card fraud.

Since people and processes are a critical part of a successful security mix, the council is expanding the current Payment Card Industry Security Standards Council training offerings to continue to increase payment card security expertise.

Additionally, we've incorporated awareness training so that all can better understand what PCI is about and how it applies to their role in protecting payment card data.

But we need your feedback to help us grow our knowledge base, keep up with and mitigate the latest attacks, and adopt the newest technologies safely and securely. I used to have a boss that periodically asked me a particular question, which I now turn to you to share: "What have you done for payment security lately?"

Christopher Barr Photography

30 seconds on...

»Keep on pushing
We have to keep pushing adoption of PCI DSS across the payment chain, and encourage further adoption among smaller merchants and franchise organizations, says Mitchell.

»All must get involved
When he says "we," he means all possible parties along the payment chain – acquiring banks, technology vendors, security assessors, merchants and industry associations.

»Obliterate old exploits
Further, he says, efforts must be doubled so threats don't continue to move down the chain, leaving mom-and-pop shops an easy target for an antiquated exploit.

»For further information
More on the PCI Security Standards Council at https://www.pcisecuritystandards.org. To join, visit https://www.pcisecuritystandards.org/get_involved/index.php.

David Pfeiffer, marketing director, mSeven Software

Shutting access to passwords

Mobile devices free us from being tied to an office computer when accessing personal information: web logins, passwords, PINs, account numbers, etc. Imagine a mobile device falling into the wrong hands – resulting in the draining of bank accounts co-opting of identities.

A lost or stolen phone constitutes a serious security threat because the attacker has unlimited time to gain access to its data. Therefore, important personal information should not be stored in any unsecured application.

Instead, critical data should be stored in a digital wallet or password manager with strong encryption – such as 256-bit Blowfish – to keep these assets safe, secure and accessible.

Front-door attacks occur when a hacker continually attempts to guess a password. A good password manager closes this front door with a self-destruct feature that can wipe data after a number of password-entry attempts. Further, an auto-lock feature will automatically lock the application in instances where users set the device down for a moment and it disappears.

Alternatively, backdoor attacks occur when a hacker has cracked the device and can access the password manager's database. Here too a strong password manager will help as it will encrypt personal data with a strong algorithm, and never store the password itself on the device. Assuming a strong password is used, this approach would take years for even a super computer to try every possible combination.

Finally, transmission attacks take place when data is captured during broadcast, such as during data sync activity. A solid password manager will have a sync architecture that encrypts the data with a separate, strong password before it is transmitted or stored on a cloud server.

A password manager should serve as an impenetrable lock to block front or backdoor access to your most sensitive data.

Ken Sanofsky, general manager, North America, Paessler

Smart network management

As IT security staff contend with the threat from cyber crime and fast-spreading malware, they consistently look for technologies to give them comprehensive network security. Implementing a network monitoring solution provides IT staff with advance warning about threats, as well as visibility into bandwidth issues that can signal security risks and point out hardware deficiencies.

Network monitoring solutions for the enterprise should be holistically integrated with the complete security suite, including various port scanners, virus monitors and encryption software that are already in place. Monitoring can identify unusual peaks in usage, which can be a sign of a threat or an indication that another part of the system is pulling too many resources and should be scanned for infection.

Without instant notification of a threat, IT admins are not able to react in enough time to limit or prevent the leakage of data or interruption of services. Enhanced visibility allows staff to better analyze and fix security gaps to prevent future problems.

The most sophisticated monitoring tool is useless if it cannot quickly alert IT staff to the existence of a security threat. Network managers need a solution that uses multiple notification technologies beyond email or SMS, including notifications to mobile devices, simple network management protocol (SNMP) traps and alarm sound files. Alerts should be segmented into logical categories, such as notices for escalations, multiple conditions, thresholds and limit warnings where usage is above/below a certain value.

Solutions that offer robust reporting will be able to provide information on requests, up- and downtime percentages, the top bandwidth users and top ping times, among many other data points. By using the monitoring solution as a source of real-time reporting, IT security management can plan infrastructure updates and reduce network costs.

> "Network managers need a solution that uses multiple notifications..."

Got something to say?

Send your comments, praise or criticisms to scfeedbackUS@haymarketmedia.com. We reserve the right to edit letters.

From the online mailbag

In response Executive Editor Dan Kaplan's January cover story, The new wave:

As director of the National Collegiate Cyber Defense Competition, I was delighted to read your article, "The new wave: Modern security education." There is a growing gap between cyber security professionals' availability and our national need. I'd like to share some of our observations regarding the value and future of cyber competitions to help mitigate this shortage.

Here at the Center for Infrastructure Assurance and Security, where the inaugural CCDC contest was organized in 2005, competitions are recognized as one of the three legs on which strengthening America's cyber security depends, along with state and community exercises, and professional education and certification.

We encourage competitive programs from high school students on up because they have proven to uniquely encourage skill sets vital to their professional prospects: teamwork, creative thinking and communication skills.

Events like DC3 Digital Forensic Challenge, CyberPatriot, and soon, the National Cyber League, will be available to encourage thousands more. Our Panoply program, which stresses both assessment and defensive skills, is preparing an online competition: online team cyber sports allow even more students from remote or economically disadvantaged areas to participate.

So far, more than 3,500 students have participated just in CCDC events since its inception, including Alex Levinson. As your article points out, CCDC proved to be his gateway to fulfillment. His RIT team competed in the NCCDC last year – like many other CCDC competitors one season was not enough for Alex.

There's very exciting work being done here at CIAS and our University of Texas at San Antonio.

Thank you, again, for the excellent article; but more, for the attention you and *SC Magazine* focus on security issues and the manner they are articulated.

Dwayne Williams
director, NCCDC

In response to Executive Editor Dan Kaplan's February cover story, Adjoining islands:

I just wanted to let you know that I thought you did a great job on the article. It is obvious that you knew what you were reporting. It is not that often you find someone who understands what they are writing about, and this is a complex subject. Thanks again for the opportunity.

Gordon Bruce, director, information technology, city of Honolulu

In response to our Data Breach Blog:

I follow the Data Breach Blog at your publication regularly. I find it a very concise tool for getting the point across to management. So many organizations want to put their head in the sand about security, and this blog shows them that breaches are in fact common, that companies do report breaches, even "minor" ones, and that it is not usually the end of the world when a company does report an incident.

Chris Close, IT operations manager, Western Dental Services

In response to a news item on February 21, Anonymous says power grid concerns are U.S. government spin:

Notably Jane Meyer just won a Polk Award for her exposé in the *New Yorker* on corruption at the NSA. These lies are par for the course for an organization that is more about depriving you of your tax money and privacy than protecting Americans. We have our own Republican Guard.

Jeff

Ha ha, they really are trying hard to stop Anonymous. I work in and design large power systems, and there is no way someone sitting at home on the internet can hack in and shut off the grid – unless they've changed things. The control rooms are manned 24/7, 365!

Any switching operation/maintenance, etc., is controlled by a human, and often planned well in advance. They also have built in fault tolorance. It would take a physical strike to take these massive machines down. However, a bad judgment from a controller could bring down some grids. Best way to take something down...strike at the source.

"Unsigned"

In response to a Feb. 9 news story, Standards body to certify PCI end-user experts:

PCI DSS compliance is a sham. Just because you are PCI compliant (checkbox please!), it doesn't mean you are secure. Unfortunately, commercial businesses out there are held to this "standard" by PCI.

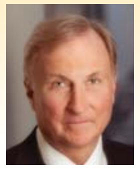
securitycrush

In response to a March Opinion piece on the website, Never off duty when malware infects the weekend, by Ross Kinder, senior security researcher, Dell SecureWorks:

I have had countless system on my kitchen table with the same problems. One trick that always seems to work: Create a new user and do all of your work from there. And last but not least, boot into the infected user and make sure the profile is clean. All in all, it's a solid four hours of fun.

Pmarsh

The opinions expressed in these letters are not necessarily those of SC Magazine.



Preston Wood, the chief security officer at Zions Bancorporation

THE BIG PICTURE

Tools are now available that can sort through massive amounts of "Big Data," so security pros can better connect the dots, says Preston Wood, CSO of Zions Bancorporation. Dan Kaplan investigates.

Consumer behavior often is influenced by slick marketing tactics, like jingles that may make you want to pull your hair out. Case in point: If you've recently walked into a Subway to order a sandwich – and haven't thought about five dollars and footlongs – you probably don't own a television.

Well, the latest craze in information security doesn't have an indelible tune to go along with it – at least not yet – but it does have a memorable, sexy-sounding name: "Big Data." And as a result, everyone is talking about how organizations are aggregating, searching and analyzing voluminous information sets to make intelligent business decisions that may have been impossible to reach in the past.

"It's a great phrase that has captured the imagination," says Andrew Jaquith, chief technology officer of Perimeter E-Security, a managed security services provider based in Connecticut.

But for Preston Wood, the chief security officer at Zions Bancorporation, the parent company of some 550 bank branches in the western United States, the concept of Big Data isn't anything new, only that there is a buzzword now to describe what Zions has been doing for more than a decade. In the late 1990s, the corporation began recognizing the enormous business value that could be generated from aggregating disparate data sets and drawing connections to glean actionable insight.

The company was an early adopter of security information and event management (SIEM) technology to make sense of its data sources. Some consider Big Data to be the next generation of SIEM.

"We had a Big Data strategy before Big Data was Big Data," Wood, 40, recalls. "We thought, 'How great would it be to take a lot of this unstructured data we have – that we are retaining for various reasons – and put it into a form factor to be able to analyze and mine that data to make better security decisions?' You'd be able to start some fascinating analytics. You'd be able to ask questions of that data that you weren't able to do in the past."

If Zions thought it was dealing with large amounts of data that needed processing at the end of the 20th century, imagine what the number is like now. Data is growing at astonishing rates across all industries. According to IDC, the amount of information created and replicated in 2011 exceeded 1.8 zettabytes – yes, zettabytes – a nine-factor increase in just five years.

Each day, the world creates 2.5 quintillion bytes of data, according to IBM, meaning some 90 percent of the information alive today was only born within the last two years. Each sector in the U.S. economy is responsible for at least 200 terabytes of stored data, says a report from the McKinsey Global Institute.

Photo by Bob Adler

This breathtaking amount of data being created, managed and stored – both structured and unstructured – is reality, and many organizations are racing to dissect it. The vendor community also is charging full speed at the new opportunity. According to Thomson Reuters data, venture capital firms poured $2.47 billion last year into Big Data technologies.

Perhaps no two verticals deal with security and Big Data more than the information-intensive industries of financial services and health care, says Sean Martin, founder of Imsmartin Consulting, who formerly held marketing roles at several security firms.

For instance, a recent panel at the O'Reilly Strata Conference examined how Big Data may help financial organizations proactively spot the next crisis. In addition, if new regulations are introduced as a result of prior events, data analysis may yield some fresh ideas of how to cope with them.

When it comes to health care, meanwhile, some, such as Craig Mundie, Microsoft's chief research and strategy officer, believe Big Data can help reign in soaring costs related to patient treatment, Martin says. When data is shared openly – assuming HIPAA requirements are met – providers can better identify areas that are causing higher-than-desired costs, Mundie reportedly told attendees last fall at the Techonomy 2011 conference. It makes sense that models like this will be explored, Martin says, considering that a Centers for Medicare and Medicaid Services report predicts that health care costs will rise from $2.6 trillion to 4.6 trillion during this decade.

Making sense of it all

To understand how Big Data came to be, it might be wise to examine the evolution of Google's flagship product, its search engine. Some may credit the web giant's meteoric rise to dominance with its intuitiveness and clean interface, but what really made Google special was the superiority of its search algorithm to produce speed and relevance. Remember the early versions of AltaVista? Or Excite? They paled in comparison.

"It's so damn fast and it's so insightful that you take it for granted," Jaquith says of Google. That had everything to do with Big Data, he says. Google developed a new way to do search by relying on non-relational databases and its home-grown MapReduce framework, which permitted the company to process queries against a massive number of distributed nodes. So instead of using conventional relational databases, Google was able to better scale and, in turn, instantaneously produce pertinent results.

"Big Data is just like the natural evolution of the fact that networks have gotten faster, bigger and servers can hold more things," says John Kindervag, principal analyst at Forrester Research. "You just naturally want to put everything in it. If you have a big closet, by nature, you throw all your crap in the closet and sort through it when you want to…Once you have data, you can rule the world. Ask [Facebook founder] Mark Zuckerberg."

Zions, in a way, is a microcosm of a Google or Facebook. Wood says that at the 30th largest bank in the United States, which counts nearly 11,000 people as employees and $50 billion in assets, applying a Big Data approach within his department is critical because security data "is different than the traditional data warehousing space."

He says security assets are mostly unstructured and include things like firewall/anti-virus logs, packet captures, web log activity across internet banking and treasury management platforms, and login behavior on internal systems. But aggregating and analyzing that type of information wouldn't fly in Zions' traditional database management systems.

After it outgrew the SIEM technology, Wood says Zions needed to develop a more robust way to process data from its 130 different sources if it were ever going to draw any real, timely value. "Say you wanted to run a query across more than 30 days of data, you may be waiting hours for that to come back," he says.

That meant, in 2005, building something called "multi-parallel computer processes," which enabled the bank to leverage clusters of computers to aggregate and mine data. This enabled Zions to shed its reliance on security tools and start building its own internal models that could do the job as good – if not better – than paying huge sums of money to a technology provider.

A GLUT OF DATA: The big dance

Not only are people and organizations producing more information than ever before, but there are new ways to store and share it all, making the job of data security professionals more complex than ever. Check out these Big Data tidbits, courtesy of a May 2011 McKinsey Global Institute study.

30,000,000,000
pieces of content shared each month on Facebook

40%
expected annual growth in global data generated.

1,500,000
"more data-savvy managers" needed to handle Big Data.

BIG DATA: The three Vs

Volume – Big Data comes in one size: large. Enterprises are awash with data, easily amassing terabytes and even petabytes of information.

Velocity – Oftentime, sensitive Big Data must be used as it is streaming in to the enterprise in order to maximize its value to the business.

Variety – Big Data extends beyond structured data, including unstructured data of all varieties: text, audio, video, click streams, log files and more.

Source: IBM

Rather than continue looking for that latest security appliance to plug into his environment, he asked himself, "How can I leverage the data I already have to make a better business decision?"

William Ronca, executive VP of sales at Red Lambda, a security intelligence company based in Florida, agrees. He says many organizations deploy solution after solution, but none of them collaborate in any meaningful way.

One of those models Zions built out of the data it analyzed was to fight spear phishing abuse, in which certain people within a business, often executives, receive legitimate-looking emails that typically seek to install malware on their machine. It's a well-known social engineering ploy that has led to some high-profile breaches in recent years, including one last year at security firm RSA.

"You've got an organization getting millions of emails a day," Wood says. "An attacker targets a handful of people and sends five emails in. How do you detect and respond before your employee clicks on a link they shouldn't?"

"None of these 15 or 17 or 20 tools are integrated together," he says. "They're doing separate jobs in the hope they're securing the environment in some way."

About two years ago, Zions needed even more scale, so it began leveraging an open-source product known as Apache Hadoop, an open-source tool inspired by Google's MapReduce and File System frameworks. The bank contracted with a small vendor that helped it develop a customizable, enterprise-friendly version of the product.

"What Hadoop is is a piece of technology that you can distribute across tens of thousands to hundreds of thousands computers, and it splits all that data and then leverages your cluster for storage and computing power," Wood explains. "Hadoop is our core security data warehouse. It's our core Big Data repository."

Zions is not alone. According to Ventana Research, which last summer polled IT managers, developers and data analysts across hundreds of companies covering multiple verticals, 54 percent are using or considering Hadoop for "large-scale data processing needs." Big Data is also becoming more popular in the cloud – where it is well-suited considering the massive number of distributed machines necessary to generate actionable intelligence. Several major providers, as well as a number of talented start-ups, are offering Hadoop embodiments via the cloud.

Define, dissect and defend

So, as business leaders turn to Big Data to spawn what they hope will be lucrative business ideas, while in the process improving efficiency and agility, someone has to protect these data stores, which, analysts say, provide an attractive target for hackers – and potentially a single point of failure for organizations.

"As security professionals, we need to realize we're eventually going to be asked to be the security custodians of this data," Forrester's Kindervag says.

According to a June 2011 report from IDC, titled "Extracting Value from Chaos," the market analyst firm concluded that less than a third of all information in the "digital universe" contains at least "minimal" protection, while only half of all information that should be safeguarded actually is.

That might be a bitter pill to swallow for security professionals, who are well-versed in the sophistication and intentions of today's cyber criminals, particularly well-funded nation-state adversaries who use low-and-slow techniques, known as advanced persistent threats (APT), to target coveted intellectual property, and then slowly and stealthily siphon out the booty without anyone noticing.

"If I'm a hacker of Anonymous, or part of an APT group, I'm really excited about the Big Data concept," Kindervag says. "This is like Christmas to me. I don't have to steal something from each individual store. I can steal the presents under the tree."

Implementing proper access controls is important to safeguarding Big Data, he says. But encryption may be the real saving grace because it renders data unreadable. "It's the only thing that's going to protect us against these nation-state attacks," he says. "We're never going to keep ahead of those guys."

But before deploying that sometimes difficult-to-manage technology, organizations must first define their data by discovering and classifying it. In other words, they need to decipher which are their most "toxic" assets. Then, they can dissect them.

"That's the exciting stage," he says. "My fear is they won't do stage one and they'll do stage two, and people will steal stuff and they won't know it because the data hasn't been classified, and people don't know how valuable it is."

That's not a problem at Zions, Wood says, where the security team has become the corporation's champion of Big Data.

"We treat this environment as any environment within our organization," he says. "Whatever security policies and controls you have, your Big Data repository needs to be looked at in the same light. Every technology has got things that need to be considered about how you secure it. It's like any new process or application." ■

PLUGGING IN PRIVACY

Ontario's privacy commissioner is ensuring that electricity firms protect data as they roll out smart grid technology, reports Danny Bradbury.

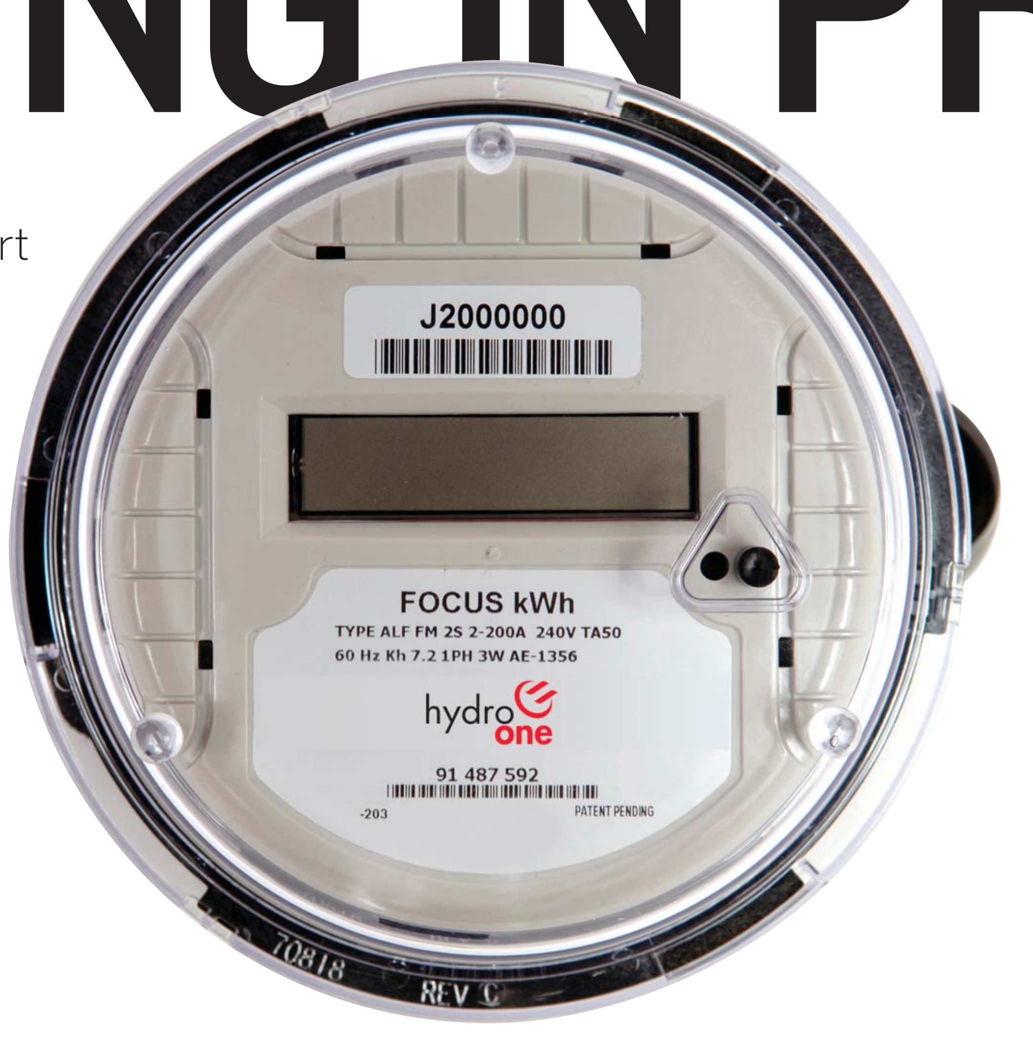


Photo courtesy of Hydro One

Canada underspent the United States by a third in upgrading its electrical systems to smart grids last year, according to analyst firm Verdantix. But, while it may be spending less overall, it is investing more in customer privacy, thanks to Ann Cavoukian, privacy commissioner for Ontario. She wants to make sure that her province leads the field on safeguarding electrical firms' customer data.

Cavoukian has advocated her "Privacy by Design" strategy since the 1990s, which advocates that privacy be baked into products and services from the beginning, rather than adding it after the fact. Utilities must play ball too, she says, as they revitalise their power grids.

Smart grids are designed to bring intelligence to electrical distribution systems. These start in the home with smart meters. Not only do the devices monitor energy use in the household more effectively and communicate it more frequently, but they can also potentially take instructions, i.e., signalling an appliance what to do.

"The home is the last bastion of privacy," Cavoukian says. "This potentially could alter that."

She has already worked with Canadian utilities, advising Hydro One in Ontario, for example, over the privacy implications of its grid rollout. Now, she is exporting her brand of privacy planning south of the border, having signed an agreement with SDG&E, a subsidiary of Fortune 500 firm Sempra Energy, to help it build privacy in from the electrons upwards.

"Our experience is that in the United States, most utilities don't understand this equation," she says. Asked to speak at an energy conference in California, she found that privacy was "an outlier".

Most organizations were more interested in monetizing the customer data dutifully delivered by smart meters. SDG&E swam against that tide, which is why she hopes that it might set an example for the rest of the privacy-averse U.S. market.

Up in Canada, companies are more restricted in how they use customer data. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) allows companies to play fast and free with individual data, but the law does not apply to utilities. Instead, they are governed at a provincial and municipal level.

In Toronto, the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and its sister equivalent, the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), stop utilities from doing anything with data not directly related to its commercial relationship with the customer.

Other Canadian provinces also take a hard line on privacy with utilities, maintaining their own versions of *PIPEDA* and provincial equivalents to *FIPA*.

This is how it should be, says Jeff Meyers, an executive at smart grid solutions vendor Telvent, which worked on the Hydro One system with Cavoukian.

"The correct position for this issue is to state clearly that your personally identifiable information (PII) will be used only to better your commercial relationship with the utility," he says. "You have every right to trust that this data won't be shared with anyone else who doesn't serve that particular purpose."

The Hydro One project uses a concept of domains to help cordon off access to that PII. It divided the grid into three areas: grid, services and customer. The customer grid includes everything on the home-area network, including the smart meter, home energy gateway and smart appliances.

The services domain is where the customer service data is held and processed for the delivery of utility services and programs to customers. It is here that billing, power network planning, demand management and customer communications are handled.

The customer and services domains are where privacy could be breached if things are handled carelessly. However, Cavoukian's Privacy by Design principles hardwired into the service domain are undeniably well thought out, experts say. And, devices in the customer domain can only be accessed from the services domain via authenticated routes and access is recorded. The customer must authorize such access, and Hydro One built role-based security into the system so that personnel can be given access based on their responsibilities.

At the grid management level, there is little worry about privacy breaches because, with a few exceptions, data is aggregated and anonymized by then.

"A big part of managing the distribution system appropriately has to do with knowing just where energy and demand are being created in the grid," says Meyers. "I don't need to know it's Danny's house. I just need to know the location on the grid," he says. Some residential customers that co-generate their energy will be exceptions to this rule.

The Privacy by Design approach seems relatively watertight and is complemented by provincial laws. But perhaps the biggest potential for privacy breaches in smart grids may not come from an overaggressive utility, but from security flaws. Some smart meters have been shown to have basic vulnerabilities that could lead them to be compromised.

Mike Davis, a security researcher at U.S. firm IOActive, has presented extensively on smart grid security and has written self-replicating code designed to compromise smart meters.

"There are security issues that are going on in these meters," he says. "It's like any other internet service. Things are vulnerable."

Data collected from smart meters does carry potential privacy implications because it can provide insights into how energy spikes in the home. Meters generally collect information approximately every 15 minutes. It could be relatively easy, then, to analyse this data and find out when someone was home or not, based on their electrical usage data.

How could that get into the wrong hands? One potential area of leakage is third-party service providers. "Services such as Google PowerMeter, that's where the dangers come in," says Davis.

Designed to be used in conjunction with smart meters, PowerMeter was marketed to utilities around the world as a way to provide customers with information on power use, which could be leveraged to help them make better decisions on proper consumption.

Google retired its service in October, but alternatives include Microsoft's Hohm, PlotWatt, myEragy, PeoplePower and MyEner$ave. Could such services leak data about users that could then be used to assemble profiles on them?

"They could learn so much more about you from all other publicly available sources than from that metering information," Davis says.

As smart meters roll out across Canada, the complaints continue. For example, opponents say their bills have increased 1,000 percent since meters were installed. Thus, for Canada's utilities, privacy may be the first of many new issues. ■

SC CONGRESS CANADA

May 8-9, 2012 | Metro Convention Centre, Toronto | sccongresscanada.com

#SCCan

The faces of data thievery: We can help you defend your enterprise from them.

Platinum Sponsors Check Point SOFTWARE TECHNOLOGIES LTD CONEXSYS COMMUNICATIONS LIMITED hp IBM KASPERSKY lab RSA SOPHOS

Gold Sponsors SentryMetrics Trustwave Security begins with Trust tripwire WHITEHAT websense ESSENTIAL INFORMATION PROTECTION

Welcome

Arming yourself for battle

Now in its third year, SC Congress Canada has become the must-attend information security event. This is where attendees gain expert guidance and timely industry information to help your companies effectively combat today's cyber criminals. Given huge jumps in the numbers of cyber attacks, such assistance should go a long way in helping organizations like yours to strengthen your risk management position and tighten up needed security controls.

With yet another all-star lineup of thought-leading professionals, the two-day SC Congress Canada promises to deliver practical insight about the latest methods of attack that you as security professionals can immediately put to use upon return to your offices. Luminaries speaking at the event will share the latest news on cyber crime and data theft incidents, cyber espionage and APTs, hacktivist attacks, vulnerabilities associated with business-enabling technologies, compliance mandates and more. Offered across three tracks, expert-led talks run the gamut.

The likes of Larry Clinton, president of the Internet Security Alliance, and Mary Chaput, CFO of Clearwater Compliance, will discuss in detail the economics of cyber security and how gaining C-level support of and involvement for IT security programs is critical. During yet another lead session, experts from the Royal Canadian Mounted Police, The World Bank and other leading organizations will share a more comprehensive view of what the bad guys are up to and the best practices you can enlist to thwart their efforts.

In addition to these sessions, an expo hall will be packed with leading vendors and service providers to help you make sense of the evolving threat landscape and the various security technologies that can support your efforts.

As well, we'll announce the winners of our third SC Awards Canada, which honors the achievements of IT security pros and companies in Canada.

If you're looking to bolster your security and risk management plans to battle today's more sophisticated cyber criminals, implement security controls that are both resilient to attacks and support regulatory compliance efforts, and address the security risks associated with the newest technologies forming the basis of your corporate infrastructures – from mobile devices to cloud services – you don't want to miss SC Congress Canada.

We look forward to seeing you there!

Illena Armstrong
VP, editorial director,
SC Magazine Canada

Speakers

Colin Adams,
Equifax

Andrea Bilobrk,
Allstream

KEYNOTE:
Dave Black, *RCMP*

KEYNOTE:
Mary Chaput,
Clearwater Compliance

KEYNOTE:
Larry Clinton, Internet Security Alliance (ISA)

KEYNOTE:
Mark Fabro,
Lofty Perch

KEYNOTE:
Robert Falzon,
Check Point Canada

Craig Gibson,
European Union Project MASSIF

Gilles Fourchet,
Ministry of Community and Social Services

Faiza Kacem,
National Bank of Canada

Robert Parham,
Marlabs

Larry Ponemon,
Ponemon Institute

KEYNOTE:
Winn Schwartau,
Mobile Active Defense

Bob Steadman,
The Herjavec Group

KEYNOTE:
Ken Taylor,
CGI

Dennis Tracz,
University of Calgary

Fiaaz Walji,
Websense

Michelle Warren,
MW Research & Consulting (MWRC)

Rick Yuen,
Direct Energy

Sam Zurzolo,
Toronto Hydro

Also speaking:
Daniel Chervenka, *Husky Energy;* **Robert Knoblauch,** *Scotiabank;* **Iain Paterson,** *Trillium Health Centre & Credit Valley Hospital;* **Sandra Sargent,** *The World Bank;* **David Schwartzberg,** *Sophos;* **Ken Taylor,** *CGI;* **Leo Thrush,** *Seccuris*

SC CONGRESS CANADA

May 8-9, 2012
Metro Convention Centre, Toronto, ON Canada
www.sccongresscanada.com

May 8th agenda

#SCCan

	Track 1 – Emerging threats/management Sessions in this track focus on the latest emerging threats faced by organizations and the best practices implemented to thwart them. This is of value to information security personnel at all levels who need to know more about what the bad guys are up to in order to protect critical data.	Track 2 – Technical This track offers a deeper dive for the more technical security and IT pros at the conference. Emphasis will be on technical aspects of threats and vulnerabilities, along with relevant solutions and processes to address these. Sessions complement those offered in the two other, more executive-focused tracks.	Track 3 – Editor's choice Given the constant change in the threat environment, every security line of business needs to be flexible. This track focuses on timely issues as seen through the eyes of Illena Armstrong, *SC Magazine*'s VP, editorial director. This is for all those wanting to stay on top of the latest security issues.
8:15 a.m.	Breakfast served in registration area		
9:00 a.m. – 9:50 a.m.	KEYNOTE: **The economics of cyber security –** Corporate executives are finally getting more involved in security in a number of organizations. But why has it taken so long and, more importantly, why is this so critical for success? How can practitioners help move this trend along?		
9:55 a.m. – 10:40 a.m.	**Mobile malware –** Where is the real threat? And what are some best practices to thwart mobile attacks?	**Technical view of defense in depth:** Many industry pundits consider the rash of hacktivist attacks in 2011 as a major distraction from focusing on more immediate cyber threats.	**Who's line is it, anyway? –** When it comes to the integrity of code – the heart of application security – whose responsibility is it in the end?
10:40 a.m. – 10:55 a.m.	Coffee break in registration area		
10:55 a.m. – 11:40 a.m.	**Effectively using security intelligence to detect threats and exceed compliance mandates –** Join this session to understand how to provide comprehensive network intelligence.	**Social engineering revisited –** How can your organization help mitigate this risk, and implement security awareness and training programs that actually resonate?	**The Social Network –** Social networking keeps up productivity but you need to somehow protect the enterprise.
11:45 a.m. – 12:30 p.m.	**The 2012 cyber security risk report –** Discussed will be results from the 2012 HP Cyber Security Risks Report, as well as input garnered from the Open Source Vulnerability Database.	**Technical look at compliance by the book –** How can we practice great security so we don't have to then jump through hoops when the auditor walks through the door?	**Latest Threats –** Pros weigh in on what they perceive to be the greatest group of threats facing organizations at the time of the Congress - noting such threats change weekly.
12:30 p.m. – 12:45 p.m.	Lunch in registration area		
12:45 p.m. – 1:30 p.m.	KEYNOTE: **What keeps me awake at night (un-PC views on our future) –** Winn Schwartau looks back on 30 years of security history, successes and failures, then tells us what really bothers him. In his customary hard-edged, honest style, he says the politically incorrect things that many of us think but rarely say. He's going to talk about lawyers, complexification, 4G-war, the real future of mobile computing, poor defenses of networks, our inability to properly respond to cyber attacks and m profiling... just to start.		
1:30 p.m. – 3:15 p.m.	Exhibit floor: Opening day cocktail party		
3:15 p.m. – 4:00 p.m.	**Privacy –** How are organizations marrying privacy expectations with their business' security practices, and how do they see customer demands in this area evolving?	**What's a computer virus? –** How does the enterprise achieve strong situational awareness and, more importantly, how do you then use that information?	**The international framework of cyber security –** Comparative research into the policy approaches to cyber security worldwide, recently released by Ryerson University.
4:05 p.m. – 4:55 p.m.	KEYNOTE: **Cyber crime in Canada –** This panel of government and law enforcement insiders will provide a deep view into the strategies that white hats are adopting to combat attacks. They will also discuss the steps and best practices you can enlist when working with law enforcement and the government to thwart today's cyberattackers.		
4:55 p.m. – 6:15 p.m.	Exhibit floor: Opening day cocktail party		
6:15 p.m. – 8:00 p.m.	**SC Canada Awards 2012 Reception/Awards Ceremony**		

SC CONGRESS CANADA

May 8-9, 2012
Metro Convention Centre, Toronto, ON Canada
www.sccongresscanada.com

May 9th agenda

#SCCan

	Track 1 – Emerging threats/management Sessions in this track focus on the latest emerging threats faced by organizations and the best practices implemented to thwart them. This is of value to information security personnel at all levels who need to know more about what the bad guys are up to in order to protect critical data.	**Track 2 – Technical** This track offers a deeper dive for the more technical security and IT pros at the conference. Emphasis will be on technical aspects of threats and vulnerabilities, along with relevant solutions and processes to address these. Sessions complement those offered in the two other, more executive-focused tracks.	**Track 3 – Editor's choice** Given the constant change in the threat environment, every security line of business needs to be flexible. This track focuses on timely issues as seen through the eyes of Illena Armstrong, *SC Magazine*'s VP, editorial director. This is for all those wanting to stay on top of the latest security issues.
8:15 a.m.	Breakfast served in registration area		
9:00 a.m. – 9.45 a.m.	**Governance, risk and compliance: A practical implementation story** – IT departments are working to better organize their risk and compliance efforts to meet growing business needs by establishing IT GRC programs.	**Security 2.0: How cloud & virtualization change the rules** This session will illustrate key technology shifts in traditional virtualization.	**What's the real mobile security threat? And, is Canada prepared? -** Hear research from a global study on mobility risks with responses from more than 4,000 global IT security practitioners.
9:50 a.m. – 10:35 a.m.	**Sponsored keynote** IBM's Kris Lovejoy will lead a discussion on the increasing influence of CISOs in being transformational business leaders.		
10:35 a.m. – 11:25a.m.	Exhibition floor opens - coffee served		
11:25 a.m. – 12:10 p.m.	**The trained security professional –** Security pros are constantly moving. How are these changes affecting the industry, and what steps are being taken?	**Key and certificate management: Reducing the risk of data loss and audit failures –** In today's high-risk world, with adaption of technologies like cloud, many organizations have to be prepared to handle risks and threats from many sources.	**Risk management by situational awareness** – Not necessarily just the CISO's job, true risk management must be a practice accepted up and down an organization.
12:10 p.m. – 12:25 p.m.	Lunch in registration area		
12:25p.m. – 1:10 p.m.	**Sponsored lunch keynote** TBA		
1:15 p.m. – 2:00 p.m.	**An APT presentation: Fighting the retro war of the future –** We will examine advanced persistent threats and countermeasures available to combat these ongoing threats.	**Cloud storage's hazy security lining –** It is crucial for companies to formulate strategies to keep personal and confidential corporate information secure.	TBA
2:00 p.m. – 3:35 p.m.	Exhibition floor break – coffee served (Exhibition closes at 3:35 p.m.)		
3:35 p.m. – 4:20 p.m.	**Business-driven security programs: Proactively communicating value to the corner office –** This presentation will outline the methods and processes used to develop an enterprise-wide security roadmap.	TBA	**Defending and securing Canada's critical infrastructures** - The controls for SCADA systems for the power industry have been violated, thus the need is to defend while we secure.
4:20 p.m. – 4:35 p.m.	Coffee break served outside breakout sessions		
4:35 p.m. – 6:00 p.m.	**Keynote:** TBA		
6:00 p.m.	Closing remarks and conference close		

Information

Pricing

Conference registration options (Canadian dollars plus 13% HST)	**Early bird rate** (ends April 7)	**Regular rate** (begins April 8)
Two-day Pass (Includes access to eight breakout sessions, keynotes, expo hall, opening reception, SC Awards Canada, plus meals and breaks each day of the event)	$795	$1,115
One-day Pass (One day of SC Congress Canada sessions, plus meals and breaks on the chosen day)	$475	$615
Exhibits Plus (Includes access to one session of your choice, keynotes and the expo hall; does not include meals and breaks)	$65	$75
SC Awards Canada Reception (Includes presentation of the 2012 SC Awards Canada winners. Food & drink provided.)	$55	$55
Expo Hall Only Pass (Includes access to keynotes and the expo hall; does not include meals and breaks)	FREE	FREE ($30 onsite)

Hotel reservations

InterContinental Toronto Centre
225 Front Street West, Toronto ON M5V 2X3

Reservations
Guest room rate: $209/CAD for single or double accommodations, plus applicable HST

Reserve your room
Call 1 (800) 235-4670 for reservations and mention SC Congress Canada 2012.

2012 SC Awards Canada

The mission of 2012 SC Awards Canada is to honor the achievements of companies and IT security professionals striving to safeguard businesses, their customers and critical data in Canada. Nominations for the 2012 SC Awards Canada are made up of IT security products and services available for sale to Canadian companies, as well as provide both customer service and support to users in Canada. Some of the categories include: Security Company of the Year • Best Enterprise Security Solution • Best Regulatory Compliance Solution • Best Mobile/Portable Device Security • Best Managed Security Service • Best Fraud Prevention Solution • Best Security Information/Event Management (SIEM) Appliance

Mark Fabro, president & chief security scientist at Lofty Perch, receives the 2011 CSO of the Year award from Illena Armstrong, SC Magazine*'s VP, editorial director.*

SC Congress Canada Innovation Theatre

Stop by the Innovation Theatre to hear from some of the top companies in the IT security space as they present their latest products and services. These 30-minute presentations will be featured on both days and are open to all attendees.

Contact

Exhibitor inquiries:
Mike Alessie
mike.alessie@haymarketmedia.com

Marketing inquiries:
Sherry Oommen
sherry.oommen@haymarketmedia.com

Program inquiries:
Eric Green
eric.green@haymarketmedia.com

Awards inquiries:
Anthony Curry
anthony.curry@haymarketmedia.com

TIGHTENING THE FED'S BELT

For government security professionals, focusing on priorities is key in these trying economic times, reports Illena Armstrong.

Sponsored by
HP ENTERPRISE SECURITY

Rising incidents of hacktivism, cyber espionage and other online attacks have most organizations reframing their risk management plans to include more than a few tweaks.

However, many information security executives are finding that implementing desired policies and supporting technologies to forge needed enhancements is proving tricky during a time of constrained budgets and resources.

Federal government leaders especially are having difficulties as dollars dedicated to their initiatives either remain the same or continue to drop – even as the adoption of business-enabling technologies, such as cloud and mobile, spikes, according to IT security leaders attending a recent SC Magazine Government Security Roundtable in Washington, D.C.

"It is how [we] cover and continue the mission that makes the difference," said one attendee from a large research-driven agency who asked for anonymity. "[We] can't control everything. We just don't have the resources."

He and others at the roundtable said getting monetary and other support needed to fully safeguard critical data, related informational flows and overall IT environments remains a huge stumbling block. Adding to this are worries about government agencies' use of public-facing applications to exchange various bits of critical information with constituents.

Participants said it is tough enough getting needed budgets, much less convincing staff and government leaders to adhere to some additional controls despite their increasing reliance on cloud services, mobile devices and other technologies. Finding ways to circumvent rules, or simply submitting requests to go around them, has become a frequent practice in many government agencies, some said during the gathering.

For instance, IT security pros may find themselves confronting a high-level individual in their organization who does not wish to follow policies. And, even with technologies in place that may help to enforce these, individuals will request and circumvent the rules. "He knows he's the subject matter expert, and no one's going to challenge him," said the aforementioned IT security pro at the roundtable, sponsored by HP Enterprise Security.

In addition, desired redundancy in IT staff and systems is often given short shrift, he said. Having dedicated roles and backup staffers when others go on vacation or are otherwise unavailable are good practices, but higher-ups often are unwilling to fund these.

"Until we find a way to address these challenges, I don't know how we can effectively address [associated security problems]," he said.

Whether some relief is in sight for federal cyber security practitioners is unclear and certain to remain so until after this year's presidential election. President Obama's budget proposal for 2013 does serve as a kick-off for negotiations with Congress. Already, however, talks are proving contentious.

Still, Obama's wish list of spending priorities seems to favor IT pros, with $78.8 billion on overall IT operations proposed. Of that, millions are earmarked for sundry cyber security operations and research initiatives.

Robert Elder, a research faculty member at George Mason University in Virginia and formerly an Air Force lieutenant general, participated in the SC Magazine Government Roundtable.

Photo by Aaron Clamage

Possible reinvigoration of IT security funding and support couldn't come soon enough. For the first time ever, hacking, as opposed to lost or stolen mobile devices, is the top reason for data breaches, according to the year-end "Data Breach Intelligence" report from Risk Based Security, an affiliate of the Open Security Foundation. Its findings revealed that hacking resulted in the exposure of 83 percent of the 368 million total records compromised last year.

But, trying to cover every possible entry point or be ready for every kind of attack is folly, said retired Lt. Gen. Robert Elder of the U.S. Air Force, who is now a member of the faculty at George Mason University in Virginia and was the lead speaker at the event.

"You need to take a look at this end to end," he said. "Because there are so many different attack vectors, perhaps you should do something more like one does in the military. Typically, you don't try to find everything." Instead, security professionals should understand the key areas requiring protection so that the appropriate systems with the most at-risk data are defended properly.

"So, if we start thinking about [the] targets, then that could be helpful," Elder said. "You can't defend the ocean, so what parts can you defend?"

Whether it is a government agency working with citizens online or a bank interacting with customers who rely on its website for processing transactions, organizations must employ the expertise of IT security heads who fully understand the systems they can't afford to have go offline for any length of time. This comes down to a risk equation: balancing the risk of having one's network compromised with the risk of not making any money, said Elder. And this means that if much of an organization's livelihood "is based on the integrity of transactions," then its executives must establish a risk management plan that won't allow for "a single one of those transactions [to] go bad."

As well, given the myriad attacks hitting government entities and private companies alike, organizational leaders should "assume somebody's already inside somewhere," said Prescott Winter, public sector CTO with HP Enterprise Security and former CIO and CTO of the National Security Agency.

"That issue of linking your assets and the state of the assets, I think, is really critical," he said during the roundtable. "That's the basis of your risk management framework and that's an area where, lamentably, many customers are way short of where they need to be. And then you begin to look at the likelihood of who is inside, what they are doing, what the policy is in relation to this risk management framework and what you have to fix first."

This becomes even more critical as agencies and private companies look to the cloud to ensure that their computing power keeps up with the growth of their businesses, or to rectify some of the missteps they have made when establishing their networks.

Elder, who has been involved in judging college and high school cyber security competitions that task contestants with architecting hardened systems from scratch, said such challenges reinforce for him how building security in from the start works. Often in the real world, though, systems are "cobbled together," and require throwing good money after bad to maintain them.

"Most businesses, because they're having to do things incrementally, can't work with the potential of re-architecting a system," he explained at the roundtable. Further, he said, "What you do to complicate the hacker's world also complicates your system administrator's piece."

This is a huge reason why cloud services are proving so attractive to many organizations, including the federal government. Indeed, over the last several months, various federal agency officials have been defending moves to the cloud as they come before congressional leaders, who are requesting assurances that in undertaking such transitions national security risks will not spike. For his part, Elder said that while cloud computing can remedy certain issues, such as system redundancy or scalability, he worries that other unforeseen risks could crop up.

Many federal officials, though, generally have maintained that the problems they face now would be no different in the cloud and, in fact, security could be enhanced.Whatever the environment and despite its unending changes, to keep it and the data on it secured, associated risk management planning must be robust and well-maintained, said HP's Winter.

"I've talked to a number of CSOs and CISOs who say, 'You know, we're just running hither and yon trying to fix everything,'" he said. "And I say, there's a way to fix this. Begin to establish a proper risk management framework with some clear priorities driven by your mission. You are not going to be able to fix everything everywhere with equal priority. That goes then to aligning your assets with the things you're trying to accomplish. How do you run a network, how do you do patch management, how do you do change management, how do you actually look at all the things going on inside. It's discipline. It's training. It's process." ■

THE GLOBAL LANDSCAPE

Managing use of copyrighted material across national borders is forging new partnerships, reports Greg Masters.

As Bob Dylan 2.0 might put it: The times, and the means of distribution, they are a-changin'.

His music and other artists' creations now often are downloaded through illegal peer-to-peer (P2P) networks, various social media and other sites by individuals who want to avoid paying the entertainment companies representing them.

On Jan. 19, MegaUpload, a P2P file-sharing site, became the victim of its own success when New Zealand police, following a request from the FBI, shut down operations with a raid on its headquarters in a rented $30 million mansion near Auckland.

Certainly the parameters of "acceptable use" have altered considerably since Sean Parker and two partners started Napster in 1999 as a P2P service. The service made it easy to distribute music, even though the enterprise was flagrantly flouting legal boundaries. Consumers who were fed up paying $19 for a CD were easily tempted to abandon ethical concerns for the convenience of downloading music for free.

But, this phenomenon was able to exist only because the internet at that time was still in its early stages. If large corporations were aware of the activity, it was still only a blip on their screens, not enough of a threat to instigate action.

Nowadays, however, copyright holders could not ignore the number of users MegaUpload attracted: MarkMonitor, an enterprise brand protection firm, put the figure at more than 21 billion visits per year. The half-billion dollars in revenue corporate big daddies were claiming to lose also proved intolerable.

Just like Napster in its early days, this site, established in 2005, had put up a pretense of legitimacy by agreeing to remove files when infringement complaints came in. This gesture proved insufficient, however. Its dissemination of purloined movies, television shows, music and other digital content clearly skirted copyright laws.

Facebook and YouTube began their existence flirting with copyrighted material, also. But, to reach mainstream acceptance and avoid being sued out of existence, they had to clean up their acts. When Google bought YouTube for $1.65 billion in October 2006, that process entailed deleting copyrighted material from the servers.

Still, the growth of file-sharing sites such as these has increased the stakes for large entertainment companies and other copyright holders, as well as the law enforcement and legal bodies attempting to exert control and enforcement over which laws govern usage across national boundaries. To date, it is difficult for law enforcement to pursue many of the electronic crimes across international boundaries – often due to country-specific laws relating to cyber crime, says Gunter Ollmann, vice president of research at Damballa, an Atlanta-based network security vendor.

"Many countries simply don't have the appropriate laws," he says. "Subsequently, law enforcement must look for other 'related' crimes conducted by the cyber thieves – and use those in their international law enforcement discussions."

For example, at the time of the massive Mariposa botnet, which was primarily employed to steal data and launch denial-of-service attacks, Spain neither had laws governing botnets nor any that made the unauthorized installation of software on someone else's computer a crime, Ollmann says. So, to arrest and prosecute the Mariposa operators there, law enforcement had to make a case around credit card fraud. That is, the criminals were caught making physical copies of the credit card details they leeched from their victims' computers to purchase goods and services in Spain.

To support efforts like these, law enforcement agencies must have 24/7 points of contact and trained personnel to track and trace cyber criminal activities, and conduct the search and seizure of digital evidence, says Jody Westby, CEO of Global Cyber Risk, a Washington, D.C.-based consultancy that helps global businesses manage risks.

As for cross-border cooperation, countries are making strides. Chester Wisniewski, a senior security adviser at Sophos Canada, says many law enforcement agencies regularly collaborate on international cyber crime cases. He points to cases in Russia, Egypt, Estonia and other countries.

"To some degree, criminal law is being passed in a coordinated fashion to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have been forging for years. "The advanced countries have specialized computer investigation units, who are familiar not only with computer forensics and investigation, but their own country's laws as they pertain to computer crimes," says Art Bowker. a member of the High Technology Crime Investigation Association (HTCIA), which provides education and collaboration to its global members.

And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigative resources and capability to go after the thieves, he explains.

Who has provenance?

Today, the principal challenges for any cross-national law enforcement efforts involve both jurisdictional rights and international laws, says Marcus Chung, COO of Malwarebytes, a San Jose, Calif.-based provider of anti-malware solutions. Any cooperating agencies would need to first agree that certain enforceable laws were broken, and then work together to coordinate the actual arrests within their respective jurisdictions.

While a police agency from one country can't enter another to arrest someone, many nations have treaties in place in which suspects will be locally arrested and held for extradition, says Bowker. That is what is occurring in New Zealand now with the MegaUpload case. This kind of law enforcement action just doesn't happen by magic, Bowker adds. Authorities around the globe recognize that contacts need to be developed and maintained and, when the need arises, they reach out to their foreign counterparts.

Concurrently, the recent arrests of LulzSec and Anonymous members clearly has led to revelations that the FBI

GLOBAL PURSUIT: Law enforcement

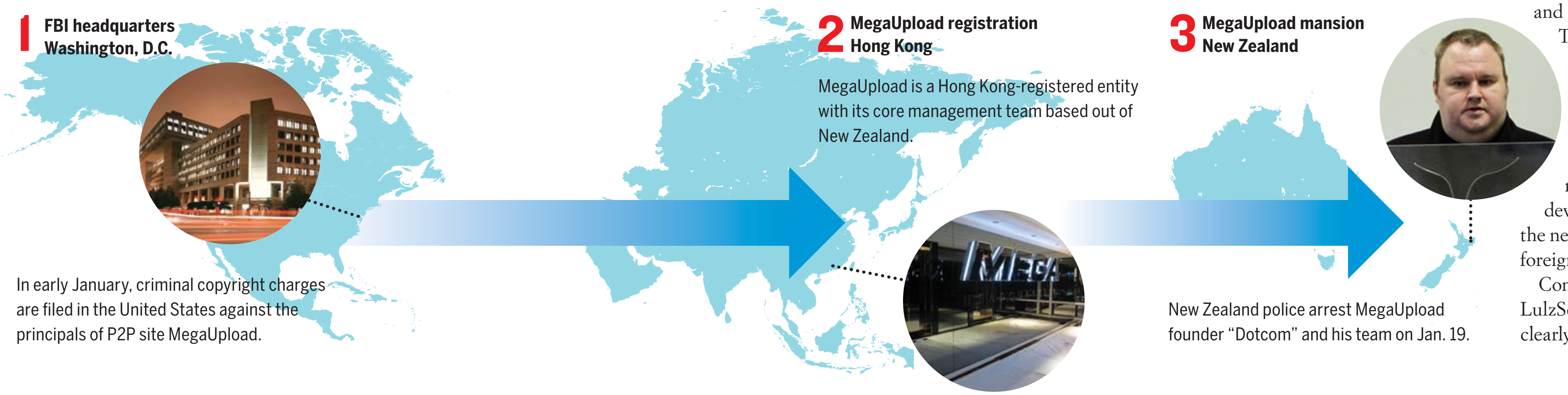

1 FBI headquarters Washington, D.C.
In early January, criminal copyright charges are filed in the United States against the principals of P2P site MegaUpload.
2 MegaUpload registration Hong Kong
MegaUpload is a Hong Kong-registered entity with its core management team based out of New Zealand.
3 MegaUpload mansion New Zealand
New Zealand police arrest MegaUpload founder "Dotcom" and his team on Jan. 19.

Photo courtesy of the FBI, Hong Kong Customs. Kim Dotcom photo by AFP/Stringer was actively notifying governments and companies to potential vulnerabilities it was uncovering during its investigation, he says, recalling one report that 300 public and private entities in the United States and around the globe were notified. In the United States, InfraGard – established by the FBI to work in partnership with the private sector – serves such a purpose. There is also the Secret Service Electronic Crime task forces performing similar functions.

"Law enforcement and the private sector both within and outside of the United States are seeing the value in networking to protect themselves from cyber threats," Bowker says.

Malwarebytes' Chung agrees, pointing out that the recent efforts of the U.S. Department of Justice (DoJ), FBI, Hong Kong authorities, and law enforcement in the Netherlands, Germany, Canada, U.K. and New Zealand highlight what is widely perceived as a successful anti-piracy operation that seized more than $50 million in assets and yielded several high-profile arrests of the leadership behind MegaUpload. The authorities, he says, had to coordinate multiple arrests, freeze financial assets and issue search warrants across eight countries.

If a crime against an American organization occurs overseas, the FBI will escalate it to its liaison who works with the DoJ to make a formal request to the foreign government's federal police, adds Wisniewski. The bar is set high for this to occur, but considering MegaUpload founder Kim Schmitz (aka Dotcom)'s record and the wealth he has accumulated, not to mention the alleged damages caused, he met these conditions, Wisniewski says.

Obstacles to overcome

But, while there are agreements for international cooperation in place, much still needs to be done, particularly within local jurisdictions. Law enforcement around the world is battling the specific laws in their countries, says Ollmann.

"I've not yet encountered a law enforcement officer that feels their own country's laws are specific enough to the electronic crimes they are encountering and being expected to investigate," he says.

Authorities are collaborating well with each other, but have been hamstrung by the disparities among the laws of the various countries in which the cyber criminals are operating, he says. "The internet is international, but the laws most certainly aren't," Ollmann says.

In the meantime, electronic crime conferences geared toward a law enforcement audience have sprung up around the world, and officers are relying on these to both meet with their international counterparts and build new relationships among international teams, he says. Chung says he expects to see this trend of cooperation to increase as the MegaUpload case is widely viewed as a success for both international law enforcement and cross-continental teamwork. "The ongoing blurring of international borders across cyber space requires such coordinated efforts to be successful in prosecuting cyber criminals," he says.

From a legislation perspective, there has been a lot of focus on copyright-related fraud, says Ollmann – e.g., Canada's *Protect IP Act* (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*, or *PIPA*]; the U.K.'s Serious Organized Crime Agency (SOCA); and the Anti-Counterfeiting Trade Agreement (ACTA), a multinational treaty intended to set international standards for intellectual property rights.

GOTCHA: Nab a cyber criminal

In early Jan., criminal copyright charges were filed in the United States by the FBI and Department of Justice against the principals of MegaUpload. The U.S. authorities alleged ill-gotten profits by the P2P site in excess of $175 million and losses by copyright owners of $500 million. As MegaUpload is a Hong Kong entity with the core management team based out of New Zealand, including the founder and CEO, Kim Dotcom, who is currently under house arrest in New Zealand, this required legal cooperation among authorities in three nations, says Marcus Chung, COO of Malwarebytes.

Outside of search warrants and extradition agreements, he says the notable laws that likely will be invoked in this case include *The Digital Millennium Copyright Act*, the *European Union Copyright Directive*, and the *New Zealand Federation Against Copyright Theft*. All of these, as well as user privacy laws, such as the *Electronic Communication Privacy Act*, are likely to be cited both by the prosecution and defense.

Jody Westby, CEO of Global Cyber Risk, says that in addition to substantive cyber crime laws, and the procedural laws that govern how investigations and search and seizure take place, a number of other legal frameworks are likely to be used in court.

Photo courtesy Hong Kong Customs

Hong Kong Customs agents discovered a MegaUpload server in a luxury hotel room.

She expects to see laws on jurisdiction and extradition, which can also include international agreements, such as mutual legal assistance treaties (MLATs), and rules that assist in going through the courts for approval for assistance from one country to another.

– Greg Masters

But, he is not so optimistic about intenational collaboration. The threats legislation is designed to address have been a problem for a couple of decades. Much of the proposed legislation still misses the mark, he says.

"I have little hope for effective legislation to deal with 'today's' complex threats appearing in this decade," says Ollmann. "There is still a tremendous need for education. There is a noticeable generation gap between those responsible for enacting legislation, and those understanding or being affected by the legislation."

As well, while progress has been made, homogenizing all the various national laws is still some time off, Wisniewski says. To illustrate differences in progress, the European Union has harmonized much of its cyber law to facilitate easier extradition and investigation on the continent. Canada, meantime, is currently considering a bill, known as *C30*, that would allow the Royal Canadian Mounted Police easier access to logs of activity from Canadian ISPs, he says. Here in the United States, President Obama has been trying to update the American cyber crime laws, but nothing has passed to date.

Bowker says he expects legislators to come up with something that is more thought out than the cyber crime bills currently under consideration, but not in an election year.

"You can bet that if the recent Anonymous arrests are as successful as they appear, that case will become one key argument for why information needs to be shared," Bowker says.

Mitigation and control

In the MegaUpload case, Dotcom was freed on bail, but had conditions put in place that prohibit him from connecting to the internet, Bowker says. "This is an area more and more community corrections officers are going to have to get up to speed on, learning how to enforce conditions that restrict and/or monitor cyber offenders' computer and internet use."

Mitigating and controlling the activities of cyber criminals across borders is part of the ongoing challenge to coordinate information sharing among various law enforcement agencies, both foreign and domestic, says Chung. There are privacy laws and due process that differ at both the regional and international levels. Due to this level of complexity, at a minimum there are typically local "search warrants," financial information (to facilitate the freezing of assets) and evidence of criminal behavior that is shared among the agencies.

Westby adds that sharing often is facilitated informally through relationships and contacts because the formal process can be cumbersome. Regulations begun under the *Homeland Security Act of 2002* allow the Department of Homeland Security to share critical infrastructure data with foreign governments, she says.

The role of ISACs

One important resource are Information Sharing and Analysis Centers (ISACs). They can play a valuable role in facilitating data exchange within their industry sectors and coordination with government agencies, says Westby.

"Many ISAC members are multinational companies, so this sharing also has a spill-over effect to international locations," Westby says. "They can also help facilitate cooperation among providers."

One must keep in mind, however, that ISACs are not designed for or intended to "hunt and prosecute" cyber criminals, she says. ISACs are primarily useful in sharing information among their members, including approaches and coordination on cyber crime.

But Chung says ISACs are likely to take an increasingly prominent role in coordinating inter-agency efforts and assisting in both the hunting and evidence-gathering stages of prosecuting cyber criminals.

"If you share information about threats, you can develop patterns, which can lead to common players," says Bowker. "The more you communicate, the more you are able to identify the bad actors. You can't arrest them until you identify them."

The key, Bowker says, is to share information that allows members to protect themselves while at the same time can lead to arrests and prosecutions. That is why he advocates law enforcement become and remain active in these groups.

Other information-sharing bodies exist as well. Westby says that IMPACT, the International Multilateral Partnership Against Cyber Threats, is helpful in building a 24/7 point-of-contact database and helping countries coordinate. It now has more than 130 nations signed up and is now the official operating arm of the U.N.'s International Telecommunication Union (ITU) Global Cybersecurity Agenda, she says.

For its part, the United States has failed to show effective leadership in helping to build international cooperation and harmonize cyber crime laws, Westby says, which has contributed to the soaring nature of cyber crime here and abroad.

Wisniewski agrees, adding that "if we want to stop the death of a million cuts that we are all suffering online, we need to ramp up the resources and cooperation and we need to do it quickly. Criminals overseas are acting with impunity, knowing that only the biggest offenders who attract the wrong sort of attention from their governments will ever face prosecution. Law enforcement budgets need to adjust to this new reality, and we need a whole lot more talented internet security experts to be trained to meet the needs of a new era in cyber crime."

In a final analysis, most agree that in a world increasingly tied together by global markets, it only makes sense that everyone comes together to protect each other's cyber assets. ■

THE NEXT COLD WAR

Instead of military assaults, today's adversaries hire coders to create attacks that can run autonomously for years, says Stephen Lawton.

History books tell us that the Cold War ended in roughly 1991 after the dissolution of the Soviet Union. But, today's security practitioners say the Cold War has simply morphed from a threat of armed conflict among major world powers into a battle of computer-savvy "troops" fighting from the comfort of offices.

Instead of countries spending billions of dollars to create new weapons, supply massive armies and spend millions of dollars (or rubles, francs or yuan) fighting conventional attacks against political, economic, religious or commercial foes, today's adversaries hire code-writers to create attacks that can run autonomously for years with little or no human intervention. By repurposing code to spawn new attacks, the cost of cyber warfare can be a fraction of the cost of a conventional war.

While China and Russia generally are considered by industry experts to be the leaders in state-sponsored cyber attacks against the United States, they are not the only countries to have sophisticated espionage infrastructures in place, says Richard Bejtlich, chief security officer at Alexandria, Va.-based Mandiant. Other nations with sophisticated capabilities include North Korea, Iran, France, Israel and, of course, the United States.

North Korea, Bejtlich says, uses technology against its neighbor, South Korea, and to make political statements against the West, generally resulting in attacks against the United States, he says. Iran primarily uses its cyber weaponry to suppress internal dissidents.

In the past, he says, U.S. politicians spoke in general terms about cyber attacks, choosing not to name those believed to be responsible. That all changed late last year when the Office of the National Counter Intelligence Executive released a report, "Foreign Spies Stealing U.S. Economic Secrets in Cyber space," which specifically identified China and Russia as key participants. However, the report also said U.S. allies are actively involved.

"Certain allies and other countries that enjoy broad access to U.S. government agencies and the private sector conduct economic espionage to acquire sensitive U.S. information and technologies," the report states. "Some of these states have advanced cyber capabilities."

It cited four factors that will shape the cyber environment over the next three to five years. These are:

A technological shift, including the use of smartphones, laptops and other internet-connected devices; an economic shift that changes the way corporations, government agencies and other organizations share storage, computing, networking and application resources; a cultural shift in the U.S. workforce, where younger employees mix personal and professional activities; and a geopolitical shift as globalization of the supply chain and worker access increase the ability for malicious individuals to compromise the integrity and security of computing devices.

Jared Carstensen, manager of enterprise risk services at Deloitte in Dublin, Ireland, likes to differentiate between cyber crime and cyber espionage because the end goals differ significantly. For an attack to be considered a cyber crime, he says, the adversary does so for financial gain. This typically includes attacks designed to obtain credit card or bank data. Cyber espionage, on the other hand, is designed to steal intellectual property, and/or disable or attack critical infrastructure. It often is performed for political purposes.

Spying has been around since the dawn of man, Carstensen says. Early tribes snooped on other tribes to learn where they found food. Today's sleuths also are looking for the same competitive advantage over their enemies – and even their allies.

In some countries, such as North Korea, students believed to have a propensity for math or technology are trained at an early age as cyber warriors. These academies provide the students with respectability and good pay. In China, for example, the Communist Party codified cyber warfare in 2010, and President Hu Jintao deemed cyber war a priority. Author and retired U.S. Marine Corps Lt. Col. William Hagestad says in an upcoming book that China bases its policies on the *Art of War,* Sun Tzu's doctrine written around 500 B.C., one of whose tenets is: Keep your friends close, but keep your enemies closer. Chinese officials, however, regularly deny they are involved in any cyber spying efforts.

In the United States, the military is also shifting its war strategy to further prioritize cyber efforts. The soldiers who pilot military drones over Pakistan and Afghanistan actually sit in control rooms at Creech Air Force Base in Nevada. This, Carstensen says, is not unlike cyber attackers who might work out of a hotel to conduct assaults.

Jens Bonnke

However, the level of expertise of foreign cyber attackers varies widely from so-called script-kiddies, who download exploit software that is widely available on the internet, to experienced computer engineers who have either religious or political reasons for staging actions.

Some of these attacks are advanced persistent threats (APTs) that are designed to enter a computer system and perhaps sit dormant for a period of time. The intrusions are designed not to be noticed.

This tactic varies significantly from those of hacktivists, who attack websites with the expressed purpose of drawing attention to the site being breached. Some groups, such as Anonymous and LulzSec, have claimed credit for damage to sites they have compromised.

Unlike hacktivists, cyber spies are so concerned about flying under the radar that once they successfully enter a target system, they actually install security patches to ensure that other attackers are unable to access the system using the same vulnerability, says Daniel Teal, founder and chief technology officer of Austin, Texas-based CoreTrace and a former officer at the Air Force Information Warfare Center (AFIWC). By installing fixes, he says, the attacker will have the compromised systems all to themselves and will not have to worry about a sloppy rival alerting the IT manager that there has been a breach.

Admins might actually see their network performance improve while the attacker ensures that others are unable to infect the environment, Teal says. Because the attacker does not want to draw attention, they simply can leave a back door open so that the malware payload is not accidentally identified by the target network.

Toney Jennings, CEO of CoreTrace, adds that companies might have the equivalent of a "cyber atomic bomb" in the server that "is not doing anything bad today." That bomb could be set off by an intruder at a later date, well after the initial breach took place. Additionally, he says companies purchasing mission-critical hardware should spot check the "guts" of the new systems, including all device drivers, for malicious code before putting them into production.

Most hardware and software today is developed outside U.S controls, so ensuring it is safe is a good business practice. "It's a valid bit of paranoia," Jennings says.

Underscoring this concern, an FBI presentation last year detailed how counterfeit Cisco Systems networking equipment originating in China – including network routers, switches, gigabit interface converters and WAN interface cards – was being sold in the United States. "Operation Cisco Raider" resulted in the recovery of 3,500 pirated network devices valued at $3.5 million, James Finch, assistant director of the FBI's cyber division, has said.

Teal says he once discovered, by accident, a malicious device driver for a keyboard he purchased for his daughter's computer. The driver was sending personal information off his home network. He contacted the system manufacturer, Hewlett-Packard, and discovered that the kernel driver was written by a third party. Further investigations by Teal and HP determined that the manufacturer was sending data off the network simply to ensure an internet connection – a task that easily could have been accomplished by sending random data bits without using personal information.

When Bejtlich was the director of incident response at General Electric, the company had an estimated half-million computers, and no shortage of defensive technologies and staff. Even still, he says, with the full resources of a sophisticated IT team and a corporate leader who recognized the need for IT security, the company still was unable to maintain 100 percent effectiveness against intruders or persistent threats.

And now, mobile and cloud

Mandiant's Bejtlich says that despite the best intentions of CISOs and IT staffs, it is nearly impossible to keep a network of a 1,000 or more endpoints safe from outside attacks.

Today, Bejtlich says, IT staffs need to address not only the needs of a company's primary computer systems, but also non-standard systems, such as smartphones and other mobile devices. While cyber espionage is normally thought of as an attack against a large computer system, many corporate executives and engineers have confidential data on their devices that might be useful to attackers.

Companies that believe they are too small or insignificant to be targeted are wrong, and do not necessarily understand how and why attacks work, says Erin Nealy Cox, managing director and deputy general counsel at Stroz Friedberg LLC and a former federal prosecutor and assistant U.S. attorney. While technology firms are obvious targets for attackers after intellectual property, small companies may be considered stepping stones.

Cox says security education is essential in companies of all sizes. Large organizations with established policies and procedures need to educate their employees on a regular basis not only about sound computing practices, but also about data and office security policies. For example, she says employees need to be reminded not to insert thumb drives they find in the parking lot or those handed to them at a trade show into a company computer. Such devices could be plants with malware on them.

"Typically," she says, "security comes at the price of convenience."

Even data security companies can fall prey to sophisticated attacks, she says. Within the past year, there have been several online raids on companies that specialize in data security. The reasons for the success vary, she says, but it generally falls into the category of an exploit that was allowed because someone was not paying attention to details. It might have been faulty website code or a misconfigured network, but generally the vulnerabilities could have been caught.

Scott Crawford, research director for security and risk management at Enterprise Management Associates, with corporate headquarters in Boulder, Colo., agrees that companies of all sizes could be targets. While smaller entities might not provide the breadth of information that a multinational corporation offers, it still could have secrets worth stealing, he says.

Crawford views this kind of cyber theft, be it from a state-sponsored or industrial source, to be similar to espionage conducted during the Cold War. There could be value in stealing information, he says, but "you don't want to kill the market." One purpose for this type of espionage is to build a country's or company's own ability to compete against existing players in the field.

If it costs $50 million to develop a product, but only $2 million to steal it, some will opt for the less costly approach. This is particularly true for emerging nations that might have technical resources, but are not necessarily competitive enough to develop their own intellectual property.

Defense is all about managing a company's or a country's risk, Crawford says. Some organizations look for fast fixes to potential weaknesses without fully understanding their risk profile or the impact of their actions. A layered approach to security is necessary.

Crawford also blames guidance or regulations that do not match the threat. The Payment Card Industry Data Security Standard (PCI DSS), for example, is prescriptive and specifies to security officers how to maintain compliance, but this is only a point in time, he says. A company's compliance "can be passé or irrelevant" immediately after passing the audit. ■

This article originally appeared as an SC Magazine *ebook. For more information about ebooks from* SC Magazine, *contact Illena Armstrong, vice president, editorial director, at illena.armstrong@haymarketmedia.com.*

Product Section

GFI
Easy-to-use SIEM that can function sans agents **P43**

NetIQ
Tool with the most mature features **P44**

SolarWinds
A SIEM that is full of options **P45**

A mature category attracts some surprising new players

This month, we look at security information and event management (SIEM) tools. What struck me about this category – which I thought was fairly mature – is that there are players this year that I did not expect.

As well, this month marks the debut of a new contributor at the labs: Frank Ohlhorst is a reviewer of long experience in our field, in particular, and computing, in general. He shares the spotlight with SC Lab Manager Mike Stephenson this month and the results, I'm sure you'll agree, are gratifying.

The whole idea behind SIEM has been evolving and morphing for several years now. Personally, I find SIEM to be one of the most important devices on the network. I take that position because a really good SIEM will do two things for you. First, it will allow alerting on complicated events that might otherwise escape notice. Second, it allows detailed analysis into root cause from a forensic perspective.

From the alerting perspective, because the SIEM is taking its input from a variety of sources, it gets different perspectives on the data flowing through the network. An especially important aspect is the ability to correlate net flows with events. This provides a sort of vectoring ability that can help the analyst figure out what devices in the enterprise have been affected by an event.

From the analytic viewpoint, a major analytical challenge is dealing with very large amounts of data. Information security should focus on the data, so even if there are devices involved – which, of course, there are –understanding how the data flows through those devices is the key to understanding how to analyze the event. The SIEM facilitates that understanding because it correlates the large amount of information on the network to pare it down to a manageable size.

Be sure that you define your needs thoroughly. There are a few of these products that excell in log management, for example, so if that is what you need, take a look at them. One of the great advantages of a maturing product group is that there should be available exactly the product for your application. This month's offerings are no exception.

—Peter Stephenson, technology editor

How we test and score the products

Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a predetermined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University.

We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor.

All reviews are vetted for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.

★★★★★ Outstanding. An "A" on the product's report card.

★★★★ Carries out all basic functions very well. A "B" on the product's report card.

★★★ Carries out all basic functions to a satisfactory level. A "C" on the product's report card.

★★ Fails to complete certain basic functions. A "D" on the product's report card.

★ Seriously deficient. An "F" on the product's report card.

SC MAGAZINE BEST BUY   SC MAGAZINE RECOMMENDED   SC MAGAZINE LAB APPROVED

What the recognition means

Best Buy goes to products the SC Lab rates as outstanding.

Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

SIEM

Security information and event management (SIEM) tools do a lot of things, but at the core they take data from sources and get useful, actionable information from it, says Peter Stephenson.

PICK OF THE LITTER

McAfee Enterprise Security Manager (ESM) (formerly NitroView from NitroSecurity) is an old war horse that just gets better and better with age and maturity. We are excited about the new home it has at McAfee. Once again this year, we designate it SC Lab Approved.

LogRhythm is one terrific product and an equally terrific value. We make it our Best Buy.

LogLogic MX is a bit of a dark horse in the SIEM race, coming from a log management legacy. Now, a first-rate SIEM product at a good price, it is our Recommended product.

SC MAGAZINE BEST BUY

SC MAGAZINE RECOMMENDED

SC MAGAZINE LAB APPROVED

The security information and event management (SIEM) segment has always been one of the most interesting groups that we examine. It is particularly interesting because over the years the definition of what we mean by a SIEM has evolved. It came out of two separate product categories: security information management (SIM) and security event management (SEM). At the beginning of the genre there was a distinction made between event and information management. Today, they are combined and have been for some time. While some refer to SIEM as security *incident* and event management, most professionals today agree that SIEM is security *information* and event management. The term was coined by Gartner back in 2005 and it has stuck with us.

This is totally appropriate since information is necessary to interpret events. Certainly it's the *events* that trigger alerts, but it's the *information* that gets the analysis done. So, what should we be looking for in a capable SIEM given that this is an evolving category – even though it's pretty mature at the moment? SIEMs do a lot of things, but at the core of why we need one of these beasts is that they take lots of data from lots of sources and provide useful, actionable information from it.

Let's dig into that a bit. Useful security-related data in a large enterprise comes from a lot of sources. Firewalls generate logs. Intrusion detection systems (IDS) or intrusion prevention systems (IPS) generate logs and alerts. Routers and switches generate net flow data. Computers generate system logs. All of these assets need to be aggregated and correlated in order to be of any use. For a large enterprise, that could mean quite a bit of data. So what does a SIEM give us that helps us analyze and alert?

First, the SIEM must aggregate the incoming data. That means that it must know how to read the different file types that generate data for it. There are a variety of ways that SIEM developers do this, but the bottom line is: If the SIEM at which you are looking cannot decode most types of security data, it is not of much use to you. The other piece of aggregation is the ability to collect all of the data without dropping packets.

Next, the SIEM needs to be able to correlate data that it has collected. This means distilling it into common events and flows. The analysis cannot begin until the correlation is complete.

SIEMs alert as well as analyze, so there must be a good way of determining alerts. Limiting or eliminating false positives, alerting based on weighting, and criticality and correlation with vulnerabilities all are important aspects of the alerting functions of a capable SIEM.

Also, the tools need a good way of displaying the results of their analysis. That usually means a good graphical dashboard, but there also is the need to drill down to original data, particularly the original source. This leads into the need today for compliance reporting.

Finally, SIEMs can process a lot of input. So you need to consider how you are going to archive the massive amount of facts that the sources feeding the SIEM generate daily. There are a couple of sides to this particular requirement. On one hand, you can archive metadata and that will let you perform credible analysis over time to get historical perspectives on threats and vulnerabilities. However, that usually does not let you drill down to the source data. That means that you will not be able to reconstruct sessions, including the data payloads of the source packets.

So, what distinguishes one SIEM from another? The SIEM that you select needs to have the features that you need in your environment. It usually needs to be scalable, and that might mean being able to function in a widely distributed network. SIEMs that do that often have a master device that communicates with subordinate devices.

Don't focus too much on cost. Rather, concentrate on value. For a large-scale SIEM, you might pay a bit more, but you may need its capabilities.

Frank Ohlhorst and Mike Stephenson contributed to this Group Test.

Specifications for SIEM tools

● = yes ○ = no

Product	Performs log collection	Performs event correlation	Allows for forensic analysis of log data	Includes pre-defined alert templates
AlienVault	●	●	●	●
CorreLog	●	●	●	●
EventTracker	●	●	●	●
GFI	●	●	●	●
LogLogic	●	●	●	●
LogRhythm	●	●	●	●
McAfee v9.0	●	●	●	●
NetIQ	●	●	●	●
SolarWinds	●	●	●	●
Tenable Network Security	●	●	●	○
Tripwire Log Center	●	●	●	●
Trustwave SIEM	●	●	●	●

	Includes pre-defined compliance templates	Includes pre-defined report templates	Uses agents for log collection	Agentless log collection
AlienVault	●	●	●	●
CorreLog	●	●	●	●
EventTracker	●	●	●	●
GFI	●	●	○	●
LogLogic	●	●	●	●
LogRhythm	●	●	●	●
McAfee v9.0	●	●	●	●
NetIQ	●	●	●	●
SolarWinds	●	●	●	●
Tenable Network Security	●	●	●	●
Tripwire Log Center	●	●	○	●
Trustwave	●	●	●	●

DETAILS

Vendor	AlienVault
Price	$32,000
Contact	alienvault.com
Features	★★★★★
Ease of use	★★★★
Performance	★★★★½
Documentation	★★★★★
Support	★★★★½
Value for money	★★★½
OVERALL RATING	**★★★★½**

Strengths Highly capable SIEM with a nice feature set.

Weaknesses Overall high cost of ownership.

Verdict A good SIEM with a lot of features, but a serious price tag.

AlienVault Professional Threat Management S3000

Part of the fun of doing these product reviews is that we get to see new products as they emerge into the marketplace. AlienVault's Professional Threat Management S3000 is no exception. This product is a component to the AlienVault Unified Security Management platform, which started out as an open source project and has now grown into a solid security event management tool. The platform contains more than 30 open-source security tools built in and ready to go out of the box. Some of these tools include intrusion detection system (IDS), host-based intrusion detection system (HIDS), Forefront Identity Manager (FIM), wireless intrusion detection systems (WIDS), netflow, asset inventory and vulnerability assessment. Working together, these tools can provide overall security management from posture assessment through finding ways to remediate and improve overall network security throughout the environment.

We found this product to be quite easy to install. The installation has to be done on a bare metal server or virtual machine. To install the product, the installation DVD is inserted into the server and, once booted, the Linux-based installation wizard is launched. The installation can be fully automated, or the user can pick a more customized installation method if needed. We chose to go with the default automated install. The installation of the software took only about 15 minutes, and the server was up and running. All configuration is done using a web GUI. We found this to be easy to navigate and intuitive to use overall, but we did have to navigate around a bit to get comfortable with how the system was organized.

This tool is pretty empty after installation by default, and there is a lot of configuration that has to be done to get everything up and running. We found configuration to be fairly simple with the help of the documentation. One thing we instantly noticed was the amount of customization that we could do with the dashboards.

Documentation was comprised of installation and user guides, plus several other pieces of supplemental material. We found all documentation to be easy to follow, with clear instructions, screen shots and configurations.

AlienVault offers a few support options. Customers can purchase a support pack, which includes a limited number of tickets or support hours. Alternatively, they can purchase assistance as part of an annual contract. This offers both eight-hours-a-day/five-days-a-week and 24/7 options, which include phone- and email-based technical support, contacts and access to a portal. All customers can access a small portion of the portal which includes product documentation and other useful resources, at no cost.

At a price of $32,000 before hardware and support, this product does come with a hefty price tag. We find AlienVault Professional Threat Management to be an average value for the money. While it does sport some nice features, we find the overall cost of ownership to be a little bit high, especially considering that a 24/7 support contract can cost up to $50,000 annually.

LogLogic MX

When we first saw LogLogic a few years ago, it was a strong log management appliance that could do some nifty stuff, but overall was focused on log management. Well, times have certainly changed, and this appliance has grown immensely in functionality over the years. Its latest iteration offers some exciting new features, including a full compliance manager, but more on that later. The LogLogic MX can collect data and logs from network devices, such as routers and firewalls, as well as many other sources, including intrusion detection system (IDS)/intrusion prevention system (IPS), Windows, Unix and load balancers. After logs are gathered, the MX solution indexes, compresses and stores the data for use in forensic analysis and compliance assessments.

SC MAGAZINE RECOMMENDED

Installing the appliance itself takes just a few minutes. Once up and running in the network, all configuration is done via a web-based management console. The tool also comes with the Compliance Suite and Compliance Manager as separate installs. The Compliance Manager can be easily installed on a Windows Server and it provides all the necessary components, including the web-based management interface. After the installations are complete, all that needs to be done is to add the appliance to the Compliance Manager and add sources to the appliance.

After our initial configuration was complete, we began navigating around the management interface and found it to be quite comfortable to move around in. The majority of the interface has not changed much, and we felt right at home managing the appliance. The combination of the MX appliance and the Compliance Suite make managing compliance easy as well. This product comes preloaded with many compliance-based reports and customizable dashboards. Also included are ready-to-go alerts based on several standards, including PCI DSS, *HIPAA, SOX,* COBIT, NERC, FISMA, ISO, ITIL, and the *HITECH Act.*

Documentation came as several PDF guides, including installation and administrator guides for the appliance and quick-start and user guides for the Compliance Manager, along with several supplemental pieces of documentation, including log source configuration guides for a variety of log sources. We found all these to be complete and easy to navigate.

LogLogic offers two levels of support – both available at an annual cost. Customers can purchase gold support, which includes phone and email technical help during business hours, or platinum support, which is 24/7.

Starting at around $35,000, this product may seem quite expensive, but we find it to be a good value for the money. Included in the price is not only the appliance and software, but also the Compliance Manager and Management Suite, which add a lot of compliance auditing/management features and functionality. Ongoing support is also quite affordable, with business-hour support coming in at around $7,000 per year and 24/7 assistance only around $12,000 per year.

DETAILS

Vendor	LogLogic
Price	$35,000
Contact	loglogic.com
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★¼
OVERALL RATING	**★★★★★**

Strengths Easy-to-deploy log management, event correlation and compliance management.

Weaknesses None that we found.

Verdict This one's a bit of a dark horse in the SIEM race, coming from a log management legacy. Now, a first-rate SIEM product at a good price. It is our Recommended product.

LogRhythm

DETAILS

Vendor	LogRhythm
Price	$25,000
Contact	logrhythm.com
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Highly customizable SIEM with many pre-built policies and dashboards backed by a powerful correlation engine.

Weaknesses None that we found.

Verdict One terrific product and an equally terrific value. We make it our Best Buy.

SC MAGAZINE BEST BUY

Back again this year is one of the most powerful SIEMs that we have seen, and it is more powerful than ever with the new version 6. To start, the LogRhythm appliance combines log management, SIEM, file integrity monitoring and host activity monitoring into a single integrated platform. From there, all these functions use the advanced intelligence engine to provide full correlation and pattern recognition to stay on top of security threats throughout the enterprise.

From beginning to end this appliance is easy to deploy and configure. The first thing that needs to be done is to get the appliance up and running. The tool is pretty much ready to go out of the box, but does need some initial configuration. At first boot the appliance will run through a short Windows setup wizard where networking and other settings can be configured. After the appliance is up and running, all management is done via a powerful management console application. Overall, we found the management console to be easy to navigate, as well as intuitive to use. We also liked that the interface can be highly customized to meet the needs of the user and is not a one-size-fits-all layout.

The management interface has a plethora of features and functions. Some of these include fully customizable dashboards – along with predefined dashboards that offer specific information at a glance, many graphs and charts that can be drilled down into all the way to the raw log data if needed, and quick navigation controls for easy movement throughout the interface. Aside from all of the management capability, this product also features many strong compliance functions, including a brand new SmartResponse system. Security administrators can use this to deploy instant and automated remediation of common alerts. The final strength of this product is a solid rule engine. While the appliance comes preloaded with many rules out of the box, creating custom rules for alerts is as easy as dragging and dropping the parts of the rule using the rule builder interface. Finally, in terms of performance and flexibility, the appliance has the ability to collect data and logs. The LogRhythm appliance is able to gather and analyze logs with or without the use of agents, depending on the type of log and needs of the environment.

The LogRhythm documentation set is included in the management console and can be easily accessed if needed. It features installation, configuration and administrator guides. We found all documentation to be well-organized and easy to follow, with many screenshots and step-by-step configurations.

LogRhythm provides both eight-hours-a-day/five-days-a-week and 24/7 support options for customers. Support must be purchased as part of an annual agreement and includes access to phone- and email-based technical help. Customers also can access a large support portal via the website, which includes a full knowledge base and FAQ section, along with other resources.

At a price of around $25,000, this LogRhythm solution is an excellent value for the money. The appliance offers a lot of functionality, along with many easy-to-use features and pre-built dashboards, making it a very powerful SIEM appliance.

McAfee Enterprise Security Manager (ESM)

In the ever-changing marketplace of today's network security products, it is not uncommon to see a company acquire another company with the idea of taking a good product and making it better. We have seen firsthand that sometimes this works and sometimes it doesn't. However, in the case of McAfee, it has found a real winner with this product. The Enterprise Security Manager from McAfee is a new iteration of our old friend, the NitroView from NitroSecurity. When we see acquisitions such as these, it always makes us nervous because we fear that a good product can easily go bad. So far, this is not the case with this one. So what does the Enterprise Security Manager, or ESM, have to offer? A lot if you ask us. This product features a powerful correlation engine that is driven by an ultralight proprietary backend database. The ESM is able to gather, store and analyze logs and data from a large amount of sources and then correlate events based on rules, possible risk or historical trends.

SC MAGAZINE LAB APPROVED

An appliance that has this much power must be difficult to configure, right? Not at all. The initial setup process takes just a few minutes and can be done directly on the LCD screen on front of the appliance. This is where all the network configuration is done, and after the appliance is connected to the network all further management is done via a web GUI. We found this interface to be one of our favorite parts of the appliance. The management interface is loaded with visuals and dashboards that include many charts and graphs that can be drilled down into all the way to raw log data. Dashboards also can be customized to meet the analysis needs of the user by simply adding or removing the various dashboard modules.

This product can take logs from just about anything with an IP address, but what makes it stand out is its Database Activity Monitor and Application Data Monitor. Using these two features, security administrators can easily collect data from database and application logs for deep forensic analysis. The ESM also comes preloaded with more than 200 different predefined compliance report templates, along with a reporting function that enables the creation of custom reports quickly and easily.

Documentation included an installation and a full user guide. We found these materials to be complete and well-organized.

McAfee offers customers 24/7 phone- and email-based technical assistance as part of an annual agreement. Customers also can access a web-based portal via the website, which includes a knowledge base, downloads, support case management and other resources.

At a price just shy of $39,000, this product may seem quite expensive at first. However, we find that its combination of features, paired with the solid correlation engine and backend database, make it an excellent value for the money. The tool can provide security event management and analysis along with forensic capability that is easy to deploy for almost any size environment.

DETAILS

Vendor	McAfee
Price	$38,995
Contact	mcafee.com
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Full SIEM appliance with a powerful correlation engine and ultralight database.

Weaknesses None that we found.

Verdict This old war horse just gets better and better with age and maturity. We are excited about the new home it has at McAfee. Once again this year, we designate it SC Lab Approved.

Trustwave SIEM

The Trustwave SIEM appliance is designed to collect, normalize, analyze and store events and logs from a wide array of network devices and security products. Administrators can then use all of the collected data to do forensic analysis of security events along with compliance management and reporting. The most interesting function of this product is its deployment flexibility. The Trustwave SIEM can be deployed as a standalone appliance that is managed by the organization or it can be deployed as a managed appliance that is monitored by Trustwave to keep everything up to date and functioning properly. If an organization deploys a managed appliance, it also has the option to have Trustwave provide analysis of mission-critical data.

Not much has changed with installation and management of the appliance since we saw it last year. The initial setup is quite straightforward. It is guided by a setup wizard, which can be accessed via a web browser that goes to the IP address of the appliance. At the completion of the initial setup, all further configuration is done using the web-based management interface. Overall, we found this to be intuitive to navigate, but we still had to spend some time navigating around and getting familiar with how to configure log sources and get the appliance collecting logs. We would like the process of adding and managing devices to be a little more intuitive.

We found this appliance to offer a lot in terms of analysis capability. The product comes preloaded with preconfigured collectors for many types of devices, including routers, switches, Windows-based event logs, and some generic log sources. Custom log sources also can be added if needed and, at no charge to the customer, Trustwave will help add support for any commercially available device.

Along with the preconfigured collectors, this appliance features many predefined compliance and policy templates that make overall analysis of events quite simple. Trustwave is also constantly pushing new updates to the appliance, which include updated log parsing definitions, new and updated reports, new charts and correlated alert definitions. This ensures that log and compliance analysis is always up to the latest standards and alerts are always kept up to date.

The Trustwave SIEM comes with a good amount of documentation. We found all of it to be well-organized and easy to follow.

Trustwave offers support to customers through an annual agreement. Customers can purchase 12/7 or 24/7 support, which includes access to phone- and email-based technical support. Also available to customers is an online assistance portal, which includes a knowledge base, FAQ section and many other helpful resources.

At a price of $19,000, we find the Trustwave SIEM to be a reasonable value for the money. The appliance offers a lot in the way of features and analysis capability, as well as ease of management, particularly after the initial configuration is complete.

DETAILS

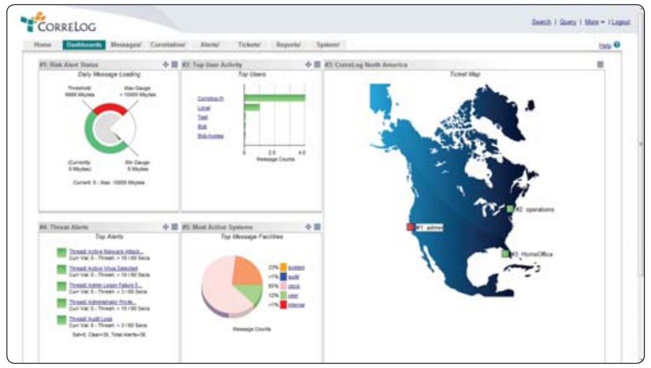
Vendor	Trustwave
Price	$19,000
Contact	trustwave.com
Features	★★★★★
Ease of use	★★★½
Performance	★★★★½
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★½
OVERALL RATING	★★★★½

Strengths Full-featured SIEM with many predefined log sources and compliance reports.

Weaknesses Initial configuration is slightly difficult.

Verdict A much-better-than-average SIEM living up to the Trustwave legacy of first-rate products.

CorreLog Correlation Server v5.1.0



The CorreLog Server is a web-based solution that leverages browser technology to present an easy-to-use, multi-platform interface that stresses point-and-click simplicity for the harried network administrator. Designed from the outset as a product that supports regulatory compliance objectives, as well as security posturing, CorreLog Server is chock full of features and reporting capabilities.

The product can be installed under two distinct scenarios, where it operates as either as a “Small Business Server” or as an “Enterprise Server.” The “Small Business Server” configuration was chosen for testing because it features the capabilities of the Enterprise Server, but without the high-end hardware and processing requirements associated with the Enterprise Server implementation.

That said, the Small Business Server configuration proves to work fine under virtualized environment, using a virtual PC as a host. The product runs on a variety of Windows operating systems, including Vista, XP and Windows 7, as well as various editions of Windows Server. That helps to make the product very flexible to deploy and eliminates the need for proprietary hardware and high-end server components.

CorreLog Server relies on an included version of Apache Server for access via a browser, and browser security is handled via an included copy of Apache SSL Server. Installation was straightforward, requiring only basic networking knowledge, and used a wizard to install and configure the product. There are a few manual steps. However, the PDF-based quick-start guide makes it almost point-and-click easy.

Once installed, the main management console is accessed using Internet Explorer v7 (or equivalent). On initial logon, the administrator will need to set up accounts and passwords. Once again, that proves to be easy, allowing administrators to get the system ready for full deployment rather quickly. CorreLog Server uses a client/server model to gather information.

Installing the client application is by no means complex, but it can take some time on a larger distributed network. One caveat is that the client should be installed on every system that interacts with the network internally and falls under the purview of compliance, security or performance.

Integration and setup aside, the real meat and potatoes of CorreLog Server is the information it can provide to a network manager – which is key when it comes to a security information and event management product. Here, CorreLog Server offers several reporting capabilities and, interestingly, integration into Microsoft Excel, which gives analysts some flexibility when analyzing specific events.

In short, CorreLog server offers a lot of bang for the buck and proves easy to install and use. Excellent documentation and very good support highlight some of the advantages offered by the product, while reporting flexibility paired with Excel integration make it a valuable ally for the harried compliance officer.

DETAILS

Vendor	CorreLog
Price	$5,000
Contact	correlog.com
Features	★★★★¼
Ease of use	★★★★½
Performance	★★★★★
Documentation	★★★★½
Support	★★★★¼
Value	★★★★
OVERALL RATING	★★★★½

Strengths Simple to deploy SIEM that covers all the basics.

Weaknesses Lacks some high-end features, such as an interactive report generator.

Verdict Excellent SIEM, especially for smaller networks with limited server resources.

Prism Microsystems EventTracker v7.2

Nowhere does a product name better describe its capabilities than with EventTracker from Prism Microsystems. From the outset, EventTracker is designed to track events and track them well. Now, in version 7.2, EventTracker has been around for some time and comes in a variety of flavors, ranging from the EventTracker Syslog product to the EventTracker Cloud offering to the EventTracker Operations Center.

Picking which edition to use all comes down to what an administrator wants to accomplish. For SIEM, multiple editions are applicable. However, once compliance and security reporting are thrown into the mix, EventTracker Enterprise seems to make the most sense.

Like many other SEIM products, EventTracker Enterprise uses a client server paradigm, where client systems report back to a server, which consolidates and normalizes events for further processing. Billed as a tool that provides a 360-degree view of log management, log monitoring, log search, file integrity monitoring, system monitoring, reporting, analytics, as well as visualization for continuous monitoring of system logs, users, file changes, servers and desktops, EventTracker Enterprise comes across as a comprehensive SIEM product.

The tool aggregates security and audit logs in real time from sources including Windows servers and desktops/laptops, Unix/Linux systems, Syslog devices (switches/routers), mobile devices, user activity, privileged user/administrator activity, security policy changes, applications and databases, USB and writeable media, routers and switches, intrusion detection system (*IDS*)/intrusion prevention system (*IPS*), anti-virus, VMware, mobile devices, as well as physical security systems and biometric systems.

Nevertheless, EventTracker proves to be as comprehensive as it is complex, with a laundry list of features, including automatic remediation, real-time alerting and monitoring, search, reporting, compliance, endpoint protection, log collection, secure log storage, correlation, behavior analysis and Windows agents. EventTracker Enterprise covers the gambit of SIEM and then some. In other words, as SIEM products go, EventTracker Enterprise proves to be much more than a traditional SIEM product.

Installation of the product is surprisingly simple and mostly automated. However, there is a prerequisite check that must be accomplished before installation takes place, though that is automated for the most part as well. Some of the prerequisites include having .NET Framework and other critical components installed. Once prerequisites are met, installation is smooth and event free.

Initial configuration is done via the product's intuitive GUI, which offers menus, wizards and real-time advice to set up the features. However, due to the rich feature set, navigating the browser-based GUI can be a little frustrating, at least until one gets used to the product.

All of its functionality comes at a price, namely an expensive one – at least when compared with basic SIEM products. Nevertheless, that high cost still offers significant value, especially considering all of the extra capabilities offered.

DETAILS

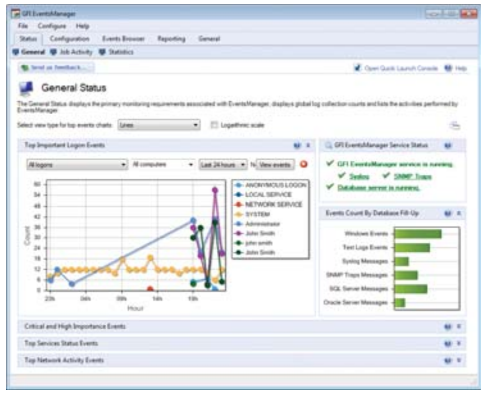
Vendor	Prism Microsystems
Price	$21,000
Contact	prismmicrosys.com
Features	★★★★★
Ease of use	★★★½
Performance	★★★★½
Documentation	★★★★
Support	★★★★★
Value	★★★★
OVERALL RATING	★★★★¼

Strengths Chock-full of features, this is a SIEM that should meet most any enterprises needs.

Weaknesses One of the more complicated SIEMs to deploy and master.

Verdict A great SIEM for those looking for all the possible bells and whistles.

GFI Software GFI EventsManager 2012



The General Status displays the primary monitoring requirements associated with EventsManager, displays global log collection counts and lists the activities performed by EventsManager

✓ GFI EventsManager service is running.
✓ Syslog ✓ SNMP Traps
✓ Database server is running.

GFI Software is one of the smaller vendors in the SIEM market. However, size doesn't matter if you build quality into a product like GFI has done with its GFI EventsManager 2012. Although it may sound like something a wedding planner may use, EventsManager 2012 is aimed directly at the SIEM market segment.

The product is designed to do exactly as the name implies – manage events – and in the case of SIEM, those events can originate from any number of network-attached devices in the typical enterprise, whether they are servers, PCs, firewalls, appliances and so forth.

GFI EventsManager takes a KISS (keep it simple & short)-approach to gathering data, while not sacrificing any robustness of the data collected. The product's log and event management capabilities prove to be more than adequate and incorporate an impressive array of filters, classifications and triggers. A notable capability is the product's ability to work without using any Windows agents. Rather, GFI has built in the ability to read native Windows events from Windows systems without the need to install a software client on the subject system.

Installation proved straightforward – as with most products today, the installation is wizard driven. However, the product is designed to run on a Windows Server-class system, but also can be run on Windows XP in a pinch. Nevertheless, there are some prerequisites that must be met, such as having .NET installed on the system acting as a server. Luckily, GFI does an excellent job of documenting those requirements, and provides a straightforward getting-started document that helps to smooth out any installation speed bumps.

EventsManager sports an excellent interface that proves to be both intuitive and loaded with actionable information. The GUI gathers up related information and displays it in a fashion that makes it easy to see correlations between events and devices, as well as using color coding to highlight the priority of alerts. However, that clean interface design proves to be a necessity simply because EventsManager does not have a threat correlation engine. In the big scheme of things that proves to be much less important than one would think, because GFI makes it easy for an administrator to correlate threats.

EventsManager offers a robust reporting engine that allows administrators to define a multitude of reports with custom parameters, which helps to ease auditing chores and streamlines the event discovery process. Perhaps, one of the product's biggest strengths lies in its ability to associate and define critical events and then choose to automatically alert administrators about critical events or even launch scripts to auto-remediate specific problems.

All things considered, GFI EventsManager proves to be very apt at what it is designed for, managing events driven by the SIEM methodology. Strong reporting tools and an interactive GUI round out the product, making it one to consider for most any SIEM project.

DETAILS

Vendor	GFI Software
Price	Servers and network devices: $147 per node for a volume of 50 to 99 nodes; includes one year of SMA; Windows Workstations: $17 per node for a volume of 50 to 99 nodes; includes one year of SMA
Contact	gfi.com
Features	★★★★¾
Ease of use	★★★★½
Performance	★★★★★
Documentation	★★★★
Support	★★★★½
Value	★★★★¾
OVERALL RATING	★★★★½

Strengths Easy-to-use SIEM that can function without agents or complex infrastructure requirements.

Weaknesses Lacks NetFlow capture and threat correlation analytics.

Verdict Capable product that nails much of what SIEM is all about.

DETAILS

Vendor	NetIQ
Price	$40,000 (500 events per second) to $650,000 (50K EPS)
Contact	netiq.com
Features	★★★★½
Ease of use	★★★★½
Performance	★★★★
Documentation	★★★★
Support	★★★★★
Value	★★★★
OVERALL RATING	★★★★½

Strengths Easy to deploy, scale and use.

Weaknesses Radical change in licensing model may be off-putting to traditionalists and can become expensive quickly.

Verdict An impressive SIEM that is feature rich, quick to deploy and easy to use.

NetIQ Sentinel v7

Sentinel from NetIQ is one of those security products that is supposed to make administrators feel assured about network events that can indicate trouble. Using the SIEM methodologies, NetIQ's Sentinel v7 looks deep into Syslogs, simple network management protocol (SNMP) incidents and other event-driven reporting mechanisms to sum up the security health of a network.

Probably one of the newest releases of a SIEM product covered here, v7 of Sentinel was announced on February 28 at the RSA Conference. That means Sentinel should have the latest and most mature features of the lot and should impress most anyone that is looking for the latest in SIEM products.

However, just because something is the newest doesn't always make it the best. That said, Sentinel 7 does a bang-up job of taming the SIEM beast. NetIQ went for a common thread with Sentinel v7 – ease of use. Indeed, great strides were taken to make the product one of the easiest-to-use SIEM solutions on the market.

One of the first elements of confusion that NetIQ chose to tackle was licensing. The company takes the unique approach of licensing the product based on events per second. In other words, low traffic networks, even those that sport a lot of different components, may be able to get by with a license that just supports 500 monitored events per second. High-value, busy networks may need to go with a license that supports 50,000 events per second. It all comes down to traffic and not physical components.

Other elements that suggest simplicity include plug-and-play deployment, as well as auto-configuration wizards. Sentinel is delivered as a virtual appliance, which can run on virtualized hardware, making it easy to scale the product by just throwing more resources at it. What's more, the virtual appliance approach makes it easier to backup or transfer Sentinel. It even seems to fit better into a failover or quick-disaster recovery scenario, as well.

The offering comes pre-equipped with packaged intelligence to detect many threats out of the box without time-consuming rule-writing and configuration. Built-in anomaly detection automatically establishes baselines of normal activity and detects changes that can represent emerging threats. New or custom rules can be created easily by business users through an intuitive and easy-to-navigate GUI.

The product is able to gather events from a multitude of sources and quickly analyze those events to present alerts to administrators in a fashion that is both easy to understand and actionable.

Also, Sentinel gathers as much information as physically possible when following an event. Information such as the who, what, when and where is readily preserved for future analysis, making the product suitable for dealing with both insider and outsider threats.

Extensive reporting capabilities are driven by NetIQ Sentinel's ability to capture rich data, instead of just the ordinary, or basic events, allowing administrators to look at "what-ifs," as well as "what-happened" in an intelligent fashion.

SolarWinds Log & Event Manager v5.3

SolarWinds is one of the smaller players in the SIEM market, but as a vendor specializing in system management and reporting tools, the company has the intelligence to effectively create a SIEM product.

Nevertheless, SolarWinds has focused on value as the keystone of the company's SIEM product, which goes by the moniker Log & Event Manager (LEM for short) and is now in v5.3. LEM has a bargain-basement price of $4,495 and is shipped as a virtual appliance. Although the product lacks some features found in other SIEM products, such as Netflow analysis, it remains surprisingly robust.

As a virtual appliance, installation proves to be rather simple – it is just a matter of importing the virtual appliance files onto a virtual server and then configuring the virtual server with the appropriate networking and storage configuration. Simply put, installation requires little more than knowledge of how a virtual appliance is added to the network infrastructure.

LEM works with hundreds of different network devices and can import Syslog data, as well as work directly with the log capabilities of dozens of security appliances, firewalls, intrusion detection systems and so on. LEM can gather data from servers, desktops and other pieces of network equipment as well.

Initial configuration proves straightforward, as the company includes hundreds of pre-defined rules and reports that make it easy to get started. The browser-based GUI offers excellent, actionable information in a clean and easy-to-use interface. Setup wizards and best practice tips round out the configuration tasks, allowing most anyone to quickly get the system up and running.

One of the key features of LEM is its ability to visualize events. The product offers a plethora of charts, graphs and more that make it easy for an administrator to observe what is going on across the network. Many of those visualizations support real-time feeds as well. The product includes more than 300 built-in templates for report generation, making it a little easier to satisfy requirements for PCI DSS , *Gramm-Leach-Bliley Act (GLBA)*, *Sarbanes–Oxley Act (SOX)*, NERC CIP, and the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* reporting.

The product also includes the ability to monitor for specific events and then execute scripts to take action. Administrators also can define notifications based on specific occurrences. Other features include compliance reporting and the ability export out data for further analysis.

A correlation engine rounds out the product's capabilities, which can process events in real time and in memory, using nonlinear and multidimensional techniques. The tool comes with nearly 700 built-in event correlation rules, potentially saving an administrator hours of work from defining rules.

Like many of the better SIEM products available on the market, LEM not only identifies and reports on anomalous behavior, it is also able to automatically take action to prevent that behavior from increasing and potentially compromising systems further, which means that LEM is able to prevent attacks in real time.

DETAILS

Vendor	SolarWinds
Price	$4,495
Contact	solarwinds.com
Features	★★★★½
Ease of use	★★★★
Performance	★★★½
Documentation	★★★¾
Support	★★★★¼
Value	★★★★★
OVERALL RATING	★★★★¾

Strengths Surprisingly effective SIEM considering the price.

Weaknesses Only available as a virtual appliance, limiting configuration options and performance potential.

Verdict A SIEM that is full of features and extended capabilities at a price that is very attractive.

Tenable Network Security Log Correlation Engine v3.6

Log Correlation Engine (LCE) from Tenable has been around for several years and has constantly been improved, enhanced and updated as needed to meet the ever-evolving needs of SIEM. The latest iteration of LCE can be considered something that is part of a bigger picture. Tenable refers to this as a unified security monitoring (USM) approach. Through this option, the company combines security management with log analysis and vulnerability scanning. That said, LCE is still a fine product when used independently of those other capabilities. However, it is nice to now that there is a bigger, integrated picture involved if one is looking to pursue a USM paradigm.

As the name implies, LCE is all about processing system logs and putting some sense to them in the form of intelligence and correlation. Its primary function is to collect, normalize and analyze logs from devices throughout the network. This, in turn, allows it to identify threats and vulnerabilities in real time.

LCE accomplishes that by analysis and data correlation from firewalls, intrusion detection and prevention systems, and data leakage prevention solutions, as well as from raw network traffic, application logs and user activity. The product also features an added bonus: the capability to perform traffic inspection, monitoring and analysis via NetFlow data, which many SIEM products cannot do.

Tenable has a focus on performance and claims that LCE can normalize and analyze one billion events in as little as 10 seconds, which speeds remediation efforts. Much of LCE's capabilities come from an anomaly detection engine that works hand in hand with event correlation to create statistical profiles, which trigger alerts when unusual behavior and never-before-seen events occur.

Simply put, LCE is one of the most sophisticated SIEM solutions on the market. However, that sophistication comes at a price – one that consists of a dedicated Linux (Redhat or CentOS) server and a significant investment in licensing fees. Still, those costs are offset by the high performance offered and the advanced capabilities included in the product.

LCE proves to be one of the more complex products to install and provision, requiring some Linux knowledge and a significant familiarity with networking devices and communications. Nevertheless, that setup complexity is offset by the product's easy-to-use GUI, which breaks events and devices up into manageable chunks so as to correlate directly with managed assets.

LCE shows real promise when integrated with Tenable's other products and wrapped under the company's top-of-the-line SecurityCenter product. Even alone, though, LCE offers some pretty amazing capabilities, such as 3D visualizations, real-time log analysis and intrusion correlation.

It is clear that LCE is designed for larger, more complex, highly active networks where SIEM is just one part of a larger posture. Yet, the product doesn't require a scientist to understand what is going on. Sure, a modicum of network and security knowledge is required to effectively use LCE, but one can leave the doctorate at the university when looking to leverage LCE's abilities.

DETAILS

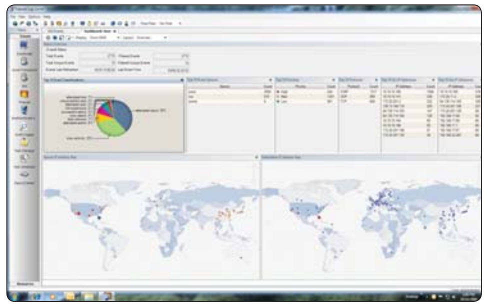
Vendor	Tenable Network Security
Price	$30,000 for 50-silo S/W; $60,000 for 255-silo S/W
Contact	tenable.com
Features	★★★★★
Ease of use	★★★½
Performance	★★★★★
Documentation	★★★½
Support	★★★★
Value	★★★★¼
OVERALL RATING	★★★★¼

Strengths Advanced analytics and impressive security event correlation.

Weaknesses : Can be complex and unwieldy to use on smaller networks.

Verdict Expensive, but capable SIEM that works best when paired with Tenable's other products.

Tripwire Log Center v6.5



Tripwire, a company better known for change management solutions, provides the perfect foundation for SIEM. After all, change management is related to tracking what's going on via logs, agents and other technologies, just like SIEM solutions do. That is not to say that Tripwire is new to the SIEM market, just that the company's Log Center product, which is in v6.5, has a great foundation to work from.

Log Center was created by Tripwire to deal with the intricacies of SIEM, which can differ from change management in several ways. First of all, there is more of an urgency surrounding SIEM. In other words, administrators need to know what is happening now as opposed to later during an audit. Log Center accomplishes that real-time data gathering by looking at log activity, such as Syslog updates, simple network management protocol (SNMP) events and so on, to monitor events that fall out of norms or baselines.

Like other products in the SIEM realm, Log Center is part of a larger product line that unifies compliance and security management. Still, the product can be used for the standalone process of SIEM, which many businesses not bound by compliance regulation only look to do.

Log Center goes a few steps further than the typical SIEM. For example, the product offers a capability called system state intelligence, which is context-aware information that combines the security state of a system with customer-specific notions of priority and risk. That may sound complex, but in practice it proves to be a valuable option, which improves security response.

Log Center is able to do that, and much else, by relying on more than just native OS auditing, by looking deeper into Syslog, SNMP, Windows Management Instrumentation (WMI) and other events. The tool then takes that raw data and performs real-time analysis to create baselines, as well as detect anomalies. By comparing the raw data against baselines and applying intelligence via defined rules, the Tripwire product can quickly identify breaches or other security threats and alert the appropriate administrator via email or other mechanisms. That creates the opportunity for a faster response to suspicious events, before they turn into full-blown security breaches.

The solution uses an intuitive GUI for management and reporting. However, this interface does not hide the product's sophistication and always seems to imply that one should be doing more with the product. It is that information overload that can prove both beneficial and detrimental at the same time. However, if Log Center is integrated into Tripwire's unified security products, the GUI makes a lot more sense and provides drilled-down, resolution-enforcing capabilities that many administrators are looking for with a unified security product.

Installation of the solution is relatively straightforward and wizards are there to help. There are some steep prerequisites though, including the need for an SQL engine of some type and a 64-bit version of Windows Server. However, those requirements do lay out the foundation for installing the rest of the company's suite of products without having to restart from scratch.

DETAILS

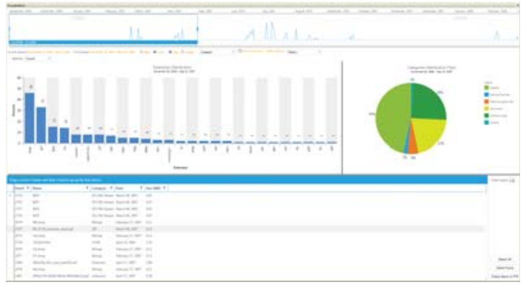
Vendor	Tripwire
Price	Console: $6,995; File Systems start at $127 per server and $32 per desktop; network devices start at $192 per device; security devices start at $319 per device
Contact	tripwire.com
Features	★★★★½
Ease of use	★★★¼
Performance	★★★★
Documentation	★★★★
Support	★★★★
Value	★★★★
OVERALL RATING	★★★★

Strengths A very capable SIEM product that offers a few advanced capabilities.

Weaknesses Can become expensive, and works best when integrated with the company's other security products.

Verdict A SIEM that is more than just a SIEM, but it really shines when incorporated into the company's expansive security suite.

Something new under the sun



AT A GLANCE

Product: FTK 4.0 with optional Cerberus and Visualization modules

Company: AccessData

Price: FTK 4.0: $2,995; Cerberus module: $2,400; Visualization module: $999

What it does: Updates FTK to a new level of functionality by adding the optional Cerberus (malware forensic analysis) and Visualization (files and email) modules.

What we liked: With these two powerful modules, this is my personal computer forensic tool benchmark.

What we didn't like: Nothing. This is the first serious advance in computer forensic tools in a long time.

As regular readers know, one of my occasional pet peeves regards the lack of innovation in our field, especially in digital forensics. In this field we tend to see more of the same tired old tools with a few new capabilities or a new point solution to specific forensic problems. But as for a sea change in the core computer or network forensics tools? Not so much.

All of that ended when AccessData introduced FTK 4.0 with Cerberus and Visualization. I almost never say this about a forensic tool, but this one blew me away. The things that you can do with this are so varied and so powerful that I predict it will become the benchmark for computer forensic tools for some time to come.

Cerberus allows one to do a deep analysis of every executable in an image for the presence of malware elements. That wants a bit of explaining. Just because an executable has some malware elements doesn't mean that it is malware, so the expert knowledge of the examiner comes into play. This tool is not as useful if one doesn't have at least a modicum of knowledge about malware mechanics. If one does, though, a deep dive into executables is possible, performing both static and dynamic analyses.

Cerberus – named after the three-headed dog of mythology that guards the gates of Hades – dissects every executable in an image and then shows all of the internals, such as memory usage, system calls and more. It scores these so that at a glance one can get an idea of which files need a bit more attention. Then one can drill into the code and Cerberus does all of the reversing and analysis for the user. It really is quite amazing, and it is very powerful if one knows how to take full advantage of it.

But the feature I found most useful was email visualization. Most visualizers break at around 25,000 items. I have a case that has been bedeviling me for about three years, and it is fairly large – well over a terabyte of images from three machines. There are more than 26,000 emails, so I thought, "What the heck…I'll just load them up and see where this takes me." It took quite a while to load – that is a lot of data – but once in, I was able to see things that I had not considered in earlier analyses.

For example, the social display shows with whom a particular individual has communicated. It gives a strong social network display – a circle with the originator in the center and the recipients toward the perimeter of the circle, closer or further depending on frequency of emails.

All of the difficult mathematical analysis and weightings have been done for the user who is left with only the need to look at the pretty pictures and draw conclusions. Lest that sound as if I am trivializing this impressive tool set, the pictures are pretty, and that is part of FTK 4's power. It helps the examiner get to the heart of the matter faster so that the real head work – the deep thinking and analysis that only an experienced examiner can perform – can start sooner, resulting in clearing more cases faster and with a higher percentage of wins.

Even though this one seems a bit pricey, for a busy FTK shop – or a shop contemplating moving to FTK – it is worth every penny. I really liked this one and I will be using it in the SC Lab. – *Peter Stephenson, technology editor*

Events Seminars

Start here for a calendar of events. To have your event included, contact scfeedbackUS@haymarketmedia.com

APRIL

»SANS Northern Virginia 2012
April 15-20
Do you need to become a more effective leader when implementing security improvements for your organization? Are you looking for more in-depth knowledge of the theory and implementation of computer security, virtualization or securing your private cloud? Then, this is the show for you.
Venue: Reston, Va.
Contact: www.sans.org/info/92299

SANS AppSec 2012
April 24-May 2
The theme for this year's conference is "Application Security at Scale." With billions of records in the cloud, millions of smart mobile devices, and millions of developers writing new code, what cutting-edge techniques are attackers using?
Venue: Las Vegas
Contact: www.sans.org/info/90589

»2012 ASIS NYC Security Expo
April 25-26
The 22nd NYC Security Conference and Expo is expanding. This year, there is a two-day format, offering more education, additional face time with exhibitors and extended networking. This event attracts attendees from both the public and private sectors who are looking for the latest security solutions, as well as benefiting from the wealth of information provided by security industry leaders. New this year: The ASIS Global Terrorism Conference and the CSO Roundtable Conference are co-locating with the NYC Security Expo.
Venue: New York
Contact: www.asisonline.org

MAY

»SC Congress Canada
May 8-9
Following up on the success of two previous events, the third annual SC Congress Canada conference and expo, a unique experience for the information security industry, offers up practical solutions to help both private and public sector chief information security officers thwart cyber attackers, safeguard critical corporate and customer assets, come into compliance with countless mandates and, ultimately, contribute to the overall profitability of their organizations. Information security leaders will be on hand to share insight, experiences and vast knowledge so attendees will leave the event armed with plenty of actionable information they immediately can put to use back in the office. Speakers to include Rick Yuen, Direct Energy; Craig Gibson, European Union Project MASSIF; Faiza Kacem, National Bank of Canada; Larry Clinton, Internet Security Alliance; Winn Schwartau, M.A.D. Partners; and many others.
Venue: Toronto
Contact: sccongresscanada.com

JUNE

»Compliance Week 2012
June 4-6
Compliance Week's annual conference is a peer-to-peer event that spotlights corporate financial, legal, risk, audit and compliance leaders. It has featured the chief compliance officers of Google, Yahoo, HP, GE, Starbucks, Pfizer, PepsiCo, Raytheon, Lockheed Martin, Coca-Cola, Sprint, McDonald's, Intel, Boeing, Fannie Mae, Altria, Ford, BP, Office Depot, Wal-Mart, and other leading public companies. *SC Magazine* readers get $400 off. Use code CW12SCMG7 to sign up.
Venue: Washington, D.C.
Contact: conference.complianceweek.com

»SANS Forensics and Incident Response Summit 2012
June 21-27
The fifth annual event will focus on high quality and relevant content, as well as panel discussions in the fields of digital forensics and incident response.
Venue: Austin, Texas
Contact: www.sans.org/info/87899

JULY

»SANSFIRE 2012
July 7-15
SANS courses will cover penetration testing and hacker exploits, security, management, wireless, forensics, secure coding and much more.
Venue: Washington, D.C.
Contact: www.sans.org/info/97911

»Black Hat USA 2012
July 21-26
This annual event delivers actionable security information in a vendor-neutral environment. This year's event will host more than 50 training courses from top experts in the field, including "Briefings" tracks on security research, and workshop tracks dedicated to the demonstration of tools, strategies and open source apps.
Venue: Las Vegas
Contact: www.blackhat.com

AUGUST

»VM World 2012
Aug. 28-30
VMworld, hosted by VMware, is a virtualization and cloud infrastructure event designed for IT pros seeking to accelerate success in their enterprises while aligning their requirements to enable cloud implementations.
Venue: Las Vegas
Contact: www.vmworld.com

SEPTEMBER

»SANS Melbourne 2012
Sept. 3-8
Following requests to bring its technical tracks to Melbourne, SANS is pleased to bring three of its top courses.
Venue: Melbourne, Australia
Contact: www.sans.org/info/95339

ADVERTISER INDEX

Company	Page	URL
Bellevue University	5	www.bellevue.edu
Compliance Week 2012 Conference	19	www.complianceweek.com
ESET	Back Cover	www.eset.com
SC Virtual Conference	7	www.scmagazine.com
SC Congress	Inside Back Cover	www.scmagazine.com
Trend Micro	Inside Front Cover	www.trendmicro.com

David can be Goliath

Be patient and give staffers a real chance to show their stuff, says recruiter Michael Potters.

Unless you are a die-hard Giants or Knicks fan, you did not have a clue who Victor Cruz or Jeremy Lin were until recent events put them in the headlines. Two years ago, Cruz, a great speedster receiver who grew up in the old mill city of Paterson, N.J., went to school at the University of Massachusetts (which had never sent a receiver to the NFL), and went unclaimed at the 2010 draft. He was a walk-on at the Giants training camp in 2010 and impressed a number of coaches and a few fans who recognized his blazing speed, sure hands and great moves. The Giants ended up signing him for the league minimum $490,000.

In his first full year as a receiver, Cruz set the Giants record for receiving yards in a season – at 1,536 – and was a big factor in making quarterback Eli Manning look so good in this year's Super Bowl win over the New England Patriots

Next we come to Jeremy Lin. Once again, in 2010 Lin goes unwanted at the NBA draft and bounces around the league. The Knicks claimed him off waivers to sit on the bench and essentially be a backup's backup. He moved to New York and ended up sleeping on his brother's couch in Manhattan since he undoubtedly thought, "No way am I buying a condo in the city if I am going to be cut." It's likely you've since heard of his remarkable run and the excitement, and wins, he's brought to a formerly mediocre team. A few weeks ago no one had any idea who this person was.

And now for the lessons learned. If you are a looking to hire an IT security professional to run your network or protect your data: Look outside the box. Not all the successful recruits come from the best schools or the top companies: 32 NFL teams and 30 NBA teams passed on these guys, despite all of their high-paid research.

Be patient, give people a real chance to show their stuff: The NBA's Warriors and Rockets are shooting themselves now for having Lin and letting him get away.

When you realize you may have a gem, let them loose to succeed. Don't become an impediment to their growth. Further, make sure your team embraces their success, and all raise their games accordingly.

It's also a good idea to not be cheap. Just because you lucked out and hired a particularly bright and energetic person at a steal, pay them what they should be paid – or you will lose them as easily as you found them.

Meanwhile, if you are a candidate looking to break into this demanding field, don't ever believe that you can't compete with the big players from the better colleges or companies. You can. Fifty percent of the top people in the IT security industry fit into this category.

> "Not all the successful recruits come from the best schools..."

As well, if given the chance by a client, don't blow it. Work hard, perfect your craft, and when the door opens a crack, kick your way through and do the job better than you ever imagined.

However, don't be greedy. If the only way into the firm is to take a lower-than-desired fee, do it. You can prove yourself once you are in there and then potentially, at least, make all the money you deserve.

And, don't be selfish. Look to make your team better around you. They will appreciate it and pay you back by making you look better – which will, of course, earn you more money and a stable career.

Final message to hiring authorities: Two years ago, the general manager of the Giants had no idea who Victor Cruz was. A few weeks ago, the general manager of the Knicks had little clue who Jeremy Lin was. They both look like geniuses now and are likely going to be rewarded for the serendipitous nature of these events. Think outside the box.

Michael Potters is CEO and managing partner of Glenmont Group, a Montclair, N.J.-based recruitment firm.

Thank you!

SC MAGAZINE AWARDS 2012 WINNER
Honored in the U S

SC Magazine readers choose ESET No.1

Best Anti-Malware Management

And the best keeps getting better—
IT experts everywhere agree.

Windows IT Pro 2011 Editors' Best BRONZE

2011 Information Security's READERS' CHOICE AWARDS gold winner

AV ADVANCED+ ★★★ PERFORMANCE TEST comparatives NOV 2011

eset®

www.eset.com