FEATURES:

URGENT CARE

Health providers have pressing reasons to now embrace security, says INTEGRIS Health’s John Delano P20

Beyond BYOD
The ever-increasing use of personal devices has tested enterprise defenses, so plans must be created to meet the challenge P26

Copy that
A groundbreaking copyright case could change the legal role of Canadian ISPs PC1
Did you know that mobile workers who use a privacy filter are 50% more productive than those who don’t?* 3M Visual Privacy Solutions give your employees the privacy they need to get work done. 3M has been helping organizations keep their data private for over 25 years.

Step up your visual privacy with 3M.
3Mscreens.com/Business

*Visual Privacy Productivity Study, Ponemon Institute 2013. 3M is a trademark of 3M. © 3M 2013. All rights reserved.
Sidestepping the humdrum

Discussing cyber security trends with a number of industry players has me sighing, “ho hum.” Don’t get me wrong, I’m just as stoked as ever to be leading the charge at SC Magazine, navigating all the happenings to bring you timely news and features, events, videos and more.

Still, the topics we’re all discussing lately have become a little routine. Sure, the IT security space is crazy hot these days. Presid-

ing that China has been victimized, too – a willingness to engage in global cooperation to push by some vendors at conferences like RSA through terribly passé-for-the-times booth buds, that’s pioneering.

According to London-based industry body BCS, The Chartered Institute for IT, a threat only pondered before could see attackers using internet-connected devices, like those in hospitals, to execute physical crimes, such as murder. Another involves near-field communication (NFC) chips used for mobile payments, which will become a part of every smartphone soon. Cyber thieves, therefore, will be able to use holes in banking/e-commerce apps leveraging these chips to launch attacks with ease.

Yet, there always will be the same old, same old. Yet, new methods of attack continually are upon us. Fortunately, there are pretty forward-thinking industry pros, like those we honed recently at our SC Awards U.S. gala. By making more interesting plays, re-configuring their departments, modifying their policies and programs to address the constantly evolv- ing threat landscape and still more, hopefully those recurring moments will be few and far between.

But, then again, we’ve still got plenty of repetitive hype pushed by some vendors at conferences like RSA through territor- ial landscape, even if they’re not selling any more data. In fact, with the average large business storing more than 200 terabytes, companies have more than enough data to tell them who is buying their product, as well as how, when and where the buying happens.

DATA’S NEW VOICE.
Today, however, customers expect a company to know why they’re buying. Or why they aren’t. Because when a company knows what motivates customers, it can serve them better.

Companies aren’t short on data. In fact, with the average large business storing more than 200 terabytes, companies have more than enough data to tell them who is buying their product, as well as how, when and where the buying happens.

The good news is such data exists, just not in the columns, rows, reports and purchase histories we’re used to. It’s called big data, and it comes from tweets, videos,чикерная and other unstructured sources. It’s the data of desire. And today, we have the technology and tools to make sense of it.

So now, instead of learning which customers it has lost, a company can learn which customers it might lose and present timely offers or products motivating those customers to stay. Using IBM Smarter Analytics to identify which customers were most likely to switch to another communications carrier, XO Communications was able to predict likely customer defections within 90 days, reducing churn by 35 percent the first year.

With IBM Smarter Analytics, companies are gathering big data and using it to ask—and answer—smarter questions about what their customers really want. IBM.com/usingbigdata

IBM. “For the first time, we can decide which promotions to run based on facts rather than gut feel!”

THE POWER OF BIG DATA.

Companies aren’t short on data. In fact, with the average large business storing more than 200 terabytes, companies have more than enough data to tell them who is buying their product, as well as how, when and where the buying happens.

DATA’S NEW VOICE.
Today, however, customers expect a company to know why they’re buying. Or why they aren’t. Because when a company knows what motivates customers, it can serve them better.

...security initiatives shouldn’t curtail citizens’ basic rights, like privacy.”
April 25  
eSymposium: Cyber espionage
Even members of Congress can agree that nation-state spying is a major problem for both the country’s corporations and government agencies. From direct attacks on companies to backdoors that allegedly are cropping up in telecommunications hardware and software sold to U.S.-based organizations, the methods to conduct cyber espionage attacks run the gamut. We take a look at the threat and find out what the U.S. government, private firms and others are doing to address the problem.

FOR MORE INFO
For details on SC Congress events, please contact Natasha Mulla at natasha.mulla@haymarketmedia.com.

For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazine.com/sc-congress-247.

WHAT IS SC CONGRESS 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 CONGRESS

Rich Baich, chief information security officer, Wells Fargo & Co.; former principal, security and privacy, Deloitte and Touche
Greg Bell, global information protection and security lead partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Algea
Jaime Cunagua, managing director, CSO Board Consulting
Rufus Connell, research director, information technology, Frost & Sullivan
Dave Cullumlane, CIO, Security Starfish; former chief information security officer, eBay
Mary Ann Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president, information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Sophos
Gene Fredrickson, chief information security officer, Tycos International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
W. Hord Tipton, executive director, (ISC)2; former CIO, U.S. Department of the Interior

WHO’S WHO AT SC MAGAZINE

EDITORIAL
VP, EDITORIAL  Ilana Armstrong  ilana.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
REPORTER  Danielle Walker  danielle.walker@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 Kilban  john.kilban@haymarketmedia.com
SC LAB EDITORIAL ASSISTANT  Judy Traub  judy.traub@haymarketmedia.com
PROGRAM DIRECTOR, SC CONGRESS  Eric Green  eric.green@haymarketmedia.com
REGULAR CONTRIBUTORS
Stephen LaRoe, Delli Raccio, Karen Epper Hoffman

U.S. SALES
VP, SALES  David Stoffman  (646) 638-6028  david.stoffman@haymarketmedia.com
REGIONAL SALES DIRECTOR  Mike Shenon  (646) 638-6005  mike.shenon@haymarketmedia.com
WEST COAST SALES DIRECTOR  Matthew Allington  (415) 346-6400  matthew.allington@haymarketmedia.com
EVENT SALES DIRECTOR  Mike Alessie  (646) 638-6002  mike.alessie@haymarketmedia.com
ACCOUNT MANAGER  Dennis Koster  (646) 638-6023  dennis.koster@haymarketmedia.com
ACCOUNT MANAGER  Samantha Annesio  samantha.annesio@haymarketmedia.com
SALES EDITORIAL ASSISTANT  Alisa Hall  (646) 638-6024  alisa.hall@haymarketmedia.com
ACCOUNT EXECUTIVE, LICENSING AND REPRINTS  Elton Wong  (646) 638-6520  elton.wong@haymarketmedia.com
SC MAGAZINE LIST RENTAL
REACH MARKETING  Wayne Hapnigowski  VP, marketing solutions  (845) 205-5338  wayne.hapnigowski@haymarketmedia.com
CIRCULATION
AUDIENCE DEVELOPMENT DIRECTOR  Sherry Dongree  (646) 638-6003  sherry.dongree@haymarketmedia.com
CUSTOMER DATA MANAGER  Joshua Blair  (646) 638-6048  joshua.blair@haymarketmedia.com
SUBSCRIPTION INQUIRIES
CUSTOMER SERVICE  (800) 558-1703
EMAIL  info@haymarketmedia.com
WEB  www.scmagazine.com/scref//sitecore
MANAGEMENT  COO, HAYMARKET MEDIA  Lee Maniscalco
EXECUTIVE VP  Tony Kaela

Imagine an enterprise network with smartphones, tablets, mobile PCs – and no compromises. ForeScout delivers real-time visibility and control over mobile computing devices. Users get the freedom, while you protect the network from data loss and malicious threats. Poof! Your primary IT problems just disappeared. Get an IDC whitepaper and more BYOD Essentials at forescout.com.
Malware Vertical encounter rate

<table>
<thead>
<tr>
<th>Position</th>
<th>Industry</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Education</td>
<td>146%</td>
</tr>
<tr>
<td>2</td>
<td>Retail and wholesale</td>
<td>104%</td>
</tr>
<tr>
<td>3</td>
<td>Health care</td>
<td>100%</td>
</tr>
<tr>
<td>4</td>
<td>Banking and finance</td>
<td>69%</td>
</tr>
<tr>
<td>5</td>
<td>Food and beverage</td>
<td>58%</td>
</tr>
<tr>
<td>6</td>
<td>Government</td>
<td>46%</td>
</tr>
<tr>
<td>7</td>
<td>IT and telecommunication</td>
<td>46%</td>
</tr>
</tbody>
</table>

The education sector was hit with the most malware in the last measurement.

Top breaches in February

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Data loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter San Francisco</td>
<td>Online attackers accessed the usernames, email addresses, session tokens, encrypted passwords (no SSNs) of users</td>
<td>250,000</td>
</tr>
<tr>
<td>Central Hudson Gas &amp; Electric Poughkeepsie, N.Y.</td>
<td>Customer banking information and other personal information may have been accessed during an attack over Presidents’ Day weekend.</td>
<td>110,000</td>
</tr>
<tr>
<td>Froedtert Health Milwaukee</td>
<td>A virus was discovered on an employee’s computer account. One of the files on the computer contained PHI of patients (including some SSNs).</td>
<td>43,000</td>
</tr>
</tbody>
</table>

The biggest increases in month-over-month zombie activity occurred in India and “other” European and North American nations, while the largest decreases occurred in China, Vietnam and “other” Asian and South American nations.

Index of cyber security

<table>
<thead>
<tr>
<th>Rate of change over previous month (%)</th>
<th>Perceived risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1.5</td>
<td>1.5</td>
</tr>
<tr>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>2.5</td>
<td>2.5</td>
</tr>
<tr>
<td>3.0</td>
<td>3.0</td>
</tr>
</tbody>
</table>

The index queries information security industry professionals monthly to gauge their perceived risk to the corporate, industrial and governmental information infrastructure from a spectrum of cyber security threats. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite.

Top breaches in February

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Data loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter San Francisco</td>
<td>Online attackers accessed the usernames, email addresses, session tokens, encrypted passwords (no SSNs) of users</td>
<td>250,000</td>
</tr>
<tr>
<td>Central Hudson Gas &amp; Electric Poughkeepsie, N.Y.</td>
<td>Customer banking information and other personal information may have been accessed during an attack over Presidents’ Day weekend.</td>
<td>110,000</td>
</tr>
<tr>
<td>Froedtert Health Milwaukee</td>
<td>A virus was discovered on an employee’s computer account. One of the files on the computer contained PHI of patients (including some SSNs).</td>
<td>43,000</td>
</tr>
</tbody>
</table>

The chart above reflects the encounter rate in January 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-media rate.

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Sinowal trojan
3. Pushdo trojan
4. Chinese InfoStealer trojan
5. Downloader trojan

Top 5 attacks used by U.S. hackers

1. ZeroAccess trojan
2. Sinowal trojan
3. Pushdo trojan
4. Chinese InfoStealer trojan
5. Sinowal trojan

There were 27,211,495 attacks in the United States last month, primarily originating from Los Angeles, Cleveland, Phoenix, New York and Chicago. There were 26,067,075 foreign attacks last month, primarily originating from Bucharest, Romania; Tokyo; Mumbai, India; Taipei, Taiwan; and Sao Paulo, Brazil.

Spam rate

The Spam rate index tracks the volume of spam by month and by region.

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Sinowal trojan
3. Pushdo trojan
4. Chinese InfoStealer trojan
5. Sinowal trojan

There were 27,211,495 attacks in the United States last month, primarily originating from Los Angeles, Cleveland, Phoenix, New York and Chicago. There were 26,067,075 foreign attacks last month, primarily originating from Bucharest, Romania; Tokyo; Mumbai, India; Taipei, Taiwan; and Sao Paulo, Brazil.

Spam rate

The Spam rate index tracks the volume of spam by month and by region.

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Sinowal trojan
3. Pushdo trojan
4. Chinese InfoStealer trojan
5. Sinowal trojan

There were 27,211,495 attacks in the United States last month, primarily originating from Los Angeles, Cleveland, Phoenix, New York and Chicago. There were 26,067,075 foreign attacks last month, primarily originating from Bucharest, Romania; Tokyo; Mumbai, India; Taipei, Taiwan; and Sao Paulo, Brazil.

Spam rate

The Spam rate index tracks the volume of spam by month and by region.

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Sinowal trojan
3. Pushdo trojan
4. Chinese InfoStealer trojan
5. Sinowal trojan

There were 27,211,495 attacks in the United States last month, primarily originating from Los Angeles, Cleveland, Phoenix, New York and Chicago. There were 26,067,075 foreign attacks last month, primarily originating from Bucharest, Romania; Tokyo; Mumbai, India; Taipei, Taiwan; and Sao Paulo, Brazil.
China Breach

A detailed report from incident response and forensic firm Mandiant on the inner workings of a Chinese-based cyber espionage group uncovered the purported theft of hundreds of terabytes of information from more than 100 organizations in the United States. The operations of the secret Chinese military unit 61398 were traced to a 12-story building in Shanghai.

China has denied the hacking accusations.

$25 million complaint after losing a USB stick containing 25,000 customer records.

On Jan. 18, the hospital went public with the news that the unencrypted USB key with patient data had been lost after an employee left the hospital with it to work at home. On March 27, the USB key was recovered. However, Sharon Strobos, a lawyer representing patients, said her clients were still concerned about whether it was accessed, and records copied during the period when it was missing.

On the heels of an email campaign in which Tibetan activists were targeted with malicious Android apps, academic researchers in Canada have detailed how foreign spies are upping their game. In an analysis released last month of another Android malware campaign targeting these same Tibetan activists, researchers at the Citizen Lab, part of the Munk School of Global Affairs at the University of Toronto, have determined that it appears to be the work of Chinese hackers, possibly with the assistance of the nation’s government or a major corporation.

The research began when a Tibetan “source” tipped off the Citizen Lab by sending it a copy of an email that was the spoofed version of an actual email sent in December from an unnamed information security expert to a member of the Tibetan Parliament-in-Exile.

Chinese hackers have long been suspected in various malware campaigns targeting Tibetan dissidents, but this latest Android threat provides some of the most convincing evidence to date that the attacks are state sponsored.

Debate

China is the top cyber threat to United States.

While it’s probably true that all nations engage in cyber espionage to support their national interests, no other country has targeted and breached the United States to the extent and with the level of daring that China has. Massive operations like Nitro, Aurora, Shady RAT, Night Dragon – and the more recent attacks on the New York Times, Wall Street Journal and Bloomberg – show the vast scale, frequency and range of targets that China is able to pull off. While the U.S. certainly faces other cyber foes, and some of these are quite serious, none of them seem to have the breadth and reach that the Chinese do. The Chinese are into virtually everything – SCADA, telecom, oil/natural gas, public companies, consumer tech companies, universities, nonprofit organizations, military agencies, government departments, etc. – basically every facet of the U.S. economy and our government.

What makes this especially dangerous is the seeming unwillingness of the Chinese government to confront this problem publicly.

Is China stealing our intellectual property and probing our networks millions of times a day? Yes. Does this make them the top cyber threat to the United States? No. Here’s why: China’s modus operandi is information gathering, not attacking. They’re in the business of gathering intel and stealing secrets, which is bad, but not as bad as destroying that data, sabotaging companies or internal networks, or launching critical infrastructure attacks. China will never go there because its economy is too intertwined with our own. Therefore, its goal isn’t to destroy the U.S., just to compete with us.

The more dangerous threat comes from adversarial countries that we could at, some point, go to war with – think Iran. Just look at what Iran did to Saudi Aramco. This is the real threat, and the one we’re least prepared for – i.e., data-wiping a major U.S. bank or taking over and crashing an unmanned aerial vehicle (UAV) into a building in retaliation for U.S. foreign policies and military intervention.

THE QUOTE

I don’t think they’re going to burst into tears if we say mean things about them.”

– James Lewis, senior fellow at the Center for Strategic and International Studies, on White House attempts to curb Chinese espionage attacks

THE STATS

8 months away: As part of the executive order, a preliminary framework is due from NIST on how to take existing security best practices and get them adopted more widely

52 percent increase in attacks on oil pipelines and electric power organizations from the number of reported attacks in 2012
Cleaning up the CVSS

C onsidering the frequency by which IT vendors release both scheduled and unexpected security updates, from Oracle to Adobe to Microsoft, prioritization is a key part of the patching strategy of any customer.

That mindset was the impetus behind the 2005 creation of the Common Vulnerability Scoring System (CVSS), a common standard created by FIRST (Forum of Incident Response and Security Teams), used to convey the severity of vulnerabilities.

The scoring system attempts to quantify the severity of vulnerabilities. But, as the software and hardware makers provide to organizations like the National Vulnerability Database to generate CVSS scores. In some cases, after all of the details eventually became public, it was apparent that certain flaws didn’t deserve the high scores they received. But that isn’t not before businesses may have thrown resources — or weekend work — at repairing a problem they could have waited on. “You don’t have to give us all the technical details, but give us enough,” Martin said of IT makers.

Serh Banford, chairman of FIRST’s CVSS Special Interest Group, said many of the concerns raised by Martin and Eiram will be worked into the v3 release, scheduled for 2014.

“Virtualization, a major shift into threats targeting client-side vulnerabilities, and a greater need to capture more information about vulnerabilities — among other things — are all driving us to the improvements we have planned for v3,” he said in an email. — Dan Kaplan

4,347 new security vulnerabilities were reported in 2012
– National Vulnerability Database

| Jobs Market |
| Me and my job |

**Blake Frantz**
director of benchmark development, security benchmarks division, Center for Internet Security (CIS)

**How do you describe your job to average people?**
My job is to build communities of experts who can define what best practice looks like for securely configuring IT components, such as operating systems, web browsers and mobile devices. At CIS, we call each set of best practices a “benchmark.” From there, our team coordinates with customers and partners to automate the assessment and implementation of those benchmarks in organizations.

**Why did you get into IT security?**
I wasn’t given a choice. I’ve had a heavy stoke for security-related work since high school, when a friend and I developed an interest in phone security. We found other like-minded people on a bulletin board system. Over the years, the communities and projects have changed, but not the stoke.

**What was one of your biggest challenges?**
CIS benchmarks cover a wide range of technologies and I enjoy studying the security mechanics of most of them. One of my biggest challenges is maintaining a balance between digging in enough to effectively perform my job and spending too much time geeking out.

**What keeps you up at night?** I lose sleep when a project isn’t progressing as fast as I’d like, or when I’m asked about a concept that CIS or another organization is developing.

**What was one of your biggest challenges?**
It takes pride in my work, but I’m most proud of my family and friends. IT accomplishments are awesome, but bear hugs and high fives are my kind of jam.

**How would you use a major IT security Ward?**
I would conjure up an infinitesimal pool of highly skilled security experts who took to the heart the wise words of Spider-Man’s Uncle Ben: “With great power, comes great responsibility.”

**Anthony Freed**
community engagement coordinator, Tripwire

**How do you describe your job to average people?**
A community engagement coordinator is essentially some kind of jam.

**What it takes**
As companies with enterprise governance, risk and compliance (eGRC) programs collect increasing amounts of data, there is a growing demand for IT-GRC-focused data and metrics analysts.

**What it takes**
These roles focus on leveraging data to make better risk management decisions. Key skills include experience working with eGRC tools, data analysis, interpretation of board creation and the ability to present findings to internal stakeholders. CS and MIS degrees are often required.

**Compensation**
Base compensation ranges from $60K at the entry level to $130K at the senior level.

**Skills in demand**
As companies with enterprise governance, risk and compliance (eGRC) programs collect increasing amounts of data, there is a growing demand for IT-GRC-focused data and metrics analysts.

**What it takes**
These roles focus on leveraging data to make better risk management decisions. Key skills include experience working with eGRC tools, data analysis, interpretation of board creation and the ability to present findings to internal stakeholders. CS and MIS degrees are often required.

**Compensation**
Base compensation ranges from $60K at the entry level to $130K at the senior level.

**Skills in demand**
As companies with enterprise governance, risk and compliance (eGRC) programs collect increasing amounts of data, there is a growing demand for IT-GRC-focused data and metrics analysts.

**What it takes**
These roles focus on leveraging data to make better risk management decisions. Key skills include experience working with eGRC tools, data analysis, interpretation of board creation and the ability to present findings to internal stakeholders. CS and MIS degrees are often required.

**Compensation**
Base compensation ranges from $60K at the entry level to $130K at the senior level.
You are an APT target

Phillip Ferrara
CSO, DRS Integrated Defense Systems and Services

Almost every week we read in the news about another organization that has been hacked. Cyber espionage is at all-time high, and businesses across the United States are being targeted and breached. Many of these attacks are nation-state-sponsored or otherwise known as advanced persistent threats (APT). However, organized crime and other hacker groups are also responsible for many of these attacks. Their goal is simple: Breach an organization and steal information of value, whether trade secrets, sensitive business information to gain economic advantage.

In February, security firm Mandiant released a 60-page report detailing its investigations over a six-year post into Operation Shady RAT, which has been hacked. Cyber security is not an IT function. Rather it is a business function. The threat must be explained in terms of the impact that it can have on the business. Not only can the cost of containment and mitigation of a breach be extremely expensive, but the loss of intellectual property, trade secrets, sensitive business information, and years of R&D work, not to mention brand or reputational damage, can put an organization out of business.

Operation Shady RAT

APTs are not a new phenomenon, says Ferrara. In 2011, McAfee researchers gained access to a single command-and-control server that showed 71 organizations were breached. The attackers then sent an email attachment with malware from inside the breached organization to RSA, consequently infecting the security firm.

But, even in this example, RSA was not the final target. It was merely a pivot point used to breach a much larger defense contractor. CSOs and CISOs must fully understand the threat and the method of operations of these malicious actors. It is extremely important that they educate the executives of their organization on these threats. When presenting to the C-level management or to board members, the CSO/CISO must keep in mind that cyber security is not an IT function. Rather it is a business function. The threat must be explained in terms of the impact that it can have on the business. Not only can the cost of containment and mitigation of a breach be extremely expensive, but the loss of intellectual property, trade secrets, sensitive business information, and years of R&D work, not to mention brand or reputational damage, can put an organization out of business.

You’ve got mail

From the top down

President Obama has gone on record stating that threat from cyber is “one of the most serious economic and national security challenges we face as a nation.”

From the online mail bag

We received quite a bit of feedback in response to an Opinion on our site. The RSA Conference expo floor offended me – and why I blamed the exhibitors, by Winn Schwartau, founder, Security Experts.

Winn, you are now my official hero. At our PR/communications firms, we’re constantly pushing clients just a bit harder to go beyond “leading edge” and other empty, jargon-loaded phrasing, and really drive down to why what one does matters. To dispense with meaningless buzz phrases and quickly convey in a compelling way the “this is what our client does...and here are the tangible payoffs for customers” with real metrics, telling anecdotes, etc. – that’s harder to pull off. Which is why I suspect you were bombarded with marketing gibberish that essentially says nothing, but is much easier to produce (regardless of whether the client benefits). Anyway, thanks for posting this terrific column. dmcplf

Well said. I couldn’t agree more. As to “lead generation” being the goal, that is the weeks and months post-conference usually result in so much spam and cold calls that I have taken to providing wrong phone numbers and unmonitored email addresses. That sort of marketing isolates me. I guess I am old school. Show me what you have and “Don’t call me, I’ll call you.” Which, I think, is a point you are making. The most egregious thing I witnessed was being requiring to “friend the vendor on Facebook for some trivial piece of swag, etc. Talk about bottom of the barrel tactics. Personally, I do not think I will approve staff to go to these conferences much longer. I can obtain the necessary information from security blogs, journals, Gardner and a Google Search.

Winn, rather than blaming the exhibitors, I think a look in the mirror is the answer. Not you, specifically, but if the majority of the people at the show respond to what is being dished out, how can you blame the exhibitors? Maybe the serious security pro like yourself is not as desirable as you would think. Ultimately the market decides what is appropriate or now. [ed. note: adds a link to the Ashshimy blog. www.ashshimy.com] Alan Shimeil

In regards to a blog post. The White House thinks Julian Assange and Jeremy Hammond are no different than Chinese cyber spies, by Executive Editor Dan Kaplan. Dan, you’re off base on this one. Classified material is classified based on the assessed harm that disclosure would do to U.S. interests. Disclosure of classified material to the “public” is as bad as disclosure to the Chinese government because it is the same act. The Chinese intelligence services can read WikiLeaks the same as we can. Doesn’t matter that you had “nobler” intents, the end result is the same and is a real threat to our security.

Bill Murphy
Bill Murphy means well, but he is dangerously wrong. The 1947 National Security Act is clear – covert actions do not entitle the government to violate the laws and the Constitution. As a result, if somebody uses classification authority to cover up illegal acts, then they have abused that classification authority and the information was properly classified. If the OCA can’t prove it, then they’re the ones who should go to jail, and the whistleblower should keep their job and their clearance.

Winn, rather than blaming the exhibitors, I think a look in the mirror is the answer. Not you, specifically, but if the majority of the people at the show respond to what is being dished out, how can you blame the exhibitors? Maybe the serious security pro like yourself is not as desirable as you would think. Ultimately the market decides what is appropriate or now. [ed. note: adds a link to the Ashshimy blog. www.ashshimy.com] Alan Shimeil

In regards to a blog post. The White House thinks Julian Assange and Jeremy Hammond are no different than Chinese cyber spies, by Executive Editor Dan Kaplan. Dan, you’re off base on this one. Classified material is classified based on the assessed harm that disclosure would do to U.S. interests. Disclosure of classified material to the “public” is as bad as disclosure to the Chinese government because it is the same act. The Chinese intelligence services can read WikiLeaks the same as we can. Doesn’t matter that you had “nobler” intents, the end result is the same and is a real threat to our security.

Bill Murphy
Bill Murphy means well, but he is dangerously wrong. The 1947 National Security Act is clear – covert actions do not entitle the government to violate the laws and the Constitution. As a result, if somebody uses classification authority to cover up illegal acts, then they have abused that classification authority and the information was properly classified. If the OCA can’t prove it, then they’re the ones who should go to jail, and the whistleblower should keep their job and their clearance.

Winn, rather than blaming the exhibitors, I think a look in the mirror is the answer. Not you, specifically, but if the majority of the people at the show respond to what is being dished out, how can you blame the exhibitors? Maybe the serious security pro like yourself is not as desirable as you would think. Ultimately the market decides what is appropriate or now. [ed. note: adds a link to the Ashshimy blog. www.ashshimy.com] Alan Shimeil

In regards to a blog post. The White House thinks Julian Assange and Jeremy Hammond are no different than Chinese cyber spies, by Executive Editor Dan Kaplan. Dan, you’re off base on this one. Classified material is classified based on the assessed harm that disclosure would do to U.S. interests. Disclosure of classified material to the “public” is as bad as disclosure to the Chinese government because it is the same act. The Chinese intelligence services can read WikiLeaks the same as we can. Doesn’t matter that you had “nobler” intents, the end result is the same and is a real threat to our security.

Bill Murphy
Bill Murphy means well, but he is dangerously wrong. The 1947 National Security Act is clear – covert actions do not entitle the government to violate the laws and the Constitution. As a result, if somebody uses classification authority to cover up illegal acts, then they have abused that classification authority and the information was properly classified. If the OCA can’t prove it, then they’re the ones who should go to jail, and the whistleblower should keep their job and their clearance.

Winn, rather than blaming the exhibitors, I think a look in the mirror is the answer. Not you, specifically, but if the majority of the people at the show respond to what is being dished out, how can you blame the exhibitors? Maybe the serious security pro like yourself is not as desirable as you would think. Ultimately the market decides what is appropriate or now. [ed. note: adds a link to the Ashshimy blog. www.ashshimy.com] Alan Shimeil

In regards to a blog post. The White House thinks Julian Assange and Jeremy Hammond are no different than Chinese cyber spies, by Executive Editor Dan Kaplan. Dan, you’re off base on this one. Classified material is classified based on the assessed harm that disclosure would do to U.S. interests. Disclosure of classified material to the “public” is as bad as disclosure to the Chinese government because it is the same act. The Chinese intelligence services can read WikiLeaks the same as we can. Doesn’t matter that you had “nobler” intents, the end result is the same and is a real threat to our security.

Bill Murphy
Bill Murphy means well, but he is dangerously wrong. The 1947 National Security Act is clear – covert actions do not entitle the government to violate the laws and the Constitution. As a result, if somebody uses classification authority to cover up illegal acts, then they have abused that classification authority and the information was properly classified. If the OCA can’t prove it, then they’re the ones who should go to jail, and the whistleblower should keep their job and their clearance.

Winn, rather than blaming the exhibitors, I think a look in the mirror is the answer. Not you, specifically, but if the majority of the people at the show respond to what is being dished out, how can you blame the exhibitors? Maybe the serious security pro like yourself is not as desirable as you would think. Ultimately the market decides what is appropriate or now. [ed. note: adds a link to the Ashshimy blog. www.ashshimy.com] Alan Shimeil

In regards to a blog post. The White House thinks Julian Assange and Jeremy Hammond are no different than Chinese cyber spies, by Executive Editor Dan Kaplan. Dan, you’re off base on this one. Classified material is classified based on the assessed harm that disclosure would do to U.S. interests. Disclosure of classified material to the “public” is as bad as disclosure to the Chinese government because it is the same act. The Chinese intelligence services can read WikiLeaks the same as we can. Doesn’t matter that you had “nobler” intents, the end result is the same and is a real threat to our security.
Decoding the cloud

Unfortunately, data security and regulatory compliance requirements do not evaporate in the public cloud. The challenge of controlling access to sensitive information remains the same. In response, three approaches have emerged: enterprise encryption services, cloud service provider encryption services, and encryption gateways. Choosing the right one depends on the type of cloud delivery model involved—software-as-a-service (SaaS) or infrastructure-as-a-service (IaaS)—and the mandates that govern the data being placed in the cloud.

Enterprise encryption services for cloud service providers (CSP) encrypt sensitive data in IaaS environments, typically via a software agent sitting in the cloud—while encryption key management remains on premise. This approach can encrypt the entire mounted storage volume, or encrypt and control access to specific files in the CSP. The more granular file-level approach provides separation of duties within the enterprise, while both volume- and file-level approaches protect against bad actors attempting to compromise data in the public cloud.

CSP encryption services are similar to enterprise encryption services, except that the CSP holds the encryption keys. While this might seem convenient, it does pose security issues since there is no separation of duties for anyone accessing the data. Furthermore, an enterprise will not know if the CSP has handed the keys and data to a third party.

Encryption gateways encrypt data flowing from the enterprise into SaaS offerings, like Salesforce.com and Gmail. This approach can provide security for data in SaaS environments, while allowing the enterprise to maintain control of the data. Encryption gateways lend themselves to SaaS offerings where the SaaS provider does not provide encryption or the enterprise wants to maintain control of the data. Meanwhile, enterprise and CSP services are best suited for encrypting and controlling access to sensitive data in IaaS environments. There are variations of the above approaches, but understanding their core differences will enable organizations to choose the one best suited to their business and technology requirements.
There’s a real dichotomy at work when it comes to managing IT assets in health care. So says John Delano, the vice president and chief information officer at INTEGRIS Health, Oklahoma’s largest health system – with nine hospitals and several doctors’ clinics and home health agencies throughout the state. Delano sees directives flying in two different directions: on the one hand to make information systems more accessible and on the other, to make them more secure.

“Over the next couple of years, there will be a shift in priorities [where health care organizations] will be more focused on patient safety,” predicts McLaughlin. And, this will apply not only to making certain the proper drug is being dispensed, but that patient records are kept safe and properly maintained. He says this will come as the result of increased enforcement, as well as increased patient demand.

“Health care organizations have so many challenges,” says John Kindervag, principal analyst for Forrester Research, “including some significant cultural challenges.” As Kindervag sees it, many health care organizations have done the bare minimum, or less, for the past decade in complying with the Health Insurance Portability and Accountability Act (HIPAA) and the subsequent Health Information Technology for Economic and Clinical Health Act (HITECH), even as the U.S. Department of Health and Human Services (HHS) steps up enforcement of violators with fines of up to $1.5 million per offense (see sidebar on pg. 25).

“The thinking has been, ‘We’re not going to do anything till someone gets fined,’” says Kindervag. “Health care, overall, has been a laggard in [IT] security.”

Now faced with what Kindervag calls a “triple whammy of compliance,” brought on by the corporate health care curve to manage IT assets, as it has policies and procedures in place in case of an incident. The system is set up to routinely assess risk and use encryption products. However, for many health care bodies, the conflicting demands of digitizing patient records and supporting mobile and cloud technologies – while complying with intensifying regulations that require more regular risk assessment – broadens the scope of the circles they need to keep secure. Plus, all this must be attended to while staying focused on the primary objective: caring for patients.

Health providers have pressing reasons to now embrace security, says INTEGRIS Health’s John Delano. Karen Epper Hoffman reports.
HIPAA Omnibus Final Rule, which takes effect on Sept. 23, industry observers say that hospitals and other health care organizations can range widely, especial-
ly of security sophistication of health care
organization. She points out that the level
a Washington D.C.-based advocacy orga-
nization. For Democracy and Technology (CDT),
part of a more global environment than
organizations must find some way to better
effect on Sept. 23, industry observers
HIPAA
Health care
president of ID Experts.
baseline: improving the outlook
What can health care organizations do to
lessen their risk of security issues? Our
industry experts weigh in:
Use encryption
HIPAA security rules recommend the use of
cryptography, but do not outright mandate it.
Still, vendors and industry-on-lookers say that
more health care organizations should embrace encryption as more of their information is going mobile and mov-
ing to the cloud. John Delano, VP and CIO at
INTEGRIS Health, says his health care sys-
tem uses encryption products for its laptops.
“The encryption of data provides you safe
harbor,” adds Rick Kam, president of ID Experts.
It should be a regular part of your internal
reviews, like a financial audit.”
Daniel Berger, CEO of RedSpin, an IT
security assessment company, agrees. “It all
starts with a security analysis,” he says. “You
have to do that baseline. But also remember
that you need to process the results. They
have a shelf life and an expiration date.”
Seek more input from the C-suite
Hospital boards and top executives do not
often concern themselves with the work-
ings of securing their information assets,
but maybe it’s time they did, according to
industry observers.
“Board trustees and chief executives need
to be inquiring and informed about security
readiness and roles,” says Larose, adding
that given the expanding role of security
and the increase of data breaches, this needs to
be a boardroom issue.
Health System, says that because his is an
academic medical center, the structure is
different. “We benefit from more sophis-
ticated security professionals and have
much larger and more diverse networks.”
Still, he says, the biggest risk is the
sheer diversity of its networks. “It’s
difficult to unpack all the different pro-
cesses,” Lacey says. However, he says the
health care industry is making strides in
pulling together its clinical and billing
applications, consolidating systems and
applications in a way that will make
them more accessible to physicians and
care providers. “We’re reducing a lot of
complexity and incompatibility…which is
most encouraging,” he says. Embracing new technologies, as well as
streamlining legacy systems, is becom-
ing increasingly important to health care
organizations, according to a late 2011
survey of 1,000 U.S. adults by PeiC’s
Health Research Institute. Twenty-eight
percent of those polled said they would
select a health care provider that offered
online doctors and nurse practitioners that
did not, and 17 percent said that whether
the facility offered an electronic health
record would affect their decision. Fur-
ther, health care organizations may need
to consider the impact of Facebook and
Twitter on their information, as almost
one-third of all respondents, including
half of those under 35, say they have used
social media for health care reasons.
One of the most challenging aspects of the
HITECH Act has been that patients
now have the right to obtain a copy of
their data in the format of their choice, or
even ask a provider to transmit the data to
a third party that they identify, says Bar-
bara Bennett, partner in the privacy and
information management group at Hogan
Lovells, an international law firm.
“There’s a lot of deference to the
patient’s choice,” Bennett says. “This
raises the issue of security: If a patient
wants you to email their medical record
to a friend or their aunt or Facebook,
how do you do that securely?”
Daniel Berger, CEO of RedSpin, an IT
security assessment company, says that
in the face of increasing technological
and regulatory demands, the health care sector
has gone from being 10 percent of his busi-
ness three years ago to representing more
than 70 percent of his client base now.
“The HITECH Act drove a great need for
security,” he says. “It breathed new life into
the HIPAA security rule.”
Under the HITECH Act, health care
organizations are incented to implement
electronic health records (EHRs) – a
change that will make patient information
more easily portable and accessible. But,
as Berger points out, this step also makes
this sensitive data much more concentrat-
ed and potentially susceptible to hackers.
Larry Warnock, CEO of Gazzang, a
cloud and Big Data security vendor for
health care, says hospitals have been “nervous” about leveraging technolo-
gies like cloud computing. But as the
pressure mounts for health care organi-
zations to make their information both
more portable and more secure,
Warnock says more of them will come
to embracing these technologies.
“Very few health care companies use
their IT department as a differentiator,”
says Warnock. “That will change.”
Our most difficult challenge
In fact, health care IT has already
undergone significant change. Perhaps
the most rapid and challenging, as well
as beneficial, has been the expansion of
mobile device use.
“A year ago, health care companies
were talking about the potential use of
mobile,” says Berger, commenting on the
speed with which it’s taken hold, “and
now smartphones are everywhere.”
But, Delano of INTEGRIS Health
warns that the move to mobility is an
anxiety producer for those charged with
keeping data secure. “Security is hard
enough as it is. Now having to extend
the reach of that data becomes this
whole new challenge.” Before the advent
of mobile and cloud, health care compa-
nies focused on building up a perimeter
defense around the centralized informa-
tion assets, he says. With mobile devices,
the data is moving and the same security
approaches don’t hold water.
Providing security for a mobile network
can be particularly challenging
when hospital staff – or physicians who
have access to the facility, but are not
hospital employees – bring in their own
devices. Delano says INTEGRIS still
tries to “centralize as much as we can,”
but he admits its hospitals have struggled with
causing providers to use their own devices
to access the network.
As a result, INTEGRIS established
both a guest network for patients to
access the internet and a separate affili-
aties’ network for doctors to reach patient
and hospital system data. Delano says his
team continues assessing the risk, as
more and more care providers make use
of tablets, laptops and smartphones.
Nonetheless, given the rising tide of
mobile, 81 percent of health care orga-
nizations are permitting doctors to use
their own devices, according to Kam’s
research. Unfortunately, he also found
that more than half of those organiza-
June 2012
Alaska Department of Health and
Social Services
Settlement: $1.7 million
What happened? The hefty settlement
price tag was based on the number of
victims – at least 500 – but by the state
agency’s alleged shoddy information secu-
rity practices it had in place.
Jan. 2013
The Hospice of North Idaho (HONI)
Settlement: $50,000
What happened? The settlement stems
from a June 2010 incident when an unen-
crypted laptop containing the electronic
protected health information (ePHI) of
441 patients was stolen from an employ-
eer’s vehicle.
Health care

FOllOW the RUleS: Hop on the (omni)bus

For health care providers already struggling to keep their systems secure, things are about to get somewhat more complicated.

The HIPAA Omnibus Final Rule, published by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in late January, represents sweeping regulation that will modify and, in most cases, beef up past HIPAA rules regarding privacy, security and enforcement, breach notification and business associates (or vendors) of health care organizations. The final rule takes effect on Sept. 23.

In particular, the expanded definition of business associate – one that creates, receives, maintains or transmits personal health care information on behalf of a covered entity – means the many vendors, and even subcontractors, to the health care industry will have the same liability as their health care industry customers, and will need to comply with HIPAA rules.

“This covers everything from document destruction to technology services to auditing,” says Barbara Bennett, a partner in the privacy and information management group at Hogan Lovells, an international law firm. “If you’re providing a service with access to medical records, you’re a business associate.”

Not only does this make these firms subject to enforcement under by the HHS, but they are more likely to be held liable in private lawsuits involving information.

And, even for large health systems, that IT budget is typically tiny relative to other industries, she adds.

In a recent survey from the Health Care Information and Management Systems Society, nearly six out of 10 respondents said the portion of IT budget earmarked for information security had increased the year before. However, at an average of just three percent of their IT allocation as a whole, the amount health care organizations spend on IT security is still well below the five to 10 percent spent in other industries.

“It’s still business as usual,” says Kam. “They’re not really taking into account the new threats.” Further, according to recent Ponemon ID Experts research, three out of five health care organizations don’t have a budget appropriate to protect their personal health information.

“It is a problem,” Kam says, “and there are so many pressures to improve health care and reduce costs, and they’re not keeping up on the security side.”

And those security and privacy demands are just going to get more stringent. According to the PwC survey, three out of 10 patients would choose a hospital with clear privacy and security policies over one without if cost, quality and access were the same.

But, as Delano sees it, the cost to provide and manage better security will increase, while typical health care reimbursements to hospitals decline. Therefore, health care IT security executives have their work cut out for them.

“Security is a cat and mouse game,” he adds. “I told the CEO a couple of years ago that my fear is to be sitting in front of the board, and explain why instead of spending a million dollars on a new CT scanner that can generate revenue, we should spend a million on securing a new wireless network.”

“We’re working through it,” Delano plainly admits. “It’s a little bit difficult to achieve.”

A longer version of this article is available on our website, SCMagazine.com

Don’t be anti-social. Follow us.

Our websites, scmagazine.com and scmarketscope.com, combined receive more than 1,000,000 monthly impressions and 80,000 monthly unique visitors. Readers have come to expect timely news, in-depth feature stories, virtual events and industry opinions, and we fully enlist social media to bring our award-winning editorial content to as extensive an audience as possible. Through blog posts, tweets and specialized newsletters, we keep you connected to the pulse of the security industry.
COPY THAT

A groundbreaking copyright infringement case could change the legal role of Canadian ISPs. Danny Bradbury reports.

D

epending on the outcome of a groundbreaking case, Canadian internet service providers (ISPs) may be looking to expand their role in copyright enforcement. The case could soon be clogged with lawsuits brought against alleged illegal file sharers. U.S. movie producer Voltage Pictures has the IP addresses of up to a million Canadians who it says have been illegally distributing its content using the BitTorrent file-sharing service. Now, it wants to know who uses those IP addresses, and it is going to court to get that information.

In November, the company served a legal notice – known as a Norwich order – against the unknown individuals. This order, which is typically used to identify potential defendants, and its counsel discontinued the case.

Why is all this coming up again now? “Some suspect that they pulled the plug [in 2011] because they wanted to avoid confusion about which legal rules applied,” says Fewer. “Perhaps they want to do it clearly under the new law.”

That new law is Bill C-11, otherwise known as the Copyright Modernisation Act (CMA). The Canadian government passed it in November, just as Voltage filed its Norwich order. The CMA is important because it clearly states for the first time what ISPs are liable for when their customers allegedly act illegally. It says that ISPs do not infringe copyright simply by providing the means for telecommunications and reproduction.

This is something that has always been enshrined in common law, says Rob Geist, a law professor at the University of Ottawa, who helps the Canada research chair in internet and e-commerce law.

ISPs may not be liable for the actions of their users, but this case will help to decide how they are required to act when copyright holders decide that their customers have violated their intellectual property. Geist says.

It is not surprising, then, that other litigants are already lining up to try the same thing as Voltage. Another case, involving movie company NGN Prima Productions, is waiting in the wings. In that case, which also involves the privacy consulting company, NGN is asking another ISP, Distributel, for customer records. The NGN case, however, won’t come to court until the TekSavvy suit is resolved, and litigants gain some clarity on the issue.

With the date set for the hearing of Voltage’s motion on June 25, it won’t be long, though, before the legal ball starts rolling.

... none of these cases will turn into court cases...

– David Fewer, executive director, CIPPIC

Legal proceedings

Logan, arguing that the settlement process is encouraged by the courts in Canada. But, he adds, Voltage and its legal team are prepared to go straight to trial.

So, will we see the Canadian courts congested with lawsuits against thousands of Canadians? It’s unlikely, says David Fewer, executive director of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), which has stepped in to help TekSavvy fight the case. “I would predict that none of these cases will turn into court cases because it costs Voltage money,” he argues.

Fewer says that whatever Voltage asks for will be far more than it has lost. The law caps the individual liability for copyright infringement at $5,000, with a minimum of $100. He doesn’t believe that people should have to pay any more than about $50 – and that the litigators should perhaps throw in a free DVD as well.

Blocked by the court

This isn’t the first time that copyright owners have tried to gain access to Canadian internet users’ details. In 2005, the courts issued a decision in a case brought by BMG Canada and other copyright holders against Shaw, Rogers, Bell Canada, Telus and Vidotron, all of which provide internet services to Canadian citizens. The copyright holders wanted information on alleged file sharers, but the Federal Court of Appeal considered it a privacy issue under the Personal Information Protection and Electronic Documents Act (PIPEDA). The court ruled that ISPs are not entitled to voluntarily disclose personal information without the customer’s consent or pursuant to a court order. The court asked for more evidence, calling the evidence submitted by both sides “inadequate.”

Voltage Pictures has also been to Canadian court in the past. In 2011, it asked for customers’ private information from ISPs, including Videotron. The ISPs did not oppose the order, which was granted by the courts. However, mysteriously, Voltage failed to identify potential defendants, and its counsel discontinued the case.

Is this an attempt to revive a case that was dropped a couple of years ago? “Some suspect that they pulled the plug [in 2011] because they wanted to avoid confusion about which legal rules applied,” says Fewer. “Perhaps they want to do it clearly under the new law.”

That new law is Bill C-11, otherwise known as the Copyright Modernisation Act (CMA). The Canadian government passed it in November, just as Voltage filed its Norwich order. The CMA is important because it clearly states for the first time what ISPs are liable for when their customers allegedly act illegally. It says that ISPs do not infringe copyright simply by providing the means for telecommunications and reproduction.

This is something that has always been enshrined in common law, says Rob Geist, a law professor at the University of Ottawa, who helps the Canada research chair in internet and e-commerce law.

ISPs may not be liable for the actions of their users, but this case will help to decide how they are required to act when copyright holders decide that their customers have violated their intellectual property. Geist says.

It is not surprising, then, that other litigants are already lining up to try the same thing as Voltage. Another case, involving movie company NGN Prima Productions, is waiting in the wings. In that case, which also involves the privacy consulting company, NGN is asking another ISP, Distributel, for customer records. The NGN case, however, won’t come to court until the TekSavvy suit is resolved, and litigants gain some clarity on the issue.

With the date set for the hearing of Voltage’s motion on June 25, it won’t be long, though, before the legal ball starts rolling.
The ever-increasing use of personal devices has tested enterprise defenses, so plans must be created to meet the challenge, reports James Hale.

"If you look at the reality of the bring-your-own-device (BYOD) trend. Just step into any corporate elevator and look around: All eyes are down, thumbs and fingers working, from the young clerk with the nose stud to the senior sales executive with the 5600 wristgits. You know the company can’t possibly issue every employee a smartphone or tablet, but everyone seems to have one, and they’re all using them on the job."

“IT security professionals agree on some basic principles until we can do that well,” Johnson says. “A mobile data management (MDM) plan is critical.”

"The analogy I like to use is that we’re at the same place we were 15 years ago with internet access,” says Dave Amsler, president and chief information officer at Foreground Security, based in Lake Mary, Fla. “Suddenly, companies were amazed at how productive everyone became when they gave them network access. Security was an afterthought, and if you asked them about it, they’d say, ‘Oh, we have anti-virus software installed.’ Today, we’d laugh at that, but that’s where we are with mobile security.”

Khan of TwelveDot Security, who has provided security analysis in 36 countries, agrees, and says organizations’ security oversight must extend to app development. “Every new OS poses a security risk because of what comes with it.”

He advises clients to study the beta versions of new apps that employees might use on mobile devices, analyze the application programming interface and reflect findings in MDM plans and mobile application management (MDA) solutions.

Privacy agreements — and laws — are yet another concern. The further organizations reach into employees’ devices, the greater the risk of collecting personal data and violating the individual freedoms of device owners and their family members.

“Personally, I’d have qualms about giving an employer full access to my device,” says Johnson. “Employees are justifiably skeptical, unless there’s a ‘sandbox’ around the corporate data on their phones or tablets.”

He says this type of data partitioning, like BlackBerry now offers on its phones, will increase the possibility for employees to have what he calls “multiple-personality” devices. “We’ll continue to face limitations until we can do that well,” Johnson says. “As things change, it’s a reality with which we continue to struggle. We have to be flexible about personal devices. That’s an important part of hiring and employee retention in today’s society.”

That’s no less a reality for organizations with a fraction of John Deere’s resources.

“Most of those small- and medium-sized enterprises (SMEs) are flying blind,” says Andrew Jaquith, chief technology officer and senior vice president of SilverSky, a Milford, Conn.-based cloud security solutions provider. “The big thing they’re wrestling with is they don’t have a security department with a lot of tools. They know the problems in a general sense, but they lack depth of expertise.”

What’s more, he says, the benefits of having fewer employees to worry about are overbalanced by new generations of devices, new apps and cloud storage, which are all multiplying the risks. For SMEs to effectively deal with the ever-changing face of BYOD, Jaquith recommends keeping it simple.

“They have to stress the basics, like having a strong mobile policy in place and ensuring that employees buy into it,” he says. “Encrypt email and calendars, something that’s pretty easy to accomplish on BlackBerry and iOS. With a smaller company, it’s also easier to control what types of devices are on the network.”

Past those basics, Jaquith suggests SMEs take a hard look at how to manage sensitive data, use mobile tools like content lockers, and pay close attention to how MDM plans are developed.

“We’re in a foundation stage with a lot of stuff around BYOD,” he says. “As an organization, regardless of size, what you do now will make a big difference in the future.”
Advanced attacks

**SUSPECT EVERYTHING**

Are there ways to catch sophisticated malware that hides in trusted processes and services? Deb Radcliffe finds out.

Despite their investments in end-point security systems, organizations are waking up to the ugly truth that they are nearly blind when it comes to advanced attacks and malware lurking in their networks.

“The million-dollar question is: ‘How do you know if you have an advanced threat in your network?’” asks Doug Powell, chair of the critical infrastructure working group for ASIS, an international alliance of security professionals with 38,000 members, and manager of security, privacy and safety at Vancouver, British Columbia-based BC Hydro, which operates 31 hydroelectric facilities with 38,000 members, and manager of security, privacy and safety at Vancouver, British Columbia-based BC Hydro, which operates 31 hydroelectric facilities and three thermal generating plants.

In a February report by NSS Labs, 69 percent of the leading intrusion prevention system (IPS) and network gateway firewalls failed to detect the top three exploits thrown at them—in most cases, multiple devices failed to protect against a single exploit. Another survey, released in February by SafeNet, reveals that 95 percent of 230 security professionals continue making the same investments, even though 55 percent of them believed new attack vectors are being made in the wrong technologies.

“All your garden variety of controls and sensors are not going to catch today’s advanced, evasive threats,” says Steve Hanna, distinguished engineer with Juniper Networks, a Sunnyvale, Calif.-based manufacturer of networking equipment, and co-chair of the Trusted Computing Group’s Trusted Network Connect Group. “Look at Stuxnet, Flame or Aurora,” he says. “Even security products are vulnerable to advanced toolkits like these.”

What comes down to it, says Powell, is connecting the right architectures and processes to capture incidents with more sophisticated, real-time data analysis.

“You can’t just rely on your IPS and your security information and event management (SIEM) solutions to catch advanced attacks occurring somewhere in your network,” says Powell. “You need to know the value of your assets, the motivation of the attacker and, as importantly, you need to know how to interpret data for signs of trouble, while filtering out data that is just background noise.”

**All in the details**

With advanced attacks, the differences between good and bad activity are so minute that the small details needed to connect the dots and determine malicious behavior cannot be captured by most of the security software running on networks and endpoints today, says Darren Hayes, computer information systems program chair and assistant professor at Pace University’s Seidenberg School of Computer Science and Information Systems in New York.

“The differences that an investigator must pick up on are so slight,” he says. “There was a case in which a company had been owned for five years without its knowledge. Once alerted by the FBI to the breach, forensic investigators found the evidence hiding in Dynamic Link Library, or DLL, files associated with the company’s Windows machines.”

The dropped-in DLL files looked legit, so detection tools couldn’t catch them, he adds. However, the tipoff was that this data was all in the wrong version of what the Windows system should be using. That version discrepancy was the smoking gun needed to track and remediate the impacted devices and applications.

However, if it weren’t for an outside agency alerting that company to the problem, its network could have been owned indefinitely. Indeed, according to a Ponemon survey of 3,329 IT/security professionals, the average time it takes to detect an advanced attack in the network is 80 days, and another 123 days to resolve the compromise.

In other words, knowing there’s a problem in order to launch a discovery investigation is still the 800-pound gorilla in the room, calling for highly specialized skillsets to know where to look for signs of trouble in approved operations and traffic.

It is equally important to determine the value of internal systems and data to understand the motivation of the attacker, says Rick Holland, senior analyst with Forrester, a New York-based global research and advisory firm.

Thinking like the bad guys will help organizations understand how advanced attackers will try and penetrate systems, what data they’d like to siphon out, and where they may attempt to hide.

“Ideally, organizations should be able to plug in tactics, techniques and procedures of the bad guys, and search their environment for these indicators,” Holland says. “This should be as easy as reaching out for a menu option of threat intelligence shared securely among peers.”

These details should cross the boundaries between physical and technical operations, adds Powell.

**THREAT INTEL: Standardizing?**

To understand and react to live attacks in as close to real time as possible, threat intelligence being developed by analytics and SIEM vendors will need standards so that the information can be shared and processed across disparate systems. Ten such standards produced by the Mitre Group are getting legs in the community.

These are:

- ** Structural Threat Information eXpresion (STIX):** stix.mitre.org, which includes

- **CAPAC**

- **Common Attack Pattern Enumeration and Classification (CAPAC)**

- **Standardizing the syntax for sharing a whole ecosystem of deeper threat information will help support legal contracts and the technical implementation of alerting and searching technologies used to protect enterprises,” says Robert Martin, head of outreach for the information technology directorate at Mitre. **You can’t just rely on your IPS and SIEM solutions...**

—Doug Powell, BC Hydro
There are steps security pros can take to achieve greater peace of mind with cloud implementations, reports Alan Earls.

Cloud providers

I f one went strictly by the numbers, it would seem that there’s no looking back for the cloud. According to Gartner, the public cloud services market is forecast to grow 18.5 percent this year, compared to the 4.2 percent rise for worldwide IT spending.

But talk to a security professional, and they’ll tell that the cloud model presents real vulnerabilities that require effort and focus to bake in defenses.

According to many cloud and security practitioners, those worries are not inappropriate. While the cloud can be safe and secure, it also opens many vulnerabilities. The key is understanding those weaknesses – the issues one’s operations bring and those inherent to the provider – and then assessing how cloud might help or hurt.

As worrisome as the cloud may be, practitioners say it can be made less risky with some relatively simple safeguards. For instance, says Trey Keifer, president and CEO of WireFarbor Security, a Chicago-based provider of IT risk management solutions, two things are critically important in verifying the security of a cloud provider.

First, he says, designate a person or team with the responsibility. “Too many companies just integrate it into a part of their IS/IT organization, and it falls by the wayside,” he says. So, having a dedicated supplier risk governance group that is both responsible for the initial verification and then any annual follow-up is key. Second, Keifer says, users should ensure that the provider has undergone an independent third-party technical assessment. “You should not trust your internal security teams or a checklist audit of controls. “Make the provider show you a client-facing copy of their reviews,” says Keifer.

He says the “good ones” almost always will have one available, because they get asked for them all the time. And, he recommends avoiding companies that refuse to provide a review because they claim it is confidential information. “This is a smoke screen for poor operational security, or a network that has grown beyond their ability to control,” he says. Michael Bremmer, CEO of TelecomQuotes.com, an internet and telephone consulting company, offers his own cheat sheet for vetting cloud providers that picks up on Keifer’s themes. Specifically, Bremmer recommends inquiring about which certifications one’s cloud data center has – SOC I, II or III; SOC III is the best, most comprehensive and most expensive certification, says Bremmer, adding that SSA 50 TPE II is acceptable, but is not a true data center certification. “It is a 20-year-old auditing standard that was never designed to be used for data centers,” he says.

Rules to live by

But the outlook isn’t completely bleak. As worrisome as the cloud may be, practitioners say it can be made less risky with some relatively simple safeguards.

For instance, says Trey Keifer, president and CEO of WireFarbor Security, a Chicago-based provider of IT risk management solutions, two companies found out the hard way, in the wake of Hurricane Sandy, that their data wasn’t housed in multiple locations. Although Bremmer admits off-site storage “isn’t usually free,” compared to the potential cost of data loss it may be a bargain.

“Assuming that physically secure the facility is another step shoppers must take, as this type of protection also matters. "If possible, ask for a tour and use your own eyes,” Bremmer says. If you cannot have a tour of the facility you’re considering putting your data into, that should be a red flag."
Cloud providers

Many businesses are subject to specific security requirements...

– Andy Maier, senior product manager, Savvisdirect

One’s hat and reputation on a stack of certification documents don’t guarantee job security, customer confidence or security. Maier warns.

Instead, Maier offers a range of suggestions, including figuring out what data needs to be encrypted in the cloud that isn’t already. Also, he says, it is wise to determine if existing monitoring solutions can be integrated with what kind of mitigation help a provider offers. Does the cloud vendor have a DDoS prevention solution, for example? “Information security alone shouldn’t be the only concern,” says Maier. “If you take all the steps of the best security experts, but implement a brittle deployment, lost transactions and custom records could still result in the ruin of your business.”

Cloud Security Alliance: First step into the cloud

The Cloud Security Alliance (CSA), a nonprofit that promotes cloud security best practices, suggests organizations use the Cloud Security Readiness Tool (CSRT), a free offering from Microsoft designed to help companies review and understand their IT maturity level and their ability to consider adopting or growing cloud services. According to a CSA statement, the tool uses the Cloud Control Matrix (CCM) to consider data security, privacy and reliability factors, as well as key compliance and regulatory standards. The tool is a simple way to adopt the CSA’s Security, Trust, and Assurance Registry (STAR) and CCM principles.

The tool helps organizations evaluate their IT potential and learn how they can adopt cloud services to reduce the overall cost of their operation. Organizations that are considering transitioning to the cloud are faced with common decision difficulties, most of which relates to a lack of understanding about the technology. The CSRT is an interactive survey of 27 questions that draw out information about an organization’s industry and the maturity level of its current IT infrastructure. The tool uses this information to provide relevant guidance in a custom report that helps organizations better understand their IT capabilities and more easily evaluate cloud services against critical areas and compliance with common industry standards.

Information from more than 800 organizations that have used the CSRT shows that only a few of them are well prepared for cloud adoption. For example, 25 percent of organizations in the banking and financial sector have embraced a formalized security program. A CCM control validates whether an organization has an information security program. A tool like the CSRT helps organizations better understand the full potential of embracing the STAR and the CCM.

“Organizations are often at a loss when it comes to how to go about determining which cloud services may be of value and whether deploying cloud services are appropriate in their environment,” says John Howe, CIO of the CSA. “We hope this tool becomes every organization’s first step into the cloud.”

Product Section

SIEM City

This month we look at security information and event management (SIEM) tools. The history of this product group is as interesting as that of last month’s UTMs. SIEMs evolved from security event management (SEM) tools. However, today’s SIEMs are a lot more than just event managers. The products that we are seeing are really a combination of log management, event and flow correlation, and cyber situational awareness.

That’s really an important distinction, by the way, as cyber situational awareness is the cornerstone of event management. The SIEM takes in data from wherever it can get it and correlates the input according to rules set up by the organization. Often this means that the SIEM has to take device inventory, vulnerability testing and flow data into account, as well as event data from firewalls, system logs and intrusion detection systems. This means that, in a perfect world, at least, every device on the enterprise is potentially a sensor for the SIEM. However, these tools are no better than the sensors attached to them. That means that when selecting a SEM, users should be certain that the device selected can take input from everything on the enterprise network from which security information must be gathered. In the case of a SIEM, the more data points it can look at, the better job it will do. And what, exactly, is the SIEM’s job?

SIEMs are often thought of as alerting tools for large, complicated networks. That is, certainly, one extremely important facet of what it is all about. But there is a lot more. The biggest additional task that a competent SIEM will perform is forensic in nature. Because the SIEM probably is the only thing that sees everything on the enterprise, it has great potential to assist in the forensic reconstruction of a security event.

Probably the biggest barrier to deploying a SIEM in a smaller organization, besides cost, is lack of sensors. Since these offerings don’t usually generate their own data, lack of sensors is a drawback. Those that accept data from a variety of sources—including events and flow data, as well as vulnerabilities and inventory—can generate risk profiles. If we think of the events as threat data and the vulnerabilities as vulnerability data, we have the two main types of data that define risk.

So, with that we’ll launch into our product reviews. We have a good crop this month, so please read on. – Peter Stephenson, technology editor

How we test and score the products

Our testing team includes SC 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 pre-determined 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.

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.

What the recognition means

Best Buy for the Product SC Labs 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 Labs environment, and which will be used subsequently in our test bench for the coming year.
SIEM

What goes into a SIEM these days is not quite so well-defined, but basically these tools aggregate network activity into a single addressable dataset, says Peter Stephenson, technology editor.

Since the term security information and event management, or SIEM, was coined by Gartner in 2005 there have been a lot of changes in what constitutes a SIEM product. Originally, the acronym was a combination of security information management (SIM) and security event management (SEM). This was presumably fairly straightforward. Today, a scant eight years later, what goes into a SIEM is not quite so well-defined.

According to Gartner, a SIEM should have the abilities of “gathering, analyzing and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating systems, database and application logs; and external threat data.” That seems pretty broad, but actually it comes down to some pretty specific requirements.

In order for a SIEM to work, it needs data. It gets its data from a wide variety of sources that we can think of as sensors. However, all of this data needs to be aggregated into a single addressable dataset. SIEMS do that. Then, they correlate the aggregated data to make sense of it. That includes normalizing disparate data formats into a single form that can be consumed by the analysis engine of the SIEM.

Once the data is correlated, there is a lot that can be done with it. First, of course, is that it can alert to security conditions that need addressing immediately. In this regard it is sort of an intrusion detection system (IDS) on steroids. It is receiving data from lots of sources and each of those sources is contributing to the picture the tool sees. How that picture is interpreted should be, in large measure, configurable. Most capable SIEMs have robust policy engines that allow customization, but also have many commonly used policies available right out of the box.

Second, the data can be used for reporting. Reporting is a critical aspect of regulatory compliance. It also allows administrators to see what the SIEM sees broken down into meaningful charts and graphs. Reporting can be file- or paper-based or it can be real-time displays useful for analysis.

Analysis is another important aspect of the SIEM. In the early days of these solutions, they were much better for analysis than they were for compliance reporting. Today, SIEMs should be able to create regulatory compliance-specific reports. Because these offerings often can take vulnerability data from tools such as Nessus, they have the ability to calculate IT risk. The data that comes from various sensors is threat data and this is the meat and potatoes of the classic SIEM.

However, risk is a combination of threats and vulnerabilities, so when the SIEM takes vulnerability data as well as threat data, there is the potential for risk measurement.

Developing a risk picture, however, is not quite that simple. If we look at the enterprise on an asset-by-asset basis, we find that some assets are more critical or sensitive than others. So, for a credible risk picture, the SIEM must not only be able to take both threat and vulnerability data, it must be able to parse down to the asset level. And, from there it must be able to weigh assets based on sensitivity, criticality or both.

Further, SIEMs retain data in a variety of ways. Some keep entire logs, and their drill-down capabilities let administrators go all the way to the source files. Some retain metadata parsed from the logs. In that case, drill-down usually gets header information and that is all. The tradeoff is the space required for archiving full logs.

While SIEMs are not inexpensive, prices have come down over the past few years. When selecting a SIEM, don’t judge cost of ownership based solely on price. The most important metric is the value in your environment.

The number and types of sensors are the only criteria to consider. Where the data is being collected on the enterprise is critically important. Also, it is useful to be able to feed flow data into the SIEM. This provides data flow vectors that help identify paths that attackers or malware take.

Specifications for SIEM tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Performs log collection</th>
<th>Performs event correlation</th>
<th>Allows for forensic analysis of log data</th>
<th>Includes predefined alert templates</th>
<th>Includes predefined compliance templates</th>
<th>Includes predefined report templates</th>
<th>Uses agents for log collection</th>
<th>Agentless log collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlienVault Unified Security Management v4.1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>BlackStratus LOG Stem v4.2.0.45</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CorreLog Enterprise Server v5.2.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>eQ Networks SecureVUE v3.6.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>EventTracker v7.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>GFI EventsManager 2013</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>HP ArcSight Express v3.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>LogRhythm 6.1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>McAfee Enterprise Security Manager v9.1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>NetIQ Sentinel v7</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SolarWinds Log &amp; Event Manager v5.5</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>ZOHO ManageEngine EventLog Analyzer v8</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
**Verdict**

This is a quality product with great potential.

**Weaknesses**

There is a need for more prepared policies and reports to help non-expert users.

**Strengths**

Simple to use as well as a large list of agent modules.

**Details**

**Vendor** BlackStratus

**Price** Starts at $9,000. LOG Storm is available in three different virtualized models—five of them being free—and four different hardware models with varied memory and storage capacities. Perpetual licensing and flexible subscription pricing is offered.

**Contact** blackstratus.com

**Features**

Ease of use ★★★★★

Performance ★★★★★

Documentation ★★★★★

Support ★★★★★

Value for money ★★★★★

**OVERALL RATING** ★★★★★

**Strengths**

Flexibility, quality and ease of use.

**Weaknesses**

Application setup can be a little challenging and the documentation could be better.

**Verdict**

Very good product.

---

**AlienVault Unified Security Management (AV-USM) v4.1**

AlienVault’s Unified Security Management (AV-USM) platform combines open source technologies for asset discovery/inventory, vulnerability assessment, threat detection, behavioral monitoring and security intelligence/event correlation. The AV-USM “All-in-One” appliance includes sensor log collection and event detection systems, IDS, Incendio information, Microsoft Windows events, and more. Another component, the AlienVault Logger, provides forensic storage, while the USM Server/Siem engine provides aggregation, correlation and real-time alerts for incident response, along with dashboards and reporting.

For more distributed and complex environments, the All-in-One appliance can be remotely upgraded via license code to support up to five remote sensors. Additional, any one of these components can be configured on dedicated hardware appliances for scalability and deployment flexibility. In addition to the built in asset discovery, vulnerability assessment, behavioral monitoring and threat detection, AlienVault offers an open API to integrate additional data sources and vendor devices.

During our initial attempt to access the AlienVault hardware appliance, the hardware failed. The support staff worked to identify the situation and then AlienVault shipped a replacement in less than 18 hours. AlienVault provided a copy of its standard contract, a document that detailed the appliance configuration and a CD-ROM that included a “quick-start guide” and a copy of the end-user license agreement. The product is based on a number of well-respected open source products. These include, but are not limited to, Snort, Nessus, Nmap, Nagios, OTX (Open Threat Exchange), OSSIM (Open Source Security Information Management), and more. The product contains approximately 15,000 signatures to identify risk. The case management workflow is relatively simple. Incidents are identified, a ticket is opened and sent to an investigator or an analyst. The list-supported system is impressive. The AlienVault was the first product that auto-generated an incident ticket during the start-up phase of initializing the product.

The reporting function provides an interesting feature. When a report is being generated, the user is presented with a number of options regarding the format of the document. No cryptic formatting language is required. The drop-downs and radio-button selections allow a facet report to be created all in a few seconds. The “Situational Awareness” function allows graphical representations of the assets, including graphic views of systems up/down status.

Fee-based support offerings include standard assistance beginning at $3,540 for eight hours a day/five days a week phone and email aid. Additional assistance is available that includes 24/7/365 support for $4,425 per year. AlienVault provides other help functions as well: a knowledge base includes video tutorials, product documentation and more. There is a forum that can be reached on the company’s website, as well as some FAQ documents.

This product is a good value for the price given its performance, functionality and presentation.

---

**BlackStratus LOG Storm v4.2.0.45**

LOG Storm combines log management and security information management with correlation technology, real-time alerting, monitoring and an integrated incident response system. The tool analyzes all event messages to identify patterns of attack, filters out false positives and prioritizes critical events. Incident information is accessible from nearly all screens within the LOG Storm GUI.

This product improves the quality of alerts by incorporating vulnerability data into its correlation technology—allowing alert administrators to better determine if the monitored assets are vulnerable to certain threats. Another interesting feature is its behavior-based analytics adding in the identification of new attacks that follow similar patterns to past attacks, but use different types of connections that attempt to bypass signature-based countermeasures.

The workflow management functions provide best-practice recommendations for remediation, mitigation, centralized case tracking and automated notification, so incident response personnel know what to do and administrators have clear insight into the actions of their team. LOG Storm provides an array of reports to aid in investigating incidents and preparing for audits, including the standard compliance package.

LOG Storm was delivered to our lab as an appliance, along with “Initial Setup” and “Quick-Start” guides. Following the instructions provided by BlackStratus made the application configuration go well. Identifying networks and registering assets was simple. Adding systems and devices was straightforward, and we were impressed with the list of agent types that were available. The dashboard was fairly easy to navigate. It took some time to learn the features under each tab. The help function was easy to read and the instructions for most tasks were simple to follow. There was a bit of trouble trying to create the desired “Custom Rules” to use for the testing. We did not find a way to create keywords inside the rules. The intention was to generate an alert trigger and an incident for detection of common hacker tools that were downloaded and used on the network. However, it should be noted that the “System Rules” were easy to set up and modify.

Support is divided into multiple tiers beginning with 24/7/365 no-cost service during the product’s trial period. Pay for services options include three levels: platinum, gold and standard. All three include virtual helpdesk and troubleshooting information online, software and signature updates, expert help for managing security incidents, and delivery of new agents as they become available. Platinum provides 24/7/365 live phone support; gold provides 9 a.m. to 6 p.m. (EST) live telephone support, seven days; and standard provides 9 a.m. to 6 p.m. live telephone support, Monday to Friday. In addition, BlackStratus provides assistance from the company’s website: a product knowledge base and a FAQ. The costs for the respective options are based on a percentage of the list price: standard: 20 percent; gold: 25 percent; and platinum: 30 percent. Overall, this product is properly priced and a value for an entry point into SIEM.
CorreLog Enterprise Server v5.2.0

CorreLog Enterprise Server combines real-time log management with correlation, auto-learning functions, high-speed search, ticketing and reporting services. This software solution can be installed in minutes on a Windows host platform with at least 312 Mb of memory and sufficient disk space to store log files. CorreLog has the capability to work either independently of, or alongside other SIEM technologies to improve threat management and incident response capabilities. The tool is designed to be as simple as possible to install and operate, and is an excellent entry point into SIEMs for small to mid-sized enterprises as it includes the basic elements of an enterprise-class SIEM.

CorreLog has a fairly unique automated workflow – from event message to correlation to alerts to tickets. The alert functions are auto-learning and intuitive thresholds for simplicity and tracking. Logs/messages are encrypted and hashed to help ensure the data is authentic. Another winning feature is the full scripting facility to launch functions and third-party applications. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI-DSS, HIPAA, GLBA, FISMA, GLBA, National Credit Union Administration (NCUA), and others.

CorreLog freely distributes versions of its Windows Agent and Windows Tool Kit (WTS) to instrument Microsoft 200x, XP, Vista and Windows 7 platforms with standard syslog capability. This non-intrusive, feature-rich, standards-based agent is distributed free of charge to all interested organizations to help advance the state of the art for SIEM and systems management. CorreLog provided a number of printed documents, as well as a collection of 35 PDF documents that covered installation, configuration and operations. Other material provided excellent insight into the philosophy and methodology employed by the company in the development of its CorreLog Enterprise Server. Installation took less than a minute to get the system up and running. Agents were deployed by logging into the target systems and launching the CorreLog Enterprise Server. The installation proceeds quickly and silently, with the only requirement being the admin password.

CorreLog readily adapts to the nature of the offering. In addition to email and phone assistance, the company’s Security Center provides custom-scoped services. The cost of these services are negotiable based on the nature of the offering. In addition to email and phone assistance, the company offers aid on its website, as well as a knowledge base and a FAQ feature. The cost of this tool is higher that many other SIEMs, but it is still money well spent given the quality of features and services.

eIQnetworks SecureVue v3.6.3

SecureVue provides all of the elements one would expect in a SIEM – log consolidation, threat correlation, incident management (including ticket issuance), event analytics, forensic analysis, compliance reporting, change auditing, event alerting, an array of user definable/customizable alerting and reporting options, and more. SecureVue also provides a friendly incident management workflow that helps keep the process clear and easy to follow. But, this is just the beginning. The performance of the system approaches phenomenal.

The reporting function features a fully indexed proprietary data store that generates near-instantaneous reports. The development of policies and the flexibility of reporting and alerting is intuitive and easy to use. The highly customizable dashboard is excellent, providing clean graphs and tables. SecureVue has a built in software development kit (SDK) to help aggregate data from third-party tools into the SecureVue Server. To aid in installation of SecureVue, a two-page instruction document was provided, presumably since the tool was preconfigured on a hardware appliance. It would have been convenient if there had been a user manual to reference some of the features that are not as common as others. The appliance was connected to dynamic host configuration protocol (DHCP) in the lab, so at startup the only information that was required was the admin password. After logging in to the SecureVue server, time was spent becoming familiar with the settings and options. Simple mail transfer protocol (SMTP) would not accept email setup because the product disallowed special characters in the user ID for SMTP authentication. A number of lab systems were enrolled (via agents) into the SecureVue appliance. This activity took about five minutes per system enrolled. To test the features of the product, a series of progressive network attacks were performed.

This is an industrial strength tool. The dashboards are uncluttered and intuitive. The product comes with approximately 1,500 prepared reports. User-definable reporting is available if one wishes to create something a little different. There is also a robust set of compliance reporting. Account policies are editable for special needs. The company’s Security Center provides change monitoring. Instant reporting is generated on differences from previous snapshots. There are a large number of predefined alerts.

Initial price for support includes one year of maintenance (software upgrades and assistance). Follow-up maintenance is priced at 20 percent annually. eIQnetworks “eCare” support is offered with two possible options: standard (eight-hours-a-day/five-days-a-week) and premium (24/7). In addition, service options (outside of standard) can be purchased. These “consultative” services include implementation, training, health checks and custom-scope services. The cost of these services are negotiable based on the nature of the offering. In addition to email and phone assistance, the company offers aid on its website, as well as a knowledge base and a FAQ feature. The cost of this tool is higher that many other SIEMs, but it is still money well spent given the quality of features and services.
EventTracker Enterprise v7.3

EventTracker Enterprise is comprehensive. It is designed to be scalable to address multiple locations, business units and domains using the EventTracker Stand-Alone, Collection Point and Collection Master architecture. The latest version (7.3) expands/improves the offering in areas of file integrity monitoring, configuration assessment, cloud integration, event correlation and writeable media monitoring and management. Some of the other new features include built-in ticketing system (with acknowledgement, search, notes and email support for log4j) and related standards, such as log4j, log4net, log4php, scheduled discovery of applications and systems, configurable behavior rules to detect new and out of the ordinary behavior by user-specified thresholds, frequency or learned behavior thresholds, and risk-based prioritization for incident identification and automatic or manual remediation solutions.

The product ships via software, virtual appliance and hardware appliance. EventTracker uses a flat file database that is fully indexed for performance and a proprietary compression function that flattens the data 90 percent or more for excellent storage management. The event data is encrypted and hashed to ensure the integrity of the information.

The anonymization feature issues an alert if tampering is attempted. Another strong feature is the integration of Microsoft’s Specialized Security – Limited Functionality (SSFL) hardening option to the EventTracker system. The SSFL was designed to help protect information in hostile environments and is required on certain government systems. EventTracker provided a number of excellent documents to aid in its installation, configuration and use. Most useful were the EventTracker Enterprise v7.3 Install-Guide, Hardening-Guide-For-EventTracker-Server and the EventTracker v7.3 Enterprise User Guide.

The product provided features to facilitate prioritized activity. In addition to the items already noted, after a brief agent enrollment process, the following features were available for viewing and processing: email alerting, remediation, behavior analysis, forensic search, change activity reporting, compliance reports and more. The system provides a risk-based prioritization facility for assets that we found pleasing. One of the most powerful set of features were found under the “Reports” tab, then selecting the “Compliance” tab. Equally rich functional- ity was found under the “Config Assessment” tab. Once this was selected, the “Report” tab was selected. Here, under the “Benchmark” tab, there were a large number of report options. The benchmarks were categorized by publisher and system platforms, and systems were tagged and assessment launched. Once completed, the system reported the Config Assessment results. The Open Vulnerability and Assessment Language (OVAL) results provided excellent references.

EventTracker support is a 24/7 fee-based service, which includes phone and email assistance, a portal via the website, a knowledge base and FAQ. The cost is 20 percent of the software list price. EventTracker also offers product support, design, planning, implementation services and training. This tool hits all of the benchmarks for a top-tier SIEM and is money well spent.

GFI EventsManager 2013

GFI EventsManager collects, centralizes, normalizes, consolidates and analyzes a wide range of log types, such as World Wide Web Consortium (W3C) and any text-based formats, Windows events, SQL Server and Oracle audits, and syslog and simple network management protocol (SNMP) traps generated by devices, such as firewalls, servers, routers, switches, sensors, SQL server systems, PCs and custom devices. GFI EventsManager includes an active network and server monitoring feature providing administrators with real-time, active monitoring of assets, network infrastructure, applications and services. This new functionality enables IT administrators to understand why a problem is occurring, and it also provides information to help remediate it.

EventsManager (like most SIEMs) provides real-time discovery and alerting of security incidents. However, it also provides critical information for risk assessment and mitigation. Administrators have the ability to assign specific computers to each EventsManager user, enabling administrators to limit users’ access to only the configuration, reporting and log-browsing data coming from computers they manage. EventsManager can be deployed in highly distributed environments – even where there is no persistent connection between sites – due to its ability to export data to encrypted files that can be forwarded by secure file transfer applications during times when the network is available. EventsManager includes some fairly unique features, including process debug information generated during process failure dumps, as well as built-in Visual Basic scripting. Other strong features include the use of two-factor access into log data and the use of interna- tion information blocking for privacy.

Documentation provided for this evaluation included administrator, evaluation, installation and smart guides. Each was excellent making the installation and operation tasks easy. GFI EventsManager can be deployed on machines running any Microsoft Windows OS version – from Windows XP SP3 onwards. The install is performed in two stages: Install the database and install EventsManager. GFI recommended installation into the customer’s domain if possible. After firewall settings were enabled, computers were selected (alternative credentials were set for systems not in the domain). GFI did a good job of maintaining the familiar look and feel of other GFI products. During the setup, GFI recommended running scans to generate log events. After creating users and groups, the next task was to open the event processing rules dropdown.

It should be noted that creating or modifying rules is possible but difficult, and GFI recommended working with the prepared rules if possible. The dashboard was intuitive and rich in features. Once the events were imported and normalized, the system was ready for use. Another great asset was the “Ano- nymization” feature. This assists in complying with privacy laws that require personal data be accessible to named individuals. The Anonymizer is used to encrypt the personal data found in Windows Security logs, SQL server and Oracle audit logs. Further, the EventsManager Audit for Windows tracks inactive users, inactive systems within the domain, IPsec policies that are not active, and inactive Microsoft firewalls.
**GROUP TEST | SIEM**

**HP ArcSight Express**

The HP ArcSight Express appliance features a full set of SIEM capabilities, including security event correlation, log management, IT search, NetFlow monitoring and compliance reporting. Using this tool, security professionals and system administrators can identify and investigate many security events and rule violations— all from a single interface. Along with the usual monitoring and reporting functions of a SIEM, this offering also features user activity and role monitoring, which provides a more complete picture of certain security events and how they occurred.

Overall, we had a fairly easy time of configuring and managing this appliance. To get it deployed in the network takes just a few minutes, but getting the product setup and configured is a slightly different story. This product is designed to be quite flexible and to provide a multitude of deployment and monitoring configurations, so setting everything up can be quite a process. However, we found that once it is up and running, it features many powerful analysis and reporting functions that more than balance out the initial deployment difficulty.

This solution has a connector or receiver for almost any type of log or device. It can take all log data, pass it through its powerful correlation engine and, in one interface, provide dozens of reports and alerts. The management console can be a little overwhelming at first due to the many panes of information, but once we became familiar with how to navigate the console we found it to be quite manageable and not as complicated as it looked initially.

We found this appliance to have a slight learning curve when it came to managing and configuration, but it also provides a lot of options and flexibility. For compliance reporting, it features reporting packs that can be loaded into the management console for specific compliance report types.

Documentation included quite a few PDF manuals and guides. Among these were administrator, configuration and user guides. There was also a short getting-started guide, but it basically provided a couple of steps to turn on the appliance for the first time and then referenced the configuration guide for further instructions. Also provided was an ESM 101 guide. This offered excellent detail on how to use the product and its various features and functions.

HP ArcSight offers standard and premium support plans to customers as part of an annual cost. These programs include various levels of phone and email-based technical aid along with other help features. Customers also can access a large support area on the website that features a user community, knowledge base and a download center.

At a price of $45,000, this product carries a heavy price tag. The HP ArcSight appliance is definitely a better fit for large-scale enterprise versus smaller environments. While the price may be high, this product does offer a lot of configurability and functionality for more complex environments. Overall, we find this product to be an average value for the money. It does have some great features and functionality.

---

**LogRhythm**

The LogRhythm appliance goes beyond traditional security event monitoring and management.

This appliance features log and event management functions as with any SIEM, but beyond that it includes advanced correlation and pattern recognition driven by its onboard Advanced Intelligence Engine, and host and file integrity monitoring and drill-down capabilities to get to the raw log data for analysis and forensics.

Overall, we found this product to be easy to set up and manage. The initial setup and deployment of the appliance has changed just slightly, but is still as easy and straightforward as its past appliances that we have seen. To get started with LogRhythm, we had to power on the appliance and allow it to go through a brief initial power-on procedure to set up Windows Server 2008. After the initial start-up process, we were able to set the IP and network settings and we were pretty much done with the initial deployment. All further management is done via a well designed, web-based management interface. We found this to be intuitive to navigate and it includes a multitude of analysis and monitoring tools, including many charts that could be drilled down into for deep event analysis.

This appliance came loaded with monitoring and reporting capabilities. On top of being able to drill down quickly and easily from any event to raw log data, this tool features a lot of automation and compliance reporting functions. The automation aspect includes the LogRhythm SmartResponse, which delivers immediate action on real-world issues, such as when specific cyber threats are detected or compliance-driven policies are violated. This allows for administrators and security managers to focus on the investigation of an incident, rather than trying to plug the hole in a time of crisis. This appliance also came preloaded with a large selection of compliance and predefined reporting templates, making report generation simple and easy right out of the box.

Documentation is included in the web-based management console of the appliance. From the console, administrators can easily access installation and administrator guides for help with advanced configuration or use of product features. We found all documentation to be well-organized and easy to follow, offering much more in-depth manuals and step-by-step instructions.

LogRhythm offers customers 11/3 standard support or 24/7 premium support as part of an annual maintenance contract. Along with phone- and email-based technical assistance, customers also have access to software updates, including major and minor releases and hardware warranty options. Customers also get access to a portal via the website, which includes a knowledge base, user forums, documentation, support tips, downloads and other resources.

At a price of $25,000, we find this product to be an excellent value for the money. LogRhythm is a powerful yet reasonably priced appliance that includes many excellent features and functions onboard right out of the box. Too, along with powerful functionality, this appliance is easy to use and manage, which makes it an all-around good value and investment for any organization looking to deploy SIEM.
McAfee Enterprise Security Manager

The McAfee Enterprise Security Manager is back this year after a full transformation from its former self, the McAfee NitroView ESM. Many of the obvious differences are skin deep, and much of the robustness of the previous product remain intact, including the familiar management console, but more on that shortly. For those who do not know this product, the Enterprise Security Manager is the ultimate high-powered SIEM. This tool uses a proprietary backend database that allows it to collect more than 18,000 events per second from a single receiver and feed them through an advanced correlation engine for deep analysis.

We found this appliance to be quite easy to deploy, configure and manage. The initial deployment is done by manually setting network and IP information on the device through a monitor and keyboard connection. After that, all further management and configuration is done via the web-based management interface. We found the management interface to be easy and intuitive to navigate and to feature many easy-to-read charts and graphs. The dashboard itself is built on Flash, so it can be customized to include information that is relevant to a specific user, such as a security engineer or system administrator. The appliance also comes preloaded with many already configured dashboards.

From a functionality standpoint, this appliance has it all. On top of prebuilt dashboards, many interactive charts and graphs, the ability to take data and logs from almost any source that has an IP address, and the ability to drill down into raw log data quickly and easily, this product also features a multitude of prebuilt compliance reporting tools. The Enterprise Security Manager comes loaded with reports for PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA and SOX, along with several others. Aside from reporting on events after they happen, this product also can help predict threats before they occur. This is done by monitoring and managing a baseline of activity while continuously looking for anomalies.

Documentation included installation and administrator guides in PDF format. The installation guide provided an excellent amount of detail on how to get the appliance up and running, as well as some basic configuration procedures. The user guide focused on overall use and management along with report creation and other tasks. We found all documentation to be well-organized and easy to follow with many step-by-step instructions and screen shots.

McAfee includes the first year of product and technical support as part of the purchase price. After the first year, customers can purchase additional support for $6,994. McAfee includes the first year of product and technical support as part of the purchase price. After the first year, customers can purchase additional support for $6,994.

At a price just shy of $48,000, this product carries a big price tag. However, we find it provides a lot of bang for the buck. The McAfee Enterprise Security Manager is a robust and feature-rich appliance that is easy to use and manage.

NetIQ Sentinel

Sentinel from NetIQ offers a lot of robust SIEM features and functions. This product features log collection, aggregation, correlation and analysis and reporting – all from one single point that is easy to use and manage. Administrators and security personnel can use this tool to gain a great amount of insight into security events, as well as prevent threats that may be unseen without the use of Sentinel’s powerful log correlation engine.

We found this solution to be of average difficulty to set up and deploy. The product comes as a software package that can be installed on either a Microsoft Windows or Enterprise Linux server. NetIQ recommends the Linux deployment, so that is the one we had for evaluation.

Overall, we found the installation to go pretty smoothly. It required minimal Linux experience after installation was complete, we were able to manage the entire product from a web-based management interface. Included in this interface is the Sentinel Control Center, which provides a centralized interface to manage data and analysis of events.

Once we became comfortable navigating around the various dashboards and menus of the appliance interface, we found this product to include a wide variety of reporting and analysis capabilities. This tool includes a fair amount of automation and remediation capabilities as well. Once configured, Sentinel will be able to detect anomalies in the network and event baseline and provide remediation and threat information automatically. Aside from threat monitoring and event management, this product also integrates with identity management platforms to help create a more specific picture of an event by tying in user information and logging. Sentinel also can correlate information from intrusion prevention systems (IPS)/intrusion detection system (IDS) sensors against known vulnerabilities to help identify possible threats before they become a problem.

Documentation included many PDF guides and manuals, including installation and administration guides. Other materials included a quick-start and a user guide. We found all to be nicely organized and to include many step-by-step instructions, along with screen shots. We also found overlap in the manuals, which made finding information on specific configurations easy.

NetIQ offers both 12/5 and 24/7 product support levels to customers as part of an agreement. This includes phone- and email-based technical aid along with access to product and software updates and upgrades. Customers also can access an area on the website at no cost. This includes a knowledge base and other resources. Furthermore, users also can access a full user forum that features many custom-built connectors and helpful information from product users.

At a price of about $48,400 for the software and one year of support, this product is quite costly for a software-only product. We find NetIQ Sentinel to be a slightly above average value for the money. While this tool does carry a monstrous price tag, it also includes a great amount of intelligent features and functions that give it solid SIEM capability, which helps make it worth the overall cost.
SolarWinds Log & Event Manager

The SolarWinds Log & Event Manager, also known as the LEM, is a virtual appliance capable of collecting logs and events from almost any network-connected device and then correlating that data for further analysis. The LEM virtual appliance can be deployed in either a VMware ESX or Microsoft Hyper-V virtual environment and can provide insight into security events, as well as help with performance monitoring and compliance management.

For our evaluation we chose to install the VMware virtual appliance. We found the installation process to be quite easy and straightforward. To get started, we simply had to download the executable from the SolarWinds support site. After the executable was downloaded, we ran it and it expanded into a folder containing the open virtual appliance (OVA) file along with installation instructions and the desktop software for additional management capabilities.

To get the appliance up and running, we simply had to import it into our ESX installation and turn it on. The appliance was able to acquire a Dynamic Host Configuration Protocol (DHCP) address and we were able to log into the web-based management console within minutes of turning the appliance on.

From a management perspective, this appliance has a lot to offer. The first thing we saw when logging into the interface was a full dashboard with many helpful charts, graphs and lists, along with access to help and support. The dashboard can be customized to fit the needs of a specific user type or group, but the default setup is a good place to start. As for reporting, this appliance features a plethora of compliance-based report templates already built in and ready to go. Furthermore, this tool can take data from other SolarWinds products and provide an extra level of analysis to ensure better security.

Documentation included a quick-start guide, along with a full user guide. The quick-start guide detailed the steps necessary to download and install the virtual appliance, as well as some other basic information. The user guide takes over where the quick-start leaves off and details configuration and management of the appliance, as well as use of product features. We found both of these to be clear and easy to follow. They each also included full step-by-step instructions and screen shots.

SolarWinds includes the first year of technical support as part of the purchase price. Customers have access to 24/7 unlimited phone- and email-based technical support, as well as a large aid area on the website. The customer support area includes documentation, product downloads, video tutorials and training materials, and access to a full knowledge base and user forum.

At a price just shy of $4,500 for the virtual appliance and one year of support, we find this offering to be an excellent value for the money. The SolarWinds LEM offers a solid feature set with an easy to navigate interface in a virtual appliance that is simple to deploy and manage at a reasonable price. This solution can be used in almost any environment and is good starting point for SIEM deployment.

Zoho EventLog Analyzer

The ManageEngine EventLog Analyzer from Zoho is a small application that provides a lot of functionality. This product takes an agentless approach to collecting and analyzing machine-generated logs. The tool can collect and normalize event logs and machine data and make them available for analysis, searching, report generation and archiving, all in an easy-to-use, web-based interface.

We found installation to be just about as simple as it gets. The installation executable can be downloaded from the ManageEngine website. Once we had the executable, we ran it on one of our Windows servers and, after a short installation wizard, were up and running. The product itself is quite small and lightweight, so it can sit on almost any hardware. After the install was complete, we were able to access the web-based management interface. We found this interface to be a little overwhelming at first, but after a few minutes of wandering around we felt pretty comfortable using the controls.

Adding assets and log sources is quite easy as well. This product can scan an entire subnet or devices can be added manually. In our Windows domain environment, we just had to provide administrator credentials and scan our subnet and we were collecting data in minutes. As for analysis, this product features many charts and graphs in its default dashboard that provide a good overview of what’s happening around the network. However, for a more detailed view, this product comes preloaded with report templates, including many compliance-based reports.

Documentation included a single help file that is built into the management interface itself. We found this to be quite detailed for a help file. It actually felt more like an administrator guide. It included many screen shots, diagrams and step-by-step configuration and management instructions in a well-organized format. While we did not receive any other manuals, we found that this file did an exceptional job of providing the necessary information to configure and use the product.

ManageEngine provides no-cost support for the first 30 days of product use. After that, customers on the perpetual license model must purchase support as part of a maintenance contract. Customers with a subscription model price have assistance included in their subscription cost. Customers receive email- and phone-based technical support, as well as access to a large online aid area. Customers who access the online support will find a knowledge base, user forum, product video tutorials, documentation and other resources.

At a price starting at $1,195 for 10 hosts (perpetual) or $395 per year for 10 hosts (subscription), we find this product to be a good value for the money. The EventLog Analyzer provides some very solid SIEM functionality at a reasonable cost for smaller environments that want to get started with SIEM, but can’t afford to invest in a full-scale product. Overall, we find this solution to be easy to deploy and manage in any size environment and to have a solid price for the feature set.
Stopping distributed denial-of-service attacks

Distributed denial-of-service (DDoS) attacks certainly are a serious issue that can cause lots of productivity loss. These incursions also can cost hard dollars when they prevent paying customers from spending money on a site under attack. The key issue, of course, is separating the DDoS packets from legitimate data packets. When the DDoS packets are flooding at nearly wire speeds, that is a lot easier to talk about than it is to do. That, though, is exactly what the Fortinet FortiDDoS-200A accomplishes.

FortiDDoS is an appliance that examines data packets in a variety of ways to separate DDoS packets from legitimate packets. In order to accommodate high volume data, all filtering is done in hardware. The platform contains hardware-based policies that can be tuned to allow such things as virtual partitioning, which in turn allows different policies for different business units, for example. Setting up the appliance is straightforward, if not exactly simple. The first step is to set up the virtual partitions – if one wishes to have different partitions. Next, the partition is baseline. The device starts in detection mode. In this mode it learns a baseline, but does not block anything. Once the baseline is complete and defining expected traffic loads, the appliance is switched to prevention mode where it begins to block and continues to learn.

One of the most powerful features of this tool is its suite of traffic graphs that allow the administrator to pinpoint DDoS activity, understand its nature and observe the effects of the appliance. Because the solution can drop traffic at layers 3, 4 and 7, spoofing or application-based attacks are caught and stopped. This is actually packet inspection – looking for malformed packets. However, even though the FortiDDoS uses these techniques, it also uses some traditional techniques, such as geo-location filtering and blacklisting.

Much of the product’s power resides in its Layer 7 filtering. Heuristic filtering addresses bot traffic, while operation code floods are blocked as well. All of these filtering activities are shown clearly on the appliance’s traffic graphs. Individual sessions can be analyzed with session diagnostics that allow drill-downs on, for example, source addresses. To the extent that this information is available, it is very valuable for after attack forensic analysis and tracing. In the FortiDDoS, the data is available. And that makes it a powerful analytic tool, as well as a protective device for the network.

We liked this for its original and common sense approach to a problem that usually is not solvable – or, at least, easily solvable – by the usual methods of blocking and filtering. Once deployed, it is an easy device to manage and tune because it is replete with graphs and tables that show clearly what is actually happening on the wire. That makes tuning much more straightforward than tuning and waiting to see if what one did caused unintended consequences. If you are troubled by DDoS attacks, regardless of the size of your enterprise, this just might be the solution for you.

– Peter Stephenson, technology editor
Cyber war, this is not Espionage and fraud in cyber is not an armed conflict, says SystemExpert’s Jonathan Gossels  

We’ve all seen such headlines as: “U.S. General: Iranian Cyber Attacks Are Retaliation For The Stuxnet Virus; “Report on China spy threat may make attackers have to work harder”; and “The cyber war is real – and our defenses are weak.”

Those who believe the current level of cyber attack is “war” are missing the bigger picture: War is war. People die in wars. Countries disappear and new countries are formed by war. People are displaced by war. Fortunes are made and fortunes are lost in war.

What we are seeing is powerful nation-states recognizing that if you prepare to fight the last war, you will lose the next one. It is obvious that rather than fighting only with tanks, planes, ships, drones and soldiers, the next war will have a significant cyber element. Countries will use this new cyber element to weaken their enemy’s critical infrastructure, such as communications, power generation, banking, rail transport and air traffic control. They will also go after targeted companies that develop and produce weapons and emerging technologies.

Every major country is creating both offensive and defensive cyber measures. The Stuxnet worm is a clear example, reportedly developed jointly by the U.S. and Israel. It is a glimpse of the capabilities and delivery vehicles already on the shelf. That attack was a surgical strike on Iran’s nuclear facilities that caused centrifuges to spin themselves apart. It is only a glimpse, but already the level of sophistication is apparent.

Every weapon system in development needs to be tested. The defense capability of its intended target needs to be determined. Intelligence estimates can only go so far. One way to view the spate of attacks on U.S. banks and critical infrastructure is that our enemies are testing their cyber capabilities and assessing our vulnerability. At the same time, none of the players want to tip their hand and reveal the true power of the weapons they have developed.

In January, Iran reportedly launched attacks that probed a wide range of Western banks, but clearly the level of attack, and its brevity, fell far short of an act of war. On the other hand, the Chinese attacks, analyzed and reported by Mandiant, are a window into China’s broad preparation for cyber war and its current expansive program of cyber espionage. It is an unlikely coincidence that Mandiant researchers observed the hacker group, known as APT1, stealing western intellectual property from companies in strategic emerging industries that had been identified in China’s 12th Five-Year Plan (submitted in March 2011 to the National People’s Congress).

The recent Chinese attacks can be viewed as a political statement: China is saying, “We are a cyber force to be reckoned with.” It is essentially the same statement being made in the recent dispute with Japan over control of the Senkaku Islands. But, those Chicken Little’s who declare that “an all-out cyber war has begun” fail to recognize the interconnectedness and interdependence of the major economies. China, while demanding respect, has no incentive to blow up the economy of one of its largest trading partners, and by cascade, Europe, Canada, and Mexico as well.

Similarly, many companies have fallen victim to attacks launched by organized crime entities in Russia. These are almost always commercial in nature. As in most countries, the government considers these perpetrators to be criminals. These attacks cannot in any way be considered cyber warfare.

In short, we are seeing cyber flexing and, in some cases, war exercises, but not cyber war.

Jonathan Gossels is president and CEO of SystemExperts.
Layered Authentication for Secure Banking

Prevent fraudsters. Get strong yet convenient security anytime anywhere.

Mobile banking and other online financial services are prime targets for fraudsters, and the risk for online attacks is at the top of mind for banking security personnel. What’s needed is a versatile authentication answer to delivering confidence and convenience for anytime anywhere banking. HID Global Identity Assurance solutions for secure banking provide that unique multi-layered solution, which includes detecting malware, blocking fraudulent access, and verifying via an out-of-band channel to transparently protect against online fraudsters. Learn more.