ADJOINING ISLANDS

Converging physical and logical security can result in a seamless operation, says Honolulu CIO Gordon Bruce P22

Canadian start-ups
The nation has its own fledgling security community. What keeps these folks up at night? PC1

Cyber beacons
Information isn’t just leaking out of organizations, it’s being broadcast over Web 2.0 mediums P32
Leverage the power of the cloud. SECURELY.

The cloud is a dangerous place for sensitive data. We make it safer.

Websense security for cloud-based apps

How can you harness the power of cloud apps securely? Effective data loss prevention (DLP) is a critical element. Websense® TRITON™ solutions combine web and email security with industry-leading DLP to identify, discover, fingerprint and protect your data everywhere.

Get a free DLP whitepaper at www.websense.com/cloud-security

www.facebook/websensecanada.com

© 2012 Websense, Inc. All rights reserved. Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Websense security for cloud-based apps

How can you harness the power of cloud apps securely? Effective data loss prevention (DLP) is a critical element. Websense® TRITON™ solutions combine web and email security with industry-leading DLP to identify, discover, fingerprint and protect your data everywhere.

Get a free DLP whitepaper at www.websense.com/cloud-security

www.facebook/websensecanada.com

© 2012 Websense, Inc. All rights reserved. Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

REGULARS

4 Editorial The apple doesn’t fall far from the tree
8 Threat report During the past month, the Asia-Pacific Japan region was the main source of zombie IP addresses
11 Threat stats Fifteen percent of spam originated from Israel last month
14 Update Canada received a mediocre ranking in a cyber security report
15 Debate M&A activity in the cyber security arena will significantly increase in 2012
16 Two minutes on... Mobile application assurance
17 Skills in demand Companies are looking for network and server engineers
18 From the CSO’s desk Information sharing grows up, by Mark Clancy, The Depository Trust & Clearing Corp.
19 Update Canada received a mediocre ranking in a cyber security report
20 Opinion Privilege transparency, by Dwain Kinghorn, partner, SageCreek Partners
22 Adjoining islands There are obstacles to converging physical and logical security, but the upshot is a more seamless operation, says Honolulu CIO Gordon Bruce.
28 Boundless information Social media sites are filled with valuable assets that must be protected.

PRODUCT REVIEWS

39 Product section Vulnerability assessment has evolved over the years, and we hope to shed a bit of light on some of those changes.
40 Group Test: Vulnerability assessment There are very few pure-play vulnerability assessment tools left in the market, and those are the old, reliable mainstays of the genre.

56 First Look: SecureDoc from WinMagic There are many products that claim to do preboot whole disk encryption. But there aren’t a lot of them that claim to do it over the network.

Gordon Bruce, CIO, city of Honolulu P22

FEATURING

22 Adjoining islands

There are obstacles to converging physical and logical security, but the upshot is a more seamless operation, says Honolulu CIO Gordon Bruce.

McAfee P47

SecPoint P52

C1 Canadian start-ups

The nation has its own fledgling security community. What keeps these folks up at night?

C2 Cyber beacons

Information isn’t just leaking out of organizations; it’s being broadcast over any number of Web 2.0 mediums.

Larry Whiteside P56

Mary Landersson P32

Cover photo by Dana Edmunds

© 2012 Websense, Inc. All rights reserved. Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.
The apple doesn’t fall far from the tree

In a time when information security and privacy concerns are mainstream, news about a company seemingly misleading customers and failing to secure their sensitive personal information is mighty incongruous.

Just last month, the U.S. Federal Trade Commission (FTC) settled a case with Upromise, which is owned by Sallie Mae, after it failed to encrypt customers’ personal information and provide clear details about its data collection practices.

With the promise of offering more customized deals, Upromise encouraged its savings account holders to download a “TurboSaver Toolbar” to find merchant rebates from partners. However, with the toolbar download, the company also collected loads of personal information, which was transmitted unencrypted.

Following the FTC’s ruling, the company now is tasked with erasing this data it collected, providing clear disclosure policies and receiving consumer consent prior to their installation of any similar products.

Although a Upromise rep told us that only one percent of the company’s members were affected and that company execs are unaware of any instances of fraud that occurred, this doesn’t negate the fact that they should have known better. We’re talking about a company owned by Sallie Mae, which has a very competent, well-respected CSO at its helm.

Further, it’s not as if customers have been mum about dissatisfaction with some of the company’s other lending and account practices. For instance, customer discontent was demonstrated last October when a contingent of Occupy Wall Street protestors in D.C. reportedly converged on the steps of Sallie Mae offices to voice various grievances about student loans. The company kept its doors closed.

This may be because even in light of sundry customer concerns, Sallie Mae’s doing just fine during an economy that sees some 13 million people out of work, according to recent joblessness figures. In fact, it has around $140 billion of federal college loans on its books – a nice chunk of change as it sees its now private lending rise. Meanwhile, the largest student lender in the country has spent millions on various lobbying efforts to Congress, including pleas to continue government subsidies to private lenders.

Working in the customer’s best interest seems a business principle ignored by Upromise’s parent company. Given the recent FTC/Upromise settlement, hopefully security and privacy practices won’t become another.

Ilenna Armstrong is editor-in-chief of SC Magazine.
Each month we host an event focused on protecting one that rarely is satisfactorily remedied. We offer solutions.

FOR MORE INFO

Safeguarding handheld devices used by employees with privileged access, believ- ing their actions on the enterprise network will lead to combat this persistent threat. We take gain. However, there are solid defenses that are undetectable, are tempted by easy breaches! Mass injection campaign affects just some of the web applica- tion breach events that made headlines in 2011. Exploits into these applications continue to take advantage of vulnerabilities in the code that security experts have known about for decades. So, why do cracks in web apps still linger, and what should security teams be doing better to plug them? We’ll find out.

WHAT IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHO’S WHO AT SC MAGAZINE

For information on SCWC 24/7 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/scwc247.

WHEN IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHERE IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHAT IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHEN IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHERE IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHAT IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHERE IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHEN IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHAT IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHERE IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHEN IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.

WHAT IS SCWC 24/7?

SC Magazine has created a free virtual event focusing on solutions.
India top producer of zombie IP addresses

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

Source: Symantec
The top attack in the United States last month was the ZeroAccess trojan.

**Spam** The world’s worst spam-support ISPs

<table>
<thead>
<tr>
<th>Position</th>
<th>ISP</th>
<th>Number of current known spam issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>chinanet-zj</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>telefonica.com.ar</td>
<td>59</td>
</tr>
<tr>
<td>3</td>
<td>ovh.net</td>
<td>54</td>
</tr>
<tr>
<td>4</td>
<td>unicom-cn</td>
<td>53</td>
</tr>
<tr>
<td>5</td>
<td>unicom-hl</td>
<td>44</td>
</tr>
<tr>
<td>6</td>
<td>chinanet-hj</td>
<td>43</td>
</tr>
<tr>
<td>7</td>
<td>telefonica.com.br</td>
<td>41</td>
</tr>
<tr>
<td>8</td>
<td>verizon.com</td>
<td>40</td>
</tr>
<tr>
<td>9</td>
<td>chinanet-jx</td>
<td>40</td>
</tr>
<tr>
<td>10</td>
<td>chinanet-gd</td>
<td>37</td>
</tr>
</tbody>
</table>

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

**Malware** Vertical encounter rate

- 169% Education
- 125% Food & beverage
- 106% Government
- 100% Banking & finance
- 88% Health care
- 88% Retail & wholesale
- 50% IT & telecom

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

**Phishing** Volume dropped 26 percent

<table>
<thead>
<tr>
<th>Month</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>July</td>
<td>25,391</td>
</tr>
<tr>
<td>August</td>
<td>25,907</td>
</tr>
<tr>
<td>Sept.</td>
<td>24,019</td>
</tr>
<tr>
<td>Oct.</td>
<td>28,365</td>
</tr>
<tr>
<td>Nov.</td>
<td>28,119</td>
</tr>
<tr>
<td>Dec.</td>
<td>25,112</td>
</tr>
</tbody>
</table>

In December, phishing volumes dropped 26 percent as compared with the previous month’s total number of attacks. Once again, a handful of brands were targeted and endured fluctuating surges of thousands of phishing attacks through the month. Leading by a wide margin, the U.K. was the country most targeted by phishing attacks last month, experiencing 50 percent of the global volume. In terms of attack hosting, the United States topped the list, having hosted 52 percent of the world’s phishing attacks. Source: RSA Anti-Fraud Command Center

**Top breaches of the month** Data loss

- **Restaurant Depot** People who shopped at Jetro or Restaurant Depot may have had their credit or debit card information taken by hackers. - 300,000
- **Massachusetts eHealth Collaborative** A briefcase was stolen from an employee’s car during lunch sometime during the spring of 2011. - 14,475
- **Good News Garage** A Nov. 25 home burglary resulted in the loss of an encrypted data tape. - 14,000

Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005: 542,986,096 (as of Jan 12)

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

---

At WGU we respect your time and intelligence, because what you know is more important than time in a classroom. WGU’s ONLINE competency-based approach puts you in control of your academic destiny... and your own security.

**Master of Science Information Security and Assurance**
- Incorporates (and includes in the tuition!) 6 security and networking certifications. (Your time to completion will be shorter if you already hold any of these certifications.)
- Certified by the National Security Agency’s IACE program.
- Meets CNSS National Training Standards.
- Scholarships Available.

**Incorporates** (and includes in the tuition!) 6 security and networking certifications. (Your time to completion will be shorter if you already hold any of these certifications.)
- Certified by the National Security Agency’s IACE program.
- Meets CNSS National Training Standards.
- Scholarships Available.

---

“WGU respected the knowledge and experience I already had, making it possible for me to accelerate my program. The curriculum is rigorous and relevant.”
1. ZeroAccess trojan
2. Downloader trojan
3. TDSS Downloader trojan
4. Zeus trojan
5. Sinowal trojan

There were 5,134,852 attacks in the United States and 1,416,688 foreign attacks last month. Source: Dell SecureWorks

Zombie IPs Global distribution

- India 19.0%
- Other Asia 16.9%
- Brazil 7.0%
- Indonesia 2.9%
- United States 3.1%
- Russia 6.2%
- China 5.4%
- Other Europe 16.4%
- Pakistan 6.2%

The biggest increases in month-over-month zombie activity occurred in Brazil, Russia, Indonesia and “other” European nations, while the largest decreases occurred in India, Pakistan and Vietnam.

Top 5 attacks used by U.S. hackers
1. ZeroAccess trojan
2. Downloader trojan
3. TDSS Downloader trojan
4. Zeus trojan
5. Sinowal trojan

Top 5 attacks used by foreign hackers
1. ZeroAccess trojan
2. Downloader trojan
3. Zeus trojan
4. Sinowal trojan
5. TDSS Downloader trojan

There were 5,134,852 attacks in the United States and 1,416,688 foreign attacks last month. Source: Dell SecureWorks

Spam rate Compared to global email

- 12/30/11: 4%
- 12/27/11: 3%
- 12/23/11: 2%
- 12/21/11: 1%
- 12/19/11: 0%

Spam rate indicates the accumulated emails tagged as unsolicited.

Received spam Top five regions

- Israel 15.85%
- USA 11.84%
- Japan 6.12%
- Canada 3.39%
- U.K. 3.10%

Source: Fortinet Threatscape Report

Internet dangers Top 10 Threats

<table>
<thead>
<tr>
<th>Name</th>
<th>Movement</th>
<th>Date observed</th>
<th>Type</th>
<th>Last week</th>
<th>Weeks on list</th>
</tr>
</thead>
<tbody>
<tr>
<td>GameVance</td>
<td>▲</td>
<td>Oct. 21, 2010</td>
<td>Adware</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zbot</td>
<td>▲</td>
<td>Sept 9, 2010</td>
<td>Bot</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zbot.genY</td>
<td>▲</td>
<td>Sept. 21, 2010</td>
<td>Bot</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>Vundo.OD</td>
<td>▲</td>
<td>July 14, 2011</td>
<td>Trojan</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SaltY.AT</td>
<td>▼</td>
<td>Dec. 5, 2010</td>
<td>Virus</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Cypbot.G</td>
<td>▼</td>
<td>Oct. 13, 2011</td>
<td>Backdoor</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>BurmanInfra</td>
<td>▲</td>
<td>Sept. 22, 2010</td>
<td>Trojan</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Winwebsec</td>
<td>▲</td>
<td>Sept. 22, 2010</td>
<td>Rogue</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>Rehisp.A</td>
<td>▼</td>
<td>Sept. 21, 2010</td>
<td>Worm</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>VItlfect</td>
<td>▲</td>
<td>Sept. 23, 2010</td>
<td>VrTool</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Kindsight

“Spam rate compared to global email.”

“Internet dangers Top 10 Threats.”

3M™ Privacy Filters offer you a crisp, clear view of your laptop, desktop computer or mobile device screen while blocking wandering eyes from seeing sensitive data. To learn why visual privacy is an important part of any data security plan, download the white paper at: 3MPrivacyFilters.com/security
**Debate** 

M&A activity in the cyber security arena will significantly increase in 2012.

For: PwC’s latest M&A report into global cyber security. “Decoding Deals,” shows that activity was strong in 2011, with deal value and volume showing significant growth from 2010. Deal activity in 2012 and beyond will likely be underpinned by three key factors. First, the cyber security market is expected to continue to grow as organizations spend more on security products and services given growing threats and vulnerabilities. The relatively high market growth versus other industries will likely attract investment and help maintain current ideal valuations.

Second, a large number of active buyers see cybersecurity as a strategic priority market, and they are looking to grow their cyber security capabilities. Buyers include technology, IT and defense companies, many of which have healthy balance sheets providing firepower for deals. Finally, active sellers, including private equity firms, may look to trade sales and secondary buyouts to exit assets, particularly if the IPO market remains subdued.

Against: With mobile and cloud-based technologies innovating at a dizzying pace, valuable data is increasingly being stored online, and cyber threats are likewise growing. Although security will not skyrocket in 2012. For one, investors are unlikely to so quickly exit new investments. Secondly, the sector will be hard-pressed to maintain – never mind exceed – its recent rate of blockbuster deals, which have driven M&A growth. Rest assured, cyber security will remain as a critical area of technology development in 2012, and there may be a few defense contractors making small cyber pickups. Just don’t expect M&A to shoot through the roof.

**THE QUOTE**

If [an] owner is under attack, who do you call?

Patrick Miller, president and CEO of the National Electric Sector Cybersecurity Organization, on the lack of a lead response agency in the event of a cyber attack on critical infrastructure.

**THE SC MAGAZINE POLL**

Do you support the Stop Online Privacy Act (SOPA)?

Source: Institute for Policy Innovation/Center for Responsive Politics.

**THE STATS**

- $12.5b in losses estimated annually to the U.S. economy from music piracy.
- $91m estimated spend in 2011 by film, music and TV industries lobbying for the approval of SOPA.

**THREAT OF THE MONTH**

Acrobat zero-days

What is it? There are two zero-day vulnerabilities [since patched] affecting Adobe Reader/Acrobat v9.4.6 and v10.1.1 and earlier on all supported platforms being actively exploited against v9.x for Windows.

How does it work? One of the vulnerabilities exists in the handling of embedded U3D data, while the other exists in the PRC component. Both can be exploited to corrupt memory, thus gaining control of the program flow and executing malicious code once a specially crafted PDF file is opened.

Should I be worried? Users should be cautious about opening random PDF files. Reader X provides an extra layer of defense via the new sandbox feature, which protects against known exploits targeting the older 9.x branch.

How can I prevent it? The company released an updated version (9.4.7) for the 9.x branch for Windows, and on Jan. 10 issued a fix for the 9.x branch for “NIX and Mac.

Source: Carbon Black, chief security specialist, Secure.
**Mobile application assurance**

N
o doubt the explosion in smartphones and tablet devices has enlivened the global marketplace and brought convenience and connectivity to consumers. However, while many benevolent mobile applications do what they’re supposed to – Apple and Android distributed close to 20 billion downloads in 2011, according to industry estimates – countless others carry malware.

Larry Stavrou, an assistant professor in the computer science department at George Mason University in Fairfax, Va., working with Jeffrey Voas of the National Institute of Standards and Technology, is creating a capability for apps to be vetted and, in the not too distant future, for the public to gain access to reports that will allow them to gauge an application’s trustworthiness.

At the moment, a portal available only to the military, FBI, Department of Justice and civilian agencies rates mobile apps in terms of code functionality and reliability. The intention is to eventually make the research available to a much wider audience.

“Consumers want to move to tablets and smartphones, but this new market is not as secure as it is for laptops,” said Stavrou. “Many of the malware applications have not gone through the process of being approved for use.”

The question becomes: What is a good application?

Metrics are needed, Stavrou said. “Most software for computers comes from companies users can trust,” he said. However, in the burgeoning mobile market, there are offerings that may have been rated highly, but may prove unreliable. Also, developers in the mobile market sometimes take legitimate code, add some of their own, and repose it as their own product, he said.

**1.2b mobile apps were downloaded worldwide in the final seven days of 2011**

Source: Flurry Analytics

“Whatever we try to do is secure the web, identify all the mobile apps posted online, and create a report of what the app really does,” Stavrou said. What he’s discovered is that most of the developers in the marketplace are young and don’t care about reliability. They care about bringing functionality to the user, but at the same time they open the door for code functionalities to be abused by others. “We want to bring a rational evaluation of the functionality, quality and the reliability of that code to the end-user, and explain why an app might not be good,” Stavrou said.

The positive news is that it is a solid market that will inevitably sort itself out, he said. “Faulty apps will fade away and be replaced by more serious apps, and people will pay more attention to reliable coding.”

– Greg Masters

**JOBS MARKET**

Me and my job

Rick JR Mayberry, consulting network and security architect, Torrey Point Group LLC

**How do you describe your job to average people?**

I tell the average person that I’m in technology or engineering. When most people ask, I tell them I help Fortune X companies develop their network security roadmap.

**Why did you get into IT security?**

I was introduced to hacking in the mid-90s on local bulletin boards. I would read text files about “phreaking” and hacking, and used that as a foundation for learning networking and systems. I got my first job a few years later based on the knowledge I had gained running Linux and a home IP network.

**What was one of your biggest challenges?**

I made the transition from technical/engineering to technical leader to people leader. Growing as a person is important to me and my life goals.

**What keeps you up at night?**

Security doesn’t keep me up at night. Making the people who work with me successful, challenged, happy, healthy and visible is what is most important to me.

**Of what are you most proud?**

For a large part of my career, I was directly responsible for securing the largest converged IP network in the world. I worked directly with the team that built this network from the ground up. I also love grooming and mentoring individuals, and helping them have successful careers in IT security.

**For what would you use a magic IT security wand?**

I would use my magic IT security wand to better communicate returns on security program investments. I’d lose terms like risk avoidance and insurance, and use my wand to create real tangible dollar and cents business proposals for security programs. There are methodologies out there that facilitate this, but they aren’t being used enough and may not be mature enough. Security investments are still driven by “checking the compliance box” and media-induced fear.

**Skills in demand**

Companies are looking for network and server engineers. Previously, these skill sets were segmented. Today, companies desire this combined knowledge. In addition, enterprises need individuals to provide oversight to their compliance issues.

**What it takes**

Experience and designations in Cisco, Microsoft and VMware are essential. To provide compliance oversight, job seekers must have five-plus years of experience and obtain certifications.

**Compensation**

Salaries range from $80k–$150k for engineers, and can range from $100k–$250k if well-versed and certified.

Source: Jerry Irvine, CIO, President Solutions

**Larry Whiteside has been named CISO and director of enterprise IT security, risk and compliance at Spectrum Health Systems, a Grand Rapids, Mich.- based nonprofit dedicated to improving the health of families and individuals. He was formerly CISO at Visiting Nurse Service of New York.**

www.spectrumhealth.org

**Larry Whiteside, CISO, Spectrum Health Systems**

A virtual malware threat protection vendor Invincea has announced it raised $5.1 million in growth capital. The cash investment expanding Invincea’s corporate sales, engineering and marketing efforts. At the same time, Christopher Smith has been named worldwide VP of sales. He was formerly Eastern VP of sales at ArcSight.

www.invincea.com

**Boulder, Colo.-based cloud security company Symplified has announced it has partnered with GCA Technology Services, a provider of identity management solutions. GCA will now offer Symplified’s identity and access management customers access to cloud infrastructure.**


**The Security Industry Association (SIA), a trade group that represents the makers, service providers and integrators of electronic physical security products, has appointed Marcus Dunn director of government relations. He replaces Don Erickson, who last year was named SIA’s CEO. Dunn formerly served as a senior account executive at Susan Davis International, a public relations firm.**

www.siaonline.org

**ManTech International, provider of IT services to the federal government, has named Mark Chadason senior vice president and general manager of its cyber and security operations business unit. Chadason will oversee a team whose goal is to provide customized security solutions to the U.S. military and intelligence community. He previously served as corporate risk officer at Susan Davis International, a public relations firm.**

www.siaonline.org

**Mark Chadason, SVP/GM, ManTech International at ManTech and is a veteran of the CIA.**

www.mantech.com

**Sam Mateo, Calif.-based network intelligence provider VSS Monitoring has named 25-year industry veteran Rob Markovich as SVP, worldwide sales and marketing. Previously, Markovich was co-founder and executive at Visual Networks, a network service assurance vendor, which he led to a successful IPO and acquisition by Fluke Networks. He was CEO of enterprise mobility startup Agito Networks, which was acquired by ShoreTel.**

www.vssmonitoring.com

**xIBM has announced it will acquire Green Hat, a provider of software quality and testing services for the cloud. The company will be integrated into Big Blue’s Rational software group. Terms of the deal were not disclosed.**


Follow us on Facebook and Twitter
Information sharing grows up

Mark Clancy
managing director, technology risk management, The Depository Trust & Clearing Corp.

Last year may have been the best, bad year for the information security profession. There were numerous significant headlines about breaches and intrusions into different companies across industries, with pundits deploring the generally serious state of affairs. But you might not have noticed that a radical improvement for the good guys was also taking hold.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was founded in 1999 to allow information on physical and cyber security threats and vulnerabilities to be shared, with the ultimate goal of protecting the U.S. critical infrastructure. In 2011, the organization saw an unprecedented in-flow of incident submissions from its membership and shared that information, as directed by the submitter, to the 4,200 institutions supported by FS-ISAC, to other critical infrastructure ISAs, and to government agencies. At the same time, other parts of the critical infrastructure community were bidirectionally sharing richer, more complete and actionable information among its members, the Department of Homeland Security and other U.S. government agencies, within a series of concentric rings of trust supported by formal agreements. This enhanced volume of sharing and level of detail is allowing critical infrastructure operators and government agencies to better defend themselves from attacks and is giving the initial submitter a deeper understanding of whether an attack is a direct target or a non-specific threat.

The FS-ISAC went from measuring prior information flow as a trickle with a single-digit number of events per month and paying little detail to the current torrent of information flow spanning dozens of events with hundreds of associated indicators per month. This increased maturity and robustness allows defenders to detect and mitigate similar attacks and, in many cases, understand what part of the attacker lifecycle the indicator information has represented.

Amplified velocity, width and depth of information that needs to be shared clearly highlights the need for the design of frameworks to be enhanced to industrial-strength capacity and near real-time dissemination.

When building these capabilities, organizations must recognize that there is a spectrum of maturity across the community to act on this information. The key point to remember is that most organizations still work in isolation. At the same time, our adversaries are recycling attacks. Sharing information within a community of trust is the best defense you can give your organization to thwart those attacks.

30 seconds on...

» CSO questions
Today’s CSO must ask themselves many questions, says Clancy. Does my organization understand the risk/reward trade-off between sharing and not sharing?

» Community of trust
Do I have a community of trust where I can share information – with or without attribution – to make that community stronger? If not, why not, and how do I find one?

» Automation, don’t be late
The only way to achieve scale is to automate, don’t be late.

» Toolkits are available
Efforts, such as MITRE’s Cyber Observable Expressive Capability (CybOX), are the kinds of toolkits needed to facilitate machine- and human-readable content exchange.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Connect to the latest knowledge in Cybersecurity

Connect to the latest knowledge in Cybersecurity

Learn what it takes to lead in Cybersecurity today.

What you’ll learn in this ultra-current master’s degree program will put you in demand in the private and public sectors.

• Protect your organization’s information and technical assets.
• Expand your knowledge of cyber protection techniques, tools, and technology.
• Focus on network and software security, business continuity planning, ethical hacking, risk management, and more.

Our curriculum is developed and continually updated with leading security experts.

Bellevue University makes it possible.

We give you accelerated bachelor’s degree completion (accepting the credits you’ve already earned), convenient online learning that fits into your busy life, engaging, interactive learning, affordable tuition, and a degree that opens doors for you.

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master's Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor's Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
• Information Technology

Learn more about this and other degrees in the IT field offered by Bellevue University 100% ONLINE.

Bellevue University offers these degrees in the IT field.

Master’s Degrees
• Cybersecurity
• Computer Information Systems
• Management of Information Systems with a concentration in Information Security
• MBA with a concentration in Information Security

Bachelor’s Degrees
• Cybersecurity
• Computer Information Systems with an emphasis in Information Security
• Systems and Network Administration (SNAP)
Don’t forget cloud availability

Between RSA, Sony and Lockheed Martin, major security failures have been unusually common in recent headlines. But, it’s not just the uptick in data breaches that should have security professionals worried – they should be equally concerned about the breaches in availability.

Take Amazon’s EC2 cloud outage last April. This single, highly publicized incident risked a major step backward for enterprise cloud computing adoption. To the public’s knowledge, sensitive business and personal data were not breached, but the failure in service broke a key tenet of network security: availability.

Cloud providers have a responsibility to ensure that they are constantly available. Recent outages, like what happened with Amazon, underscore the absolute necessity of always-on connectivity. However, because increasingly sensitive data now resides in the cloud, availability is no longer solely tied to access – it’s also tied to security. In short, if the cloud is not available, you can’t guarantee that security was not the culprit. Why? Because the two cannot be separated. They are inextricably linked.

As cloud computing evolves, security strategies must address load, perimeter and behind-the-firewall protection, as well as availability. Unfortunately, it’s difficult to assess the level of security in the cloud today. Even those service providers which have been vocal about security have limited their mindset to traditional devices and fail to discuss how they’re addressing availability and uptime.

If service providers want to gain the trust of enterprises to fully migrate to the cloud, and if enterprises want to fully realize the benefits of cloud computing, providers in the arena must offer transparency in how they’re handling all aspects of security – from device implementation (both virtual and physical) to addressing resilience and manageability. Only when these three areas act in concert and cohesively will security in the cloud reach maturity and gain the full trust of the public.

Privilege transparency

Particularly with Windows 7 migrations in full swing, few would argue the advantages of a strong privilege management solution for IT. A recent vendor survey shows a 463 percent jump in demand to implement privilege management among companies moving to Windows 7. Sixty-three percent of respondents consider it critical to manage administrative privileges for end-users to ensure security and reduce vulnerability.

When users don’t have local administrator rights, they can’t make changes that destabilize the system or require extra support to correct the problems they accidentally create. Additionally, a locked-down system is less susceptible to malware.

But by its very name, a “personal computer” is generally seen by a user as “my device.” Many organizations allow users to run with local admin rights simply because it’s too difficult to keep the system locked down.

But removing admin rights is only a part of the fix. There are legitimate situations that require elevated privileges for users to accomplish their jobs. What companies really need is a way for users who need those rights to gain those privileges smoothly.

How do you accomplish that? A strong privilege management solution needs to take individual and collective user needs into consideration. Users have a set of things they do to get their jobs done, and they expect to be able to perform their necessary work without IT intervention. If users have been able to perform certain tasks on their own in the past, they are naturally going to expect that right to still be in place after a desktop lockdown happens.

As a company moves to a locked-down environment, it should do so in conjunction with an effective privilege management solution to make the transition as transparent as possible. This will help to ensure the enterprise users’ ease and cooperation, which is the optimal objective of every major IT or operational change.

Privilege transparency

Particularly with Windows 7 migrations in full swing, few would argue the advantages of a strong privilege management solution for IT. A recent vendor survey shows a 463 percent jump in demand to implement privilege management among companies moving to Windows 7. Sixty-three percent of respondents consider it critical to manage administrative privileges for end-users to ensure security and reduce vulnerability.

When users don’t have local administrator rights, they can’t make changes that destabilize the system or require extra support to correct the problems they accidentally create. Additionally, a locked-down system is less susceptible to malware.

But by its very name, a “personal computer” is generally seen by a user as “my device.” Many organizations allow users to run with local admin rights simply because it’s too difficult to keep the system locked down.

But removing admin rights is only a part of the fix. There are legitimate situations that require elevated privileges for users to accomplish their jobs. What companies really need is a way for users who need those rights to gain those privileges smoothly.

How do you accomplish that? A strong privilege management solution needs to take individual and collective user needs into consideration. Users have a set of things they do to get their jobs done, and they expect to be able to perform their necessary work without IT intervention. If users have been able to perform certain tasks on their own in the past, they are naturally going to expect that right to still be in place after a desktop lockdown happens.

As a company moves to a locked-down environment, it should do so in conjunction with an effective privilege management solution to make the transition as transparent as possible. This will help to ensure the enterprise users’ ease and cooperation, which is the optimal objective of every major IT or operational change.
Converging physical and logical security can result in a seamless operation, says Honolulu CIO Gordon Bruce. Dan Kaplan reports.

When Honolulu was preparing for an expected onslaught of protests that typically mark the annual APEC Economic Leaders’ Meeting, city and county leaders knew they had one security measure working in their favor which no one could compromise.

“We are on an island and are 2,500 miles away from the other states,” Gordon Bruce, chief information officer of the city and county, says. “So it’s not easy to jump on a bus and come here.”

But the government, of course, didn’t simply rely on its geographic isolation to ensure the annual forum – attended by dignitaries of 21 Pacific Rim countries and the United States to discuss economics, trade and investment policies – went off without a hitch. The integration of physical and logical security assets, namely bringing some 300 traffic cameras online under Honolulu’s integrated physical and access control monitoring system, also played a major role to ensure there was limited disruption to operations.

“We know where all the cameras are,” Bruce says. “If we need to bring them into some event going on, we can now easily fold them in... The whole point was to limit conflict and encourage participation in the process. The Secret Service even said it was one of the tightest events with which they’ve ever been a part.”

Since it embarked on a project seven years ago to converge physical and logical security, Honolulu, which makes up the entire 600-square-mile island of Oahu, is an entity that finds itself flaunting a rare synergy: Physical and facilities security and data/network/application security all fall under its Department of Information Technology. In other words, both sides of the house – the guards, gates and guns piece as well as the IT component – all work together under one roof.

“That was a conscious decision that was made in 2005 to bring all that together as one set of security complements,” says Bruce, 62, the CIO for seven years. The result is a more holistic, risk-based approach to security, he says.

Security convergence is certainly nothing new – the Sept. 11, 2001 attacks certainly gave it a healthy push forward – but its widespread adoption remains a work in progress. Brian Contos, senior director and customer security strategist at McAfee, defines convergence as a process by which physical and logical protection can be centrally managed and monitored through analytics, policies and procedures – all the while keeping a clear, communication channel between the two disciplines.

“If I have a solution in place that lets me centrally manage, configure and respond to all these disparate endpoints, whether it’s a computer or a door, that’s an efficiency win,” says Contos. “It allows one to be more effective and mitigate threats.” He adds that it also leads to cost savings over the long run.

More businesses are realizing that the lines of demarcation between physical and logical are certainly not what they used to be, especially as organizational leaders think about their security in terms of risk. Besides, IT-specific or
Security integration

blended threats are more likely to affect many organizations today than an exclusively physical attack. Once one accepts the benefits of integration, it’s easy to understand how boundaries can quickly erode. As a sign that the tide is turning, in September, ASIS International – an association for physical security professionals – and the IT-focused (ISC)³ held their annual meetings concurrently for the first time.

But the path to this aggregated style of security remains littered with obstacles, most notably the philosophy that the physical and IT security departments are distinct groups. According to a poll conducted by ASIS and (ISC)³ in the fall, almost half of 1,841 respondents said they do not have a definitive, enterprise-wide view of risk.

That explains why convergence is more common outside of the United States, in countries where IT connectivity is just beginning to emerge, places like Latin America, Southeast Asia and Africa. “It’s easier to go ahead and integrate this type of risk. But they do not have a definitive, enterprise-wide view of risk.”

That explains why convergence is more common outside of the United States, in countries where IT connectivity is just beginning to emerge, places like Latin America, Southeast Asia and Africa. “It’s easier to go ahead and integrate this type of risk.”

Pan Kamal, vice president of market- ing at AlertEnterprise, which makes software that unifies systems and applications across domains, offers a mock scenario of how a blended threat may warrant convergence within these environments: A warehouse supervisor who is marked as “disgruntled” in the HR system badges into the plant’s physical security system during off-hours. He then proceeds to look up valuable data related to pharmaceuticals on an inventory control system, adjusts the quantities in an inventory IT application, and then physically removes some of that merchandise from a warehouse shelf. Kamal explains that no single action the employee performs may have signaled the impending threat, but taken in concert, between physical and logical systems, he may have been stopped.

“It’s really connecting the dots,” Kamal says. “You must analyze risk across all those siloes to get the most comprehensive view of risk.”

CONVERGE OR NOT? Pros and cons

THE UPSIDE:

- Offers a single, centralized point for operation, administration and provisioning.
- Provides a more efficient model, which leads to cost and time savings.
- Allows for quick removal of physical/logical access if an employee is fired.

- Physical and IT systems can be reviewed in tandem in the event of a breach.

THE DOWNSIDE:

- A single point of failure could cause a major business impact.
- The introduction of a virus can prevent both network and physical access.
- “Turf wars” may result when merging physical and IT security teams.
- Initial costs to integrate and educate both disciplines may run very high.

Source: Trustwave

You had to figure out how the PACS systems worked. We’ve come a long way since then,” Diodati adds that logical sys-

tems, too, particularly the Windows Vista and 7 platforms, are offering increased smart card support.

This corporate symbiosis makes sense, experts say, given the more prominent role that security plays in today’s business environment, with concerns over data breaches, compliance and even terrorism remaining at high levels.

Perhaps no vertical has been leading the convergence push more than the federal government. In 2004, the Home-

land Security Presidential Directive 12 (HSPD-12) was approved, requiring all federal employees and agencies to use a converged physical and logical ID badge, known as a PIN card.

Other industries, such as financial services and health care, are also seeing accelerating adoption rates. In the case of the latter, a market that traditionally lags in the area of technology, health care is beginning to place an uncharacteristi-
cally heavy emphasis on IT security, in response to audit fears of HIPAA and the HITECH Act. This is enabling the linking of physical and logical security functions.

Synergies allow physical security to benefit from technologies that were large-

ly considered the domain of IT, such as security information and event manage-

ment (SIEM). In the past, if something suspicious showed up on a surveillance camera, for example, the process to review the incident was arduous.

“You had to take out the video tape and watch for hours and fast forward,” Diodati says. “Now these can be catalogued and indexed, and can be fed into a SIEM product to correlate across disparate systems. SIEM is about looking at what’s going on across systems.”

Perhaps the upside of convergence is no better expressed than in a manufactur-

ing or critical infrastructure entity, which often must follow strict mandates govern-

ing the access and identity of users.

Perhaps the upside of convergence is no better expressed than in a manufactur-

ing or critical infrastructure entity, which often must follow strict mandates govern-

ing the access and identity of users.

You wouldn’t know it to look at her, but Irene is dangerous. She’ll never let on that she’s ready and willing to steal sensitive information for her nefarious purposes. But with BeyondTrust Privileged Identity Management solutions, she’s not able. So instead of being an exposure, she’s the one who will be exposed.

Learn more at BeyondTrust.com/Identity/ThiefIrene

©2011 BeyondTrust. All rights reserved. BeyondTrust is a registered trademark of BeyondTrust Software, Inc.
doesn’t have a statewide Department of Motor Vehicles. Vehicle registration is handled by each county government – Bruce and his team are responsible for securing the process – and the system interfaces with DMVs from around the country and in Canada and Mexico. In addition, Bruce has overseen the collapse of Honolulu’s 14 phone systems into the state’s largest VoIP system.

In 2005, Bruce embarked on a $300,000/year project – largely covered by federal funds – to make Honolulu’s security fully converged. Specifically, that meant centralizing video surveillance and access control across Honolulu’s numerous buildings and facilities, which includes six highly sensitive wastewater treatment plants.

“(Now) we have 9,000 ID badges issued to [all] city and county employees,” he says. “We are logging you electronically and visually that you have gone in and out of facilities. Now we get alerts when cameras break or doors are left ajar.” Any pushback that employee unions gave on the camera systems – which previously were managed by individual departments – were assuaged when Bruce explained how the new protocol would better protect the safety of workers. “The key to the unions that helped them understand is that it’s not just about protecting the employee, it’s about protecting the employee,” Bruce says. “We’ve had incidents of when employees were harassed by the public because there was no security in place.”

Turf wars
With door access and video surveillance increasingly IP enabled – IMS Research estimates that some 22 billion devices overall will be internet connected by 2020 – it’s really just a matter of time before most companies consider convergence, say experts. But before any organization can realize the potential gains – like cost savings and efficiency – it must sort out the power struggles and turf wars likely to result between the physical and IT departments. “We’ve seen situations where we’ve brought our solution, and the first time the physical and IT people talked to each other was at our meeting,” Kamal says.

Contos says this is a realconcerts, considering workers from both divisions come from different backgrounds and have different salary expectations. The issue further complicates itself when talking about organizations that outsource their physical security, in arrangements such as leased offices.

To what degree do the traditional and IT security areas within your organization work together?

All of those systems have to work together.”

– Jonathan Kaplan, San Francisco International Airport

“We have the technology to pull this off,” Contos says. “We can integrate all your virtual stuff, as well as physical access cards and video analytics. That part’s been solved. But the technology is only one piece. The second part is the process around how it’s to be managed.” C-level buy-in, a governance framework and robust training are good places to start, experts say. “The stereotype is that guards with guns and system administrators are different people,” Diodati says. “But if you want to be successful with a convergence initiative, you need to have executive support that makes those two organizations play together.”

At San Francisco International Airport, one of the busiest in the nation, security is the name of the game, says Jonathan Kaplan, the director of information security. As a result, he hasn’t encountered too much resistance when merging the two disciplines. Both are treated as equally critical to the airport’s overall mission. For example, the airport is in the process of transitioning 1,500 analog, closed-circuit security cameras, which are trained on access doors, security checkpoints and roadways, to run over IP.

Kaplan admits that there will “always be tension as complexity evolves,” but in his experiences he believes members of both sides of the aisle get the merits of convergence. “It’s easy to think about the physical aspect, because when you travel, that’s what you think about,” he says. “But all of those systems have to work together. A door protects a physical asset. A pass-word also protects an asset. We have to be safe and secure at all times we’re operating. So either we find a solution, or we shut down.”


Poor Annie. She means well, but can be a little distracted and sometimes clumsy. So if you give her administrative access, her carelessness can be your peril. But with BeyondTrust Privileged Identity Management solutions, Annie can access what she needs without the worry of accidental harm. She can’t stumble onto sensitive information or accidentally wreak havoc with your system. (Whew!)

Learn more at BeyondTrust.com/AccidentProneAnnie

©2011 BeyondTrust. All rights reserved. BeyondTrust is a registered trademark of BeyondTrust Software, Inc.
Social networking

A man named Joe Parrish had a Facebook page with 27 friends listed. Not long ago, he posted a comment on his wall about a recent visit he had with his sister.

Sounds harmless, right? In fact, there are innumerable similar messages posted everyday on many different social media sites throughout the web. Only problem here is that Joe Parrish is an inmate at the state’s Pocahontas State Correctional Center within the Virginia Department of Corrections (DOC), serving a 16-year sentence for involuntary manslaughter. Parrish was able to update his page by relaying information to family members, who colluded with him in posting the information. When DOC officials became aware of the activity, they had the page removed. But the fact is that social networking remains fertile ground for the many with a criminal mindset – even for those who have been caught.

“Social networks create a new type of communication structure – one that encourages openness, sharing, collaboration and cooperation,” says Ed Amoroso, senior vice president and chief security officer of AT&T. “These are wonderful goals, but unfortunately sometimes create special challenges for security teams. The security goal should be to ensure that proper controls are in place for emerging social networks.”

Social media sites are filled with valuable assets that must be protected, reports Jim Romeo.
Social networking

– beyond the ‘friend model’ we see in many common systems, and that these controls maintain the original collaborative objectives.”

Take a look at the U.S. Secret Service’s 10 Most Wanted list, and you’ll find a common pattern: fraudulent activity. This most often occurs not with a loaded gun, but in the form of a nonviolent crime where someone, often in a far-off nation, used their ability to capture information from some infrasctructure, personal or assets. For example, the wanted list describes a Hong Kong man who parlayed his knowledge of a health care company to steer claims payments directly to his own account in Asia.

Distant danger

Peruse the list and you’ll find clever criminals who take money, Social Security numbers, and detailed personal information out of the pockets of thousands of people without ever setting foot outside of their apartment, often in a country halfway around the world from most of their victims – and without ever using force.

“It is increasingly easier for hackers to obtain personal information online that is voluntarily posted by individuals,” says Theodore Theisen, director of information security, forensics and data breaches for Kroll, a security consulting firm.

“Well, the most recent personal information available, hackers subsequently have much more information that can be used to socially engineer their way into corporare networks. As a result of all of this information, there is an increase in spear (targeted) phishing attacks.”

The worst part of this is that victims may never know anything is going on at all. “An additional risk is that, in general, there is no transparency into failed login attempts on social networking websites,” says Theisen. “If a hacker tries to brute force their way into a social networking website account, there would be no way of knowing these attempts were being made. If similar or same passwords are being used by individuals to login to their social network accounts as their enterprise account, the hacker is much closer to being able to obtain unauthorized access to your business.”

Just last month, a new variant of the Ramnit virus was discovered stealing login credentials of millions of Facebook users. Computers are infected through drive-by-download attacks, which occur when users simply visit a malicious website and become infected without taking any action.

The danger, says Aviv Raff, CTO of Seculert, whose research lab discovered the attack, is that the hackers could now pare the personal information they’ve gathered to launch further targeted attacks. Users should not use the same password for Facebook and other online services, such as Gmail, Raff adds.

Michael Logan, president of delivery and operations for Axis Technology, a Boston-based provider of data masking software and solutions for enterprises, says social networking sites’ open sharing of information in an unfiltered and unsecured manner, and this presents a Pandora’s box of problems that seems to frustrate security professionals.

“This presents new risks for enterprises that they don’t know how to manage,” he says. “The typical reaction is to shut down access to social networking sites. However, business people are not willing to do this since they see exciting potential in social networks.”

The current trend is for social networking sites, like LinkedIn and Facebook, to provide more security- and privacy-related features, he says. However, these sites don’t want to make it harder for their users to “share,” while their network. The result is a set of capabilities that are a compromise and can be confusing to users.

Logan says personal information, often thought to be a wonderful facet of social networking engagement, may be a haunting enigma when it comes to social networking breaches.

“Employees and managers need to be aware of what will happen to information they share,” he says. “Most social networking sites have privacy policies that are one out of four. This means you basically share everything unless you explicitly tell the site you don’t want to share it. Most enterprises would prefer an opt-in strategy, where you only share information based on choices you explicitly agreed to. The risk is that many people will have to make a mistake and share some information they did not want to before they learn how to opt-out, and this process could be painful.”

Data hygiene

Data hygiene was formerly mainly paper based and, people believed, held securely. “Many years ago, the places where personal information was available were few and far between,” says John Eggleton, head of risk products for WorldPay at The Royal Bank of Scotland. The birth of the internet has shown that one’s information can be stored and accessed instantly at the touch of a button, and includes much more detail than in the past, he says. Plus, data is now stored in multiple locations and accessible via the internet.

“As much of this information is freely available, it is much easier for anyone to build a robust picture about us without actually needing to know us.”

The tidiness of information that abounds on social networking channels and pipelines is where the problems begin. “Data leakage is primarily a social engineering threat,” says Michael Sutton, vice president of security research at Zscaler, a SaaS security provider based in Campbell, Calif. People have become accustomed to sharing intimate personal details online, assuming that the information is safely housed in a trusted environment, with trusted individuals. Of course, this is not always the case.

While social networks may permit users to determine with whom information is shared, it is important to remember that data is shared among accounts, not people, Sutton says. “Accounts can become compromised. Even though a request may come from a ‘trusted source’ within the social network, that source may actually be an infected PC, not a known individual.”

As a general rule, when it comes to social networks, if one wouldn’t share the information on a public billboard, don’t share it on Facebook, says Sutton. Further, social networks are struggling to keep up with the inspection of online content, he says. “It has become a cat-and-mouse game as attackers continually look to bypass implemented security controls, and network owners attempt to implement new controls to detect the latest scan,” Sutton says. “Users cannot assume that social networks have succeeded in protecting them from attack, and users may take steps to implement their own security measures to protect against all content.”

So, will security managers ever be able to combat and safeguard against the threat that social network hacking poses to enterprise networks?

Management conundrum

Social networking is nothing new. The phenomenon was not created last week, last month or last year. It seems that as one door closes, another swings wide open, and security managers struggle to keep up.

“Cyber crime will continue to happen whether social networks are there or not,” says Scott Emo, head of software blade product marketing at Check Point Software Technologies, a Redwood City, Calif.-based provider of protection against internet threats. “Security managers are responsible for the safety of their enterprise networks.” He recommends a multilayered approach to defending against malware. A comprehensive security architecture should include firewall, intrusion prevention system, anti-malware, URL filtering, anti-bot, data leakage prevention and other technologies.

Exploit by organized gangs

Jim Kardaras, a senior vice president with the FINPRO practice of Marsh, an insurance broker, cites organized crime rings as the primary culprit in new methods to abscond with ill-gotten gains. “Cyber crime has grown and intervention by legislators at the federal level, may be warranted, particularly when resources aren’t plentiful to combat the ever-impending threat of criminals exploiting social networking mediums to violate the masses.

“Many small and midsize companies and government entities lack the rigorous security programs of larger companies,” says Kardaras. And companies cannot rely too heavily on their banks for protection against account fraud, as business accounts are currently not covered by the laws that provide zero-liability protection and hold banks totally responsible for fraud and losses, outside of insurance.”

This article originally appeared in SC Magazine Spotlight on Social Media

Influencing factors when choosing a social network

Security 92% 91%

Privacy 90% Ease of use 87%
The nation has its own fledgling security community. What keeps these folks up at night? Danny Bradbury reports.

Follw the freeway up from Seattle to Vancouver and you'll notice very little change when you hop over the border. A scowling bureaucrat and a few squat buildings are the only things punctuating the change from one country to another. The visible landscape looks largely the same on either side of the line. But the same cannot be said for the security vendor landscape...

Where anchor firms do exist, one problem facing Canadian security firms is the lack of interest in protecting data and meeting compliance among Canadian customers, says Brian Bourne, founder of the Toronto-based security show SecTOR. “That may be surprising for a country with such a large number of U.S. customers, or the regulatory need to be secure that our friends do south of the border.”

The lack of interest in the local market makes it difficult for companies to make headway in particular subsectors of security, such as services. Services often depend on regional customers, which ties Canadian security firms more closely to a tepid local market. Another problem for Canadian companies is that there are relatively few large anchor firms to help kickstart development in key markets, such as security. “We need those companies that teach and train people, that spit out entrepreneurs over time, like Amazon, which is an anchor company that trains entrepreneurs,” says Boris Wertz, an angel investor who runs Grow Lab, a Vancouver-based incubator.

In the United States, large firms such as RSA, Symantec, McAfee and CA, all provide fruitful conditions for the growth of smaller security firms, which can draw on the larger company’s resources. In Canada, there are few large security players. Symantec made $6.2 billion in revenues last year. The top Canadian security company, as measured by the Branham Group, a technology consulting firm, is MXI Security, which sells portable security systems and had 2011 revenues of $72 million. MXI was acquired last June by U.S. firm Imation, in a revealing example of a Canadian start-up malaise: early exits. Where anchor firms do exist, the security start-up community in Canada is sure to capitalise on them. Fixmo, a Toronto-based company which recently landed $23 million in series C funding, produces mobile security solutions for a flagship Canadian product, the BlackBerry. Research in Motion (RIM), the Canadian behemoth behind that mobile platform, may be troubled of late, but it still sits at the centre of a vibrant start-up community.

Both RIM and the BlackBerry Partners Fund, started by the Royal Bank of Canada (RBC), have produced some energetic members of the start-up community. Rick Segal, CEO and founder of Fixmo, was a part of that fund, which was started in 2008. Tyler Lessard, Fixmo’s chief marketing officer, was a key employee at RIM.

“An example of the new companies is the security start-up community. Rick Segal, CEO and founder of Fixmo, was a part of that fund, which was started in 2008. Tyler Lessard, Fixmo’s chief marketing officer, was a key employee at RIM.

“An example of the new companies..."
A ter learning its SecurID authenti-
cation product had been accessed
by outsiders, security vendor RSA
shut down certain social media traffic
for several months in 2011 as investiga-
tors tracked the origin back to an email.
Information gathered to target the recipi-
ent was provided freely over social net-
working sites, says Williams. "Working
in a world where our entire emerging
workforce has grown up online
and has been engineered to overshare.
Big data miners have taken notice.
"Not only are employees (current and
ex), partners and contractors beaconing
information that can be used in targeted
attacks, they also spread product and
other intellectual property (IP) over
attacks, they also spread product and
information that can be used in targeted
channels and mediums. According
to experts.

"Monitor for data leakage at the
network egress point..."

—Branden Williams, CTO of marketing at RSA

which is why so many organizations are
not even through the policy stage, let
alone the education process, Miles says.
However, even when a solid use policy
does exist, it is only as effective as the
staff’s willingness to follow it, he adds.
This is especially true with the young,
emerging workforce, according to the
"Cisco Connected World Technology
Report," released in December, which
surveyed more than 2,800 young workers
and college students in 14 countries.
Of those respondents who were
employed, seven of every 10 went
around IT policy with troubling regu-
larly. They either thought they weren't
doing anything wrong or believed they
couldn’t get their job done without
accessing personal resources. The
majority (61 percent) also felt that
their carriers or IT departments were respon-
sible for securing data downloaded to
their devices.

"This survey shows the shift in user
belief surrounding their right to choose
their own devices, their interconnect-
edness, and their more open views on
privacy," says Mary Landesman, senior
security researcher for Cisco. "Unfortu-
nately, it also shows the complex issues
organizations are facing in terms of their
sensitive data management."

As in the case of RSA, organizations
can shut down access to social networks.
RSA later restored this access, but only
for use over employees’ own personal
devices. For those wanting access
to email and other sanctioned applica-
tions on their devices, RSA engineered a
dynamic virtual desktop infrastructure
(VDI) using VMware View so users
could get to specified apps from their
devices, but not actually transfer any data
to or from their devices in the process.

Of those organizations trying to
facilitate bring-your-own-device (BYOD)
in their workplace, many are turning
to network access control (NAC) to handle
guest access from controlled devices,
which can be set up in locations identi-
fied for personal use. Like the protected
internal network, the guest network can
be monitored for data flows indicative of
IP or personal data moving onto devices
or out of the organization.
Enhanced NAC tools can also be used
to scan the security state of the device
attempts accessing. Is it configured prop-
erly? Does it contain a beaconing appli-
cation, such as malware or file sharing?

"Monitor for data leakage at the
network egress (outbound) point using
an NAC and element of network and
agent technologies," says RSA’s Williams.

By logging in, employees are also reg-
istering their feeds through the organiza-
tion, which then provides critical records
for follow-up on policy, says Thomas
Logan, CTO of HiSoftware, which
provides software and services around
collaborative data environments.
Logan also recommends using web
search engines and keywords to search for
abuses of policy across web mediums.
Brand recognition software can do
some of this, but much of the search
involves good, old-fashioned keyword
searches on behalf of the organization,
according to experts.
"Sensitive data should not be put into
unmonitored, collaborative Web 2.0
environments in the first place," Logan
says. Access should be based on need
to know, and sensitive data should be crypticled,
"Once data is published somewhere
on the web, it’s hard to redact," AIIIM’s
Miles says.
The advent of West Coast Labs’ Real Time testing program has heralded a new era of independent anti-malware product evaluation with regard to both product performance and efficacy.

As the profile of the security threat landscape has evolved in recent years, the characteristics of individual threats have morphed into a complex range of multi-faceted problems.

Targeting home users and small businesses, SMEs and major corporations, financial institutions and government organizations, these threats to personal property, corporate information assets and confidential data now know no bounds. Unrestricted by geography and time zones, they pose a continuous and permanent security risk.

Thus, the independent validation of these security products and services can no longer rely on periodic static reports to provide the most up to date and relevant product performance data.

The very nature of the threat landscape has dictated that security solutions are now complex technologies, requiring a detailed understanding of their features, functionality and interoperability with other systems in order to achieve optimum performance.

Corporate users’ risk management decisions are now bound by regulation and governance, and even today’s consumers are challenged by the need to evaluate a range of technical criteria in order to arrive at a purchasing decision.

Valid and relevant product performance data has always been a key component in the purchasing decision-making process. But nowadays the nature of that data not only has to be relevant and meaningful, it also has to be time-sensitive to the rate at which new threats are emerging and evolving.

Hence, the days of solely using static, historical performance data to guide and influence security management and purchasing decisions are passing.

**West Coast Labs Real Time Product Performance Testing**

West Coast Labs’ Real Time Product Performance validation system is probably the world’s leading program of its kind, which has anti-malware technologies on test 24x7x365.

With threats identified and captured globally in real time through its research network, which spans 25 countries, West Coast Labs tests the ability of anti-malware products to deal with such threats on an ongoing basis.

The result is genuine, real time performance data and the most accurate measurement of how an anti-malware technology deals with a threat targeting either a home network or an enterprise environment.

However, not only does the Real Time system measure performance against individual threats, it also tests the detection capabilities of products across a range of attack vectors and the full spectrum of threats to provide a complete picture of overall performance – providing critical data on which well-informed purchasing decisions can be made.

A fully-operational example of the Real Time Product Performance reporting system can be viewed at westcoastlabs.com where a selection of free anti-malware products are on test.

The Real Time test network is complemented by leading-edge systems of analysis that supplement the detection capability data with additional operational and functionality information to deliver a well-rounded report on product efficacy which is available in real time and on a continually updating basis.

**Real Time Product Performance Information Service**

With five years development experience in hand, the Real Time analysis systems have been refined to the point where they are shortly to be made available as a public-facing real time product performance reporting system. The RSA show in February 2012 and Infosecurity Europe 2012 will be the launch platforms for this service.

Known as the West Coast Labs’ Product Performance Index for Security Products and Services, its development has been fuelled by demand from corporate end users for real time product performance data.

The information service will also accumulate performance data to produce annual product and market sector-specific...
Technology Reports. They will focus on specific product groups and be regularly supplemented with quarterly updates.

Individual Technology Reports will examine anti-malware technologies included in West Coast Labs’ Checkmark Real Time and Dynamic test programs, and provide a technical overview of the real world efficacy of individual products and services against a range of pre-defined and relevant performance criteria.

**The Anti-Malware Products for SMB and Enterprise Technology Reports**

The products included in these Technology Reports are a selection of the most popular products – both certified and non-certified under the Checkmark scheme – for these market sectors.

They include products that are tested at a variety of levels within the Checkmark Certification system, including those that are registered for Baseline testing only, as well as those that are registered for additional Dynamic and Real Time testing.

All the products included in the test program are subjected to the same performance examinations, in the same network environment and are measured for performance effectiveness in the same way.

The test framework will comprise a series of tests to measure the overall effectiveness and detection capabilities of all the products included:

- Ongoing real time testing HTTP and FTP threat vectors
- Dynamic testing
- Baseline Static detection testing
- False Positive testing
- CPU/RAM measurements
- ‘Time to Detect’ analysis

The vendors whose anti-malware solutions included in the anti-malware Products for SMB Technology Report are:


Calculating a Product’s Performance Index Score

Each of the individual scores within the test framework are combined to provide a total score per product out of a maximum of 1000 points.

For example, a product achieves 97 out of 100 in Static tests, 100 out of 100 in the Dynamic tests, 308 out of 400 in the Real Time tests, 88 out of 100 in False Positives, 95 out of 100 in CPU/RAM and 50 out of 100 in Time to Detect it will produce an overall performance indicator of 738 out of 1000. This will be stated as 73.8% within the West Coast Labs’ Performance Index for Anti-Malware Products Technology Reports and updated accordingly throughout the ongoing test program.

Can you be sure the security products you use have a high enough level of independent performance validation?

AVG, Total Defense Inc, Kaspersky, McAfee, Microsoft and Webroot are taking certification to the next level.

USA Headquarters & Test Facility
West Coast Labs, 16842 Von Karman Avenue, Suite 125, Irvine CA 92606 USA - Telephone: +1 (949) 870 3250; Fax: +1 (949) 251 1586

Europe Headquarters & Test Facility
West Coast Labs, Unit 51 Oak Tree Court, Mulberry Drive, Cardiff Gate Business Park, Cardiff CF23 8RS, UK - Telephone +44 (0) 208 267 8280; Fax: +44 (0) 29 2054 8401

Asia Headquarters & Test Facility
West Coast Labs, A2/9 Lower Ground Floor, Safdarjang Enclave, Main Africa Avenue Road, New Delhi 110 029, India
Telephone: +91 (11) 4602 0622; Fax: +91 (11) 4602 0633

Full details of West Coast Labs product testing, certification and performance validation services can be found at www.westcoastlabs.com
A look at vulnerability assessment tools

We always look forward to this group because there always is something new to report. This year is no exception. Vulnerability assessment has changed over the years, and we hope to shed a bit of light on those changes.

It is important that, when performing vulnerability assessment, one keeps a perspective on exactly what one is doing. Doing a simple vulnerability scan tells little, taken by itself. Performing a penetration test in isolation is even more limiting. So, the implication is that vulnerability assessment is a holistic process. And that, it turns out, is exactly the case.

In the formative days of vulnerability assessment and penetration testing, everything was about finding the vulnerability and, if one was clear on the concept, verifying whether the vulnerability could be exploited. Today, that is only a piece of the process. Vulnerabilities – real vulnerabilities – need to be verified for their exploitability. That is where pen testing comes in. If one wants to address the vulnerability, one needs to add vulnerability management. That is not anywhere near as simple as it sounds.

This month, the biggest thing we saw was the maturing of vulnerability assessment into vulnerability management, which is good news for the information assurance community. It means that the biggest issue that we face is, at least, identifiable and manageable.

However, there are complexities that simply referring to a vulnerability as a risk don’t address. The message is clear: To manage vulnerabilities fully we need threat and vulnerability information. Then we need to apply management techniques.

Just because some vendor wants one to believe that vulnerabilities are risks, don’t take the easy way out and just fix the vulnerability. The fact is that one is likely to see far more vulnerabilities than can be fixed economically, and represent a serious hole in one’s enterprise. This is all about triage. What can one afford to fix – or not fix? That is what we’ll try to help answer in this month’s Group Test.

—Peter Stephenson, technology editor
Vulnerability assessment tools

We see a trend toward vulnerability management as opposed to simple vulnerability assessment, says Technology Editor Peter Stephenson.

We always look forward to the vulnerability assessment group because there is usually something new. This year was no exception, and certainly no disappointment. SC Lab Manager Mike Stephenson took the lead on this month’s reviews, but I got the opportunity to have a look as well.

The big, new trend is the move toward vulnerability management as opposed to simple vulnerability assessment. Vulnerability management includes several functions beyond scanning for vulnerabilities. These functions provide the means to analyze and remediate, as well as assess the vulnerabilities in the enterprise. There are few pure play vulnerability assessment tools left in the market, and those are the old, reliable mainstays of the genre. What is much more difficult to automate, though, is penetration testing, and we did not see pen testing tools participating in the trend toward vulnerability management.

The question often arises as to why one would select a pen testing tool over a vulnerability assessment tool. Now we can add in the vulnerability management tools. The fact is that one would not make that choice. Pen testing is a separate function from vulnerability assessment or management. In vulnerability assessment – and by extension, vulnerability management – we are interested in identifying all possible flaws in the enterprise. Of course, at any particular time, we cannot do that. We can only find those that have been defined up to the time we conduct our tests – so that, as we would expect, is a moving target.

Pen testing has a similar limitation, but it’s how we do pen testing that differs from how we do vulnerability assessment. Once we have completed a vulnerability assessment, we are faced with hundreds of vulnerabilities of varying severity. And, please, vendors, stop referring to vulnerabilities as risks. They are not. A risk requires a threat plus a vulnerability, together. Without one or the other, we have no risk. In fact, if the threat is not capable of exploiting the vulnerability, there is no risk. This is Information Security 101, and we need to look at the big picture. We can limit risk by managing threats, vulnerabilities or both.

Once we have discovered the vulnerabilities in the enterprise, we need to supply the threats to see if these vulnerabilities are exploitable. That is exactly what penetration testing is doing: supplying the threats. There are lots of reasons that a vulnerability does not pose a risk. One is exploitability. For example, the SQL Slammer worm cannot exploit a Linux box because it exploits Microsoft SQL Server, which does not run in Linux.

Another limitation is reachability. If the threat cannot reach the vulnerability, due to a firewall or other impediment, the risk is eliminated, or at least greatly reduced. Thus, pen testing should be used with vulnerability assessment to enhance vulnerability management.

Once one has decided what vulnerabilities actually need to be addressed – due to the existence of the vulnerability and the existence of a threat that can exploit it – one needs to decide how to address it. The usual way is to apply some identifiable form of remediation. That, it turns out, is pretty straightforward. The usual form of remediation is patching, and just about all major operating systems and application suites offer patching recommendations. These range from the Patch Tuesday mandates of Microsoft to far less formal schemes. Many of our products this month have twigged to this in a big way. They provide direct connectivity to patching sites and they perform automatic updates.

Be careful of these, though. Make certain they are not introducing patches that break something in a particular enterprise. This is a real problem and it poses a real challenge. Can one afford to test every patch in a sandbox? Probably not. That means one pays good money and takes a chance. Again, that is what this month is all about. Have a look and see what makes sense in your enterprise. The tools are here, and we are getting close to maturity in this product space.
Core Impact v12

Core Impact Professional started life as a pure-play penetration test tool. It was, at the time, the premier product of its type. Today, Impact Pro has a lot of added capability, and touches on both pen testing and vulnerability assessment. For all of that evolution, the product has retained its most beneficial benefit: it is a pen testing tool that works for both old pros and entry-level pen testers. If one has a lot of experience, the tool can do just about anything, including working in tandem with another old favorite, Metasploit, and writing one’s own exploit scripts for identifying zero-day vulnerabilities.

If, on the other hand, one is relatively new to the game, Impact Professional has a host of structured capabilities – for everything from typical pen testing tasks to client-side exploits to some sophisticated wireless testing.

We begin our testing by downloading a copy of Impact after receiving a link from Core. Here is where the controls on access to the product begin. Each copy is set up for the customer. The licensed address range is hard-coded into the copy that we downloaded. That copy is, as well, encrypted. By a separate email we receive a key to unlock the encrypted distribution.

Once we download the distribution and unencrypt it, we are ready to install, which goes smoothly. However, we have another step to consider. Core Security is good about developing new exploits to keep the tool current and, of course, if one plans on using Impact in concert with Metasploit there are new exploits for that being developed as well. So the next step is to update our copy. That is a bit time-consuming, but it is, of course, necessary.

Users receive frequent – sometimes daily – notifications of updates, so keeping a copy of Impact current is easy.

When we have our copy of Impact updated and ready for testing, we run a quick, scripted discovery scan. There are a variety of canned, or scripted, tasks that even the most novice pen tester can use. The discovery phase is a good example. Impact uses a variant of some old standbys, such as Nmap, for initial discovery scanning. We run our copy of Impact against the same test bed we have used for many of our vulnerability tests, and we add the extra dimension of real-world testing.

Core Impact has been SC Lab Approved for several years, and that has given us ample opportunity to use it on real-test scenarios. Our experience has been that Impact lives up to its advanced billing better than most products we test and use. After we run our discovery scan, we perform an automated network pen test, and Impact has no trouble placing agents on the vulnerable machines in our target range, which sits in a VMware vSphere virtual environment.

We test several of its other advanced capabilities – web vulnerabilities, client-side exploits, etc. – all with excellent results. Its biggest benefit is its production penetration testing at whatever level the organization demands.

Documentation is first-rate, as is support. Although this is not an inexpensive tool, it is priced appropriately for what it offers, and we find that it is an excellent value.

eEye Digital Security Retina CS

The Retina CS from eEye Digital Security provides a multitude of vulnerability scanning and management features and functions. Beyond simple vulnerability scanning, this product also can provide patch management and compliance monitoring. The Retina CS also can be used to scan and assess vulnerabilities in mobile devices and virtualized applications, which provides a full view of environmental vulnerabilities. Furthermore, it can integrate with popular penetration testing tools, such as Core Impact and Metasploit.

We have seen Retina grow and change a lot since we first reviewed it several years ago. The one big change we noticed – other than its growing list of features and capabilities – is that this tool has become much easier to use and is leaps and bounds better than any of its previous versions. When we first saw this product, it was installed as a software package and was plagued with Net and IIS errors. Now, all the software comes installed and ready to go on a hardware appliance, so there is no need for software installation. The web-based management interface has also substantially improved.

Configuration is almost fully automated. The initial setup is done – by way of the web interface and a short wizard – the first time the appliance is powered on. At the completion of the wizard, network scanning can begin almost immediately depending on the complexity and type of scan needed for the environment. Scans can be configured to a granular level, including the use of many compliance templates. This product also can be configured to provide patch-based remediation of vulnerabilities throughout the enterprise, including a direct plug into Windows Server Update Services. This solution provides strong compliance features and functionality, too. In fact, Retina comes loaded with many compliance templates ready to go right out of the box. It also can use Regulatory Report Packs included from eEye. These provide compliance scorecards, dashboards and trend reports to easily identify and manage compliance violations throughout the enterprise.

Documentation includes installation and full user guides. The installation guide details not only the initial setup of the Retina CS server, but also some information on base configuration and agent deployment options. The user guide provides a full, in-depth look at configuration and use of the product features. Both guides also provide many screen shots, step-by-step instructions and configuration examples in a well-organized and easy-to-follow layout.

The Retina CS comes with standard support included. This features eight-hours-a-day/five-days-a-week phone-based technical assistance, as well as access to an online portal. Access to many resources, including downloadable product documentation, an online knowledge base, and user forum are available there. Customers also can purchase 24/7 phone-based technical help as part of an ongoing agreement.

At a price starting at $8,000 for 256 IP addresses, we find this product to be an excellent value for the money. The Retina CS from eEye provides a lot of functionality – beyond just vulnerability scanning – in an easy-to-use format. It is a great value for almost any environment.
The FortiScan-3000C from Fortinet provides full agent-based and agentless vulnerability scanning, as well as patch management capabilities and remediation. With this appliance, administrators can easily manage assets throughout the network and perform full compliance-based auditing and reporting to ensure compliance and security policies are met on an ongoing basis. This tool is available both as physical hardware or as a virtual appliance that can be deployed on VMware ESX or vSphere, as well as on a Citrix Xen system.

We find this product to be easy to deploy and configure. The initial deployment took just a few minutes and we were setting up asset groups almost instantly. A feature we find quite useful is the way the FortiScan organizes administration of assets. An administrator can set up multiple administrative domains (ADOMs), and the administrator responsible can access the domain and manage assets. This provides granular control, as well as ensures that sensitive assets are only managed by an administrator that understands the necessary patch and security level of those assets.

From a compliance and reporting standpoint, this tool has a lot built in and ready to go right out of the box. The FortiScan is capable of doing an agentless network scan, which yields information throughout the enterprise, such as asset discovery and inventory management, as well as security, vulnerability and compliance posture. For more in-depth scan detail, agents can be deployed onto assets, and this will yield full patch management and remediation capabilities, as well as compliance scanning, with templates included for NIST’s Security Content Automation Protocol (SCAP) and Federal Desktop Core Configuration (FDCC), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), ISO 17799 and FISMA.

Installation documentation includes user and installation guides and a full help file. The installation guide provides a great amount of detail on installation and configuration of the appliance, as well as some initial setup steps to get started with the scanner. The user guide takes over from there and provides detailed instructions on how to use the product and navigate around the web-based management GUI. We find all documentation to be well-organized and easy to follow.

While Fortinet only provides no-cost support to proof-of-concept customers, it does offer two options as part of an annual contract. Customers can purchase support through the FortiCare program as part of an eight-hours-a-day/five-days-a-week or 24/7 package. These include both phone and email technical assistance, as well as access to an online portal loaded with product downloads and other resources.

At a price just shy of $40,000 for the appliance-based option, this product does come with a hefty price tag. However, we find it to be a good value for the money as it contains some excellent features, is easy to use, and can scan, report and remediate many platforms, along with a multitude of compliance management and reporting options.

GFI LanGuard 2011

LanGuard 2011 from GFI is a powerful vulnerability management application. This product can provide vulnerability assessment, patch management, asset remediation, asset inventory, compliance reporting and many other great features. This solution also provides flexible installation options as it can be installed on several Microsoft operating systems, so there is no need to buy expensive dedicated hardware to run it. For added flexibility, LanGuard 2011 also can run as an agentless or agent-based deployment.

Installing this tool is easy and only takes a few minutes after launching the initial setup wizard. At the completion of the wizard, all configuration and management is done via an intuitive management console application. The console itself is not only easy to navigate and use, but has a large amount of configurable options. The tab-top design of the application also enables administrators to easily navigate between scanning and remediation tasks, as well as providing a dashboard that provides an overview of information, including trends, missing patches and asset details.

We find this solution to combine a lot of powerful tools and information in one nicely designed application. We really like that all tasks, information, reporting and remediation information was all there and well-organized at the click of the mouse. This product is also not burdened by IP limitations. As long as the license supports it, this product can scan and manage up to 5,000 machines – all from a single console – and then provide automated patch management and remediation. Beyond simple patch management and vulnerability scanning, this offering also can perform many asset management tasks, including scanning for and removing unauthorized applications, checking for anti-virus applications and making sure they are up to date, and performing full software inventory throughout the environment.

Documentation includes several PDF guides. Among these are installation, administration and supplemental scripting guides. Additionally, a SmartGuide provides some basic information on deployment and planning. The scripting guide provides scripting information for advanced installations. The installation guide and administration guide, however, are the bulk of the documentation. These both provide in-depth installation, configuration and management information. We find all documentation to be easy to follow.

GFI provides the first year of technical support as part of the initial license cost of the product. After the first year, customers can purchase additional assistance as part of an ongoing agreement. Support offered by GFI includes both phone and email based technical help, downloadable bug fixes and patches, web-based chat and access to downloadable “dot” releases. Customers also get full access to an online knowledge base and a user forum.

At a price starting at around $10 per seat for 100-249 seats, we find this product to be an excellent value for the money. GFI LanGuard combines features from vulnerability assessment, patch management and remediation, inventory management and asset management in one easy-to-use application that can be installed on almost any already existing machine in the network.
Lumension Scan

Lumension Scan is a part of the larger Lumension Vulnerability Management platform. While this tool is only a part of the larger platform, it does have some good capability built in. This product can be used to scan the enterprise network and identify assets and seek out vulnerabilities and weak points on devices that can be exploited by an attack. The powerful scanning engine uses information from databases – such as Common Vulnerabilities and Exposures (CVE), Bugtraq, SANS, MS Advisory and National Vulnerability Database – to provide a comprehensive picture of vulnerabilities. Once the audit is complete, the tool provides a multitude of reporting options that provide a great amount of detail on the security posture of the environment.

Installation is straightforward and can be done on almost any Microsoft Windows machine running XP, all the way up to Server 2008. The installation itself is done by simply launching an executable file, which brings up a short installation wizard. At the completion of the wizard, the application can be launched and scanning can begin. The first thing we noticed when we brought up the application is that the interface is simple in design and easy to navigate. Configuring and starting a scan takes just a few clicks of the mouse and the scan is running within minutes of the initial setup.

We find this application to be a good news/bad news type of tool. The good news is that this scanner provides a large amount of scanning capability. This product can scan, as well as assess, several platforms, including switches, routers, Microsoft Windows, Mac OS and Linux. Scans can be configured to use credentials, and the tool even has some nice automation options available. The bad news is that it is primarily just the first step in vulnerability management. That is, it lacks options such as remediation. Other components from the suite must be purchased separately. With that said, we did find it to be a very solid scanner, which provides useful information in its scanning results.

Documentation is average at best, primarily consisting of a single user guide PDF, which includes all information – from setup through configuration and management. We find this to be quite comprehensive and easy to follow, but it lacks clear instructions in various areas and there are no screen shots or diagrams anywhere in the guide.

Lumension includes standard support as part of the subscription cost of the product. This includes eight-hours-a-day/five-days-a-week phone-based technical support, one-business-day response to email, and full access to an online knowledge base and user forum, as well as free updates and upgrades. Premium assistance is available at an added per-node cost to the subscription fee. This includes 24/7 phone technical support with four-hour response on weekends and unlimited, four-hour email response, among other advanced help features.

At a price of $6.50 per node per year for 1,000-2,499 nodes, this product is quite expensive for what it does. However, it does include some strong features and includes a solid scanning engine that provides comprehensive vulnerability scanning to a large number of devices and systems. We find this product to be an average value for the money.

McAfee Vulnerability Manager

We are an appliance that combines a powerful vulnerability scanner, penetration testing, web application scanning, compliance checks and integration into the existing environment? Well then, the McAfee Vulnerability Manager should make your short list. This appliance comes loaded to the gills with powerful onboard tools for solid vulnerability management. The McAfee Vulnerability Manager, or MVM, also packs the punch of built-in compliance and auditing through several ready-to-go compliance templates, such as Sarbanes–Oxley Act (SOX), FISMA, Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS), among others.

We find this appliance to be easy to set up and manage, but also quite easy to break. We will get into that shortly. The initial setup is quite straightforward as the appliance is pretty much plug-and-play with much of the heavy lifting of installing the applications already done out of the box. Management is done through a web-based management console that we find to be quite overwhelming at first. However, we quickly got the hang of navigating around and setting up scans and managing the configuration. This tool also gives the option of doing both credential-based and null credential scans, along with many other types of scans, for discovery, inventory and compliance.

But, all this functionality comes with possible pitfalls. We found at one point in our testing that we were able to simply change a few things on the appliance itself, including the IP address, and things started going wrong almost instantly. After our IP change, the appliance lost its ability to find the scanning engine, so we deleted it in the settings in hopes of being able to re-add it and bind it to the new IP address, but no dice. The scanning engine was lost and it would require a call with technical support to get things up and running again. With that said, this appliance has some outstanding features and functionality, and does a lot of compliance-based reporting at a granular level. It also features a dashboard that provides an excellent, in-depth look into trouble spots throughout the network at a single glance, along with risk assessment through scoring of assets.

Documentation includes a full installation guide and a user guide, along with a few other supplements. The installation guide, for the most part, covers the actual software installation that is already done when the appliance arrives, but it also includes some helpful initial configuration tasks as well. The user guide provides excellent step-by-step instructions on configuration and management of the appliance, as well as detailed examples on how to use product features and functions.

McAfee provides several support options to customers based on the size and needs of their particular installation. Customers can obtain phone- and email-based technical help, as well as access to an online support area with many resources, including a knowledge base, tutorials, product documentation and web-based chat.

At a price just shy of $12,000, we find this solution to be an excellent value for the money. The McAfee Vulnerability Manager provides a strong combination of features and function for full vulnerability management and compliance.
Internal Scan from netVigilance provides vulnerability scanning without the need of hardware or even a dedicated machine. This product is a hybrid, cloud-based offering that only requires a small agent to be installed on the machine that will be used for scanning. So, what can it do? Well, this tool features the ability to scan throughout the enterprise for vulnerabilities, and then gives information on how to remediate vulnerabilities that are found.

Installation is quite straightforward requiring a few simple steps. The initial part is downloading and installing the correct agent from netVigilance. Once the agent is downloaded and installed, all further configuration takes places via a web browser. An administrator can simply launch the web browser and log into their account on the netVigilance website to begin configuring running scans. We find this site to be quite well-organized and intuitive to navigate. We were scanning our environment within minutes of installing the agent.

This product also can use prebuilt scanning policies that are ready to go right out of the box. Some of these policies include SANS Top 20, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Sarbanes–Oxley Act (SOX), and vulnerabilities are taken from several databases. This provides comprehensive vulnerability results across multiple platforms. Scans also can be run based on several templates – from a safe scan, which does not perform any brute force-type attacks, all the way up to a full-scale, brute force, denial-of-service-type scan ensuring the security of any type of system. The overall best part of the system is that not only is it easy to manage, but it does not require any extra hardware, so there is no overhead or additional operating costs.

Documentation includes a short user guide in PDF format. This features all the necessary information to get started using the product and becoming familiar with how to run scans and generating reports. This also explains in excellent detail how to navigate the web-based interface and how to download and install the agent. We find this PDF to be easy to understand and well-organized with many screen shots, configuration examples and easy, step-by-step instructions.

NetVigilance offers no-cost support as part of the purchase price for 12 months. This includes email and phone technical help, as well as installation assistance. Also included are ongoing weekly updates and product upgrades for the 12 months. Customers also can choose to obtain fee-based support options, which entails on-site and 24/7 technical assistance. Customers also have access to an online area, which offers a user forum and many resources, including downloads, security advisories and an FAQ section.

At a price just shy of $12,000 for 1,024 IP addresses, we find this product to be an excellent value for the money. The netVigilance cloud-based scanning service offers all of the functions of a full vulnerability scanner and reporting engine without having to obtain extra hardware – or worry that existing hardware is not going to have sufficient resources to perform tasks correctly.

**GROUP TEST | Vulnerability assessment**

**netVigilance Internal Scan - Cloud**

Internal Scan from netVigilance provides vulnerability scanning without the need of hardware or even a dedicated machine. This product is a hybrid, cloud-based offering that only requires a small agent to be installed on the machine that will be used for scanning. So, what can it do? Well, this tool features the ability to scan throughout the enterprise for vulnerabilities, and then gives information on how to remediate vulnerabilities that are found.

Installation is quite straightforward requiring a few simple steps. The initial part is downloading and installing the correct agent from netVigilance. Once the agent is downloaded and installed, all further configuration takes places via a web browser. An administrator can simply launch the web browser and log into their account on the netVigilance website to begin configuring running scans. We find this site to be quite well-organized and intuitive to navigate. We were scanning our environment within minutes of installing the agent.

This product also can use prebuilt scanning policies that are ready to go right out of the box. Some of these policies include SANS Top 20, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Sarbanes–Oxley Act (SOX), and vulnerabilities are taken from several databases. This provides comprehensive vulnerability results across multiple platforms. Scans also can be run based on several templates – from a safe scan, which does not perform any brute force-type attacks, all the way up to a full-scale, brute force, denial-of-service-type scan ensuring the security of any type of system. The overall best part of the system is that not only is it easy to manage, but it does not require any extra hardware, so there is no overhead or additional operating costs.

Documentation includes a short user guide in PDF format. This features all the necessary information to get started using the product and becoming familiar with how to run scans and generating reports. This also explains in excellent detail how to navigate the web-based interface and how to download and install the agent. We find this PDF to be easy to understand and well-organized with many screen shots, configuration examples and easy, step-by-step instructions.

NetVigilance offers no-cost support as part of the purchase price for 12 months. This includes email and phone technical help, as well as installation assistance. Also included are ongoing weekly updates and product upgrades for the 12 months. Customers also can choose to obtain fee-based support options, which entails on-site and 24/7 technical assistance. Customers also have access to an online area, which offers a user forum and many resources, including downloads, security advisories and an FAQ section.

At a price just shy of $12,000 for 1,024 IP addresses, we find this product to be an excellent value for the money. The netVigilance cloud-based scanning service offers all of the functions of a full vulnerability scanner and reporting engine without having to obtain extra hardware – or worry that existing hardware is not going to have sufficient resources to perform tasks correctly.

**DETAILS**

Vendor: netVigilance Internal Scan - Cloud

Price: $11,994 for 1,024 IP addresses

Contact: netvigilance.com

Features: ★★★★★

Ease of use: ★★★★★

Performance: ★★★★★

Documentation: ★★★★★

Support: ★★★★★

Value for money: ★★★★★

**OVERALL RATING** ★★★★★

Strengths: Cloud-based full scanning with no overhead.

Weaknesses: None that we found.

Verdict: We liked this tool a lot. As a foray into cloud-based vulnerability assessment, this is well worth considering, especially for its value.
Rapid7 Nexpose Enterprise Edition

The Nexpose Enterprise Edition appliance from Rapid7 is another tool that has grown into a vastly different product over the years. This latest version we believe is the best yet. This solution has gone from its early days as pretty much just a vulnerability scanner to a full-scale vulnerability management tool. With this appliance, administrators can manage the entire vulnerability lifecycle – from discovery of assets through reporting and mitigation – all from one place. The Nexpose incorporates the ability to run more than 75,000 vulnerability checks against more than 22,000 vulnerabilities across multiple operating systems, databases, web applications and virtual assets throughout the enterprise.

Getting started is as easy as plugging the device in and turning it on. The appliance can grab a dynamic host configuration protocol (DHCP)-assigned IP address, or a user can easily enter one manually using the LCD screen on the front of the appliance. There is no need to look up monitors or keyboards just to get an initial configuration. Once the IP address is assigned, the Nexpose web-based management console can be accessed from any web browser on the network. The interface itself is easy to navigate and has a clean and organized look and feel. We also find running scans and using the appliance functions to be easy and straightforward.

This appliance does more than just simple vulnerability scanning. With the Nexpose, the scan is only the first step, and once the initial scan is complete this appliance can do a whole host of analysis. This product can do various correlations and risk analysis based on the results of a scan, including analyzing overall possible exposure to risks, including malware and dangerous exploits. After the analysis is complete, administrators are shown what Rapid7 calls a Remediation Roadmap, which details how to remediate and repair security holes throughout the network. This appliance also comes preloaded with many compliance templates.

Documentation includes a quick-start and a full administrator guide. The quick-start guide is short, but includes a lot of helpful steps on how to get the appliance up and running to gain access to the web-based management console. We find both guides to be well-organized and easy to follow and understand. Rapid7 includes support as part of the annual license fee. Customers have access to both phone- and email-based technical assistance, along with access to an online knowledge base, user forum and software updates, upgrades and fixes. Customers who require more than the basic plan can purchase additional options, which includes an upgrade to full 24/7 technical help along with faster response times.

At a price of $22,900, this appliance does carry quite the price tag. However, we do find it to be a great value for the money. The Nexpose incorporates a lot of great features and functionality that is both easy to use and highly comprehensive. We have seen this product grow and mature substantially over the years, and we are sure it is not done growing yet.

Saintscanner and Saintexploit

Last year at about this time, we were introduced to Saintbox from Saint and found it a wonderful marriage of all the Saint products in one easy-to-use appliance. Well, this year Saintbox is back and it is still quite the product. The tool brings together all the various Saint modules, such as Saintscanner, Saintexploit and Saintwriter, all in one convenient package. Using these modules together provides full scanning and penetration testing capabilities to ensure systems are secure throughout the environment.

Some may remember Saint’s early days when to install and use the product one had to have an available Linux box, install all the modules, and then go through a license process before finally starting to use the product. This whole process has been simplified using the Saintbox. The appliance itself comes preloaded with all the necessary software, so users no longer have to touch Linux to get it running. At the first power-up of the appliance, the user is taken through a short on-screen setup wizard that installs the initial network and appliance settings. From there, all further management and administration is done using an intuitive web-based interface. The one thing we really find appealing about the interface is that it has become more organized and easier to use with better integration across all the various components.

So what can you do with Saintbox? Well, the better question is, what can’t you do. This product starts with an initial scan that can be run from various prebuilt templates or a custom template designed by the user. These scans can have various goals in mind, including vulnerability scanning, configuration compliance testing and penetration testing. At the completion of the scan, Saintwriter can be used to generate in-depth reports and analysis of the security posture throughout the environment. Also included are several compliance templates, and the scanner uses references from several databases.

Documentation is comprised of a quick-start guide and help file. The quick-start guide details how to connect the Saint appliance to the network, obtain the license key and start the first scan, all in clear, step-by-step instructions. The help file provides further information on how to use the product and configure functions with many nicely illustrated screen shots, step-by-step instructions and configuration examples. We find all documentation to be complete and well-organized.

Saint offers base-level phone and email support to customers as part of the product price. Phone technical help is available during business hours, Monday through Friday. Customers also have access to an online portal, which includes documentation, a vulnerability knowledge base and an FAQ section. Customers who require 24/7 assistance can purchase it as part of an extra cost.

At a price of $19,000 for a 1,000 IP scanning license, we find this product to be a very good value for the money. The Saintbox, loaded with Saint Enterprise, combines all the tools needed for solid vulnerability management – from simple scanning through compliance and penetration testing – ready to go right out of the box.
SecPoint Penetrator

The Penetrator from SecPoint is an interesting tool. The first thing to note about this device is its form factor. Unlike traditional hardware appliances, this product is available as both a rack mount server, but also as a smaller Dell OptiPlex unit. This helps make the Penetrator a slightly portable, less bulky option for mobile penetration testing. However, do not be deceived by its small appearance. This product packs a punch. It is capable of doing an onslaught of vulnerability and penetration testing along with built-in Wi-Fi auditing.

We were first introduced to this product last year, and believe that this year’s model is much better than the previous one. Setup and configuration is quite easy, requiring only a few simple steps to get the appliance up and running. After the initial configuration is complete, all further administration and management is done via a well-designed, web-based management interface. We notice that the interface has a more fluid feel than it had last year, and screens seem to load much faster. Aside from the performance, not much has changed in the interface. We find it to be intuitive and easy to navigate. Setting up scans was a breeze.

The Penetrator offers a strong combination of vulnerability scanning and penetration testing. Using this appliance, administrators can scan the network, see where there are vulnerabilities, and easily find ways to fix them before they are exploited by an attacker. The device can use denial-of-service-type attacks, as well as other exploits, to ensure enterprise devices are secured against incursions.

One of its most interesting features, however, is its ability to audit Wi-Fi security. Using an optional antenna, the Penetrator can be set to try to brute force attack against both WEP and WPA/WPA2 encryption, and work to discover the passphrase to attach to the network. After scanning and auditing is complete, administrators can easily run reports and have them generated in a variety of formats, including XML, PDF and HTML.

Documentation includes an easy-to-follow quick-start guide, which illustrates in good detail deployment options, initial setup procedures and an overview on how to navigate the web-based interface. Also provided is a full administrator guide that includes more in-depth detail on how to configure and use the features. Both had a lot of screen shots, easy-to-follow, step-by-step instructions and configuration examples in a well-organized format.

SecPoint offers complete 24/7 support to customers at no extra cost. Technical assistance includes live, web-based chat, phone, email and Skype. Customers also can access a small help area on the website, which includes resources, such as product documentation, a knowledge base and a detailed FAQ section.

The price of the Penetrator can vary greatly depending on the size of the environment and the type of hardware needed. With a base price just shy of $11,000, we find this product to be a good value for the money. It provides some solid functionality, both on the side of vulnerability scanning and also penetration testing, along with the added value of Wi-Fi auditing.

Secunia Corporate Software Inspector (CSI)

The Corporate Software Inspector (CSI) from Secunia takes an interesting approach to vulnerability assessment. This product focuses primarily on application-based vulnerabilities, rather than just open ports or other security holes. The CSI can assess the security state of all installed programs running throughout the enterprise and suggest possible remediation steps to fix any potential security risks or outdated applications. Furthermore, this solution can assess applications running on Microsoft Windows machines, as well as Mac OS X platforms.

Installation is simple and quick, launched from a small executable, which initiates a short setup wizard. At the completion of the wizard, the application can be run and the main console opens. The management console has an organized layout. The first time it is run, it shows a few brief configuration steps to get started. We also find it quite easy to navigate around the interface, as well as configure scans. The navigation structure of the interface is also quite well organized with intuitive sections for easy configuration and browsing. One of the nicest features of the console is a fully customizable dashboard, which starts out as a blank canvas onto which multiple modules can be dropped right in. There are many modules to choose from and all provide a clean overview of previous scan information and historical data at a glance.

The main driving force of this product is the database backend that is hosted by Secunia and interfaces directly with the application. The Secunia Advisory and Vulnerability Database includes complete and constantly updated information that is always available on demand to the front-end installed application, so there is less time spent updating the product and more time spent scanning and analyzing results. CSI also can be integrated with an onsite Windows Update Server to easily, and with little administrator interaction, deploy Microsoft Windows-based updates to assets.

Documentation includes a single user manual that covers the product from installation all the way through advance configuration and use of features and functions. We find this to be well organized and to include an excellent amount of information without being overly lengthy or hard to follow. The guide is also enhanced with many clear, step-by-step instructions, configuration examples and screen shots.

Secunia provides no-cost phone- and email-based technical support to enterprise customers during their subscription period. Customers also can opt for additional assistance as part of an agreement. Additional levels include faster response times and onsite installation and training. Also available to all customers is access to an online portal, which includes a user forum and knowledge base. At a price starting at $2,840 per year for the small business version of the product, we find this to be a good value for the money. Secunia Corporate Software Inspector provides full application vulnerability scanning that is always updated and ready to go to ensure solid security among all applications throughout the enterprise environment.
Tenable Network Security
Nessus ProfessionalFeed

Back again this year is our old friend Nessus from Tenable Network Security. For as long as most can remember, this has been a necessary tool in any vulnerability assessment toolkit. It is easy to see why. Nessus has become increasingly lightweight and easier to use over the years, and this version is no different. It can scan many devices on the network for vulnerabilities, and its device list is always growing longer. Nessus can scan Microsoft Windows and Linux systems, databases, web applications and Cisco routers and switches, among many others.

Installation is straightforward and only takes a few minutes. Initial setup is done by running a single installer, which, after a short setup wizard, installs both the Nessus server and a shortcut to the company’s web interface. After installation is complete, the server can be engaged by entering an activation code. Once activated, it immediately begins pulling down the various plug-ins and updates for the scanner. All scanning and administration is done via the web-based management console, which relies on Adobe Flash. We find this console to be easy to navigate and intuitive to use.

The Nessus scanner uses vulnerability information from both Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) v2, and can perform a multitude of compliance and configuration audits using various standards. This product also can generate reports in various formats, including HTML and Nessus XML. While this tool is strictly a vulnerability scanner, it can be a valuable addition to a larger vulnerability management plan, as it includes several auditing and scanning templates ready to go out of the box. Scanning policies also can be highly customized to meet the needs of pretty much any type of environment, and it can include both credential-based and null credential scans.

Documentation consists of installation and user guides, along with other supplemental materials, such as compliance and credential checks manuals. The installation guide provides detailed information on installing the Nessus scanner on either a Windows or Linux box, along with preinstallation and deployment option information. The user guide illustrates all other necessary details on configuration of the scanner and using the product. Tenable offers email- and web-based support to customers who only are using the Nessus Scanner. Customers who integrate the tool into the full Tenable Security Center, at an additional cost, receive phone-based technical support and ongoing help also is available as part of the purchase price for the first year. After the first year, customers can then purchase assistance as part of an agreement at a cost of 20 percent of the original license cost. We would like to see a knowledge base as part of the support site.

At a price of $1,200 per year per scanner, this product is a reasonable value for the money. However, users benefit a lot more if it is integrated into the Tenable Security application, which adds substantial vulnerability management functionality, but also adds cost. Overall, this product can be a useful tool and should be considered as a part of vulnerability assessment, but it’s not a complete vulnerability management tool.

Zoho ManageEngine
Security Manager Plus

ManageEngine Security Manager Plus from Zoho is a full-scale tool that provides a lot of punch in a relatively tiny package. With this application, administrators can proactively scan the network for vulnerabilities and directly remediate them to ensure compliance throughout the enterprise.

This product uses a mix of vulnerability scanning, open ports detection, patch-level scanning and Windows file, folder and registry change detection to find and repair possible trouble spots on the network. All functionality is integrated into a simple and easy-to-use application.

Installation of the application is quick and straightforward. It is installed by running a short setup wizard that engages all the necessary components, including the web-based administration interface. After installation is complete, the web-based management interface is used to perform all configuration and management of the application. We find this interface to be well organized and intuitive to navigate. One thing we instantly noticed about the interface is that not only did it have a clean and organized look, but it also had a fluid feel. We find it to be quite effortless to move within the interface with little lag and redraw.

Aside from the look and feel of the interface, we also find this product to have a complete feature set with many configurable options. Scans could be configured to do credential-based scanning using Windows or Linux credentials, as well as null scans. At the completion of the initial scan, we were presented with many charts and graphs that were all clearly displayed on the dashboard of the management interface, and we were able to drill down into several of the dashboard elements. Finally, coming full circle from scan to remediation, this product integrates direct remediation and patch management right into the interface.

Documentation is slightly weaker than we like to see. The product contains a help file, as well as a separate PDF user guide. Both contain pretty much the same information, covering the product all the way from installation through configuration and management. While we find both documents to provide a lot of great information, there is a definite lack of step-by-step instructions, screen shots and diagrams. We find that features like these help aid in the installation and configuration process and they should be present.

Zoho provides free 24/7 phone and email support as part of its 30-day evaluation period, and ongoing help also is available as part of the purchase price for the first year. After the first year, customers can then purchase assistance as part of an agreement at a cost of 20 percent of the original license cost. We would like to see a knowledge base as part of the support site.

At a price starting at $695 per year for 25 systems and going all the way up to about $6,000 per year for 1,000 systems, this product can be quite expensive over time. While it has a strong feature set and some good functionality, we find it to be an average value for the money for larger environments. On the other hand, it is a good value for smaller environments looking to gain a sleek vulnerability management platform at a reasonable cost.
Enterprise whole disk encryption done right

There are lots of products that claim to do preboot whole disk encryption. But there aren’t a lot of them that can claim to do it over the network. While several products can, pretty much, get to the same point without doing it over the network, the network is a key component and, if one ignores the network, one essentially ignores the enterprise.

This month’s First Look specializes in whole disk encryption and, unlike many other products, can do the entire process of encryption and encrypted disk access throughout the enterprise. It’s a big deal as many of the products that claim to do it really don’t.

First, and probably most telling, is that PBConnex is a combination of whole disk encryption and access management. That, really, is not too surprising given that some smart people have hypothesized that all that really is needed to protect the enterprise is to encrypt everything. Not too practical today, I would guess, but the premise is well worth considering.

There are several challenges to overcome when one is restricting asset access on the enterprise based on encryption. The big one, in my view, is what happens when the user cannot access the network? Is the computer a dead piece of meat on the enterprise based on encryption. The big one, in my view, is what happens when the enterprise cannot encrypt everything. Not too practical today, I would say, but the premise is well worth considering.

The answer is simple, really. Everything is encrypted – regular files, unallocated space, boot sector, directory – indeed, everything that would allow an attacker to see what is on a secure disk.

There are a lot of little – but important – aspects to the product. For example, it handles self-encrypting devices. It really doesn’t care if the target is Windows or Linux in that regard. Virtually all of the action takes place on the SecureDoc Encryption Server. This is where keys are managed, authorization happens (if the encryption is over the network) and authorization occurs. It is a clean solution to the challenges of whole disk encryption over the network.

Of course, encryption of external attached devices is a given. If one is using flash drives or USB disks, these can be managed as easily as the primary hard drive. An extension of this is the ability to create encrypted containers on removable media, complete with a reader that allows recipients of the encrypted containers to unencrypt them even if they do not have the encryption tool itself. That includes CDs and DVDs – with the caveat that an external version of the reader must be available since it cannot be included directly with the burned disk.

There are neat capabilities, such as supporting the hardware password manager in Lenovo computers. Overall, this is an extraordinarily flexible, well thought-out and effective application of encryption. We like it a lot, and it is well worth your consideration.

– Peter Stephenson, technology editor
State breach rules need revamp

If you trust a company with your personal data and it loses your information to cyber criminals, should the company tell you? That’s a question with an obvious answer. What if the company entrusts it to a third-party and they lose it? Here there’s no clear legal answer. Generally, it is agreed that it’s the original company’s responsibility. But, there’s no federal law, so security professionals have to rely on a patchwork of state laws that leave it unclear exactly who is responsible for notifying consumers of data breaches—an enormous headache.

For example, when thousands of names and email addresses were compromised in the breach of online marketing giant Epsilon every one of its clients—major companies like Best Buy and Capital One—stepped in and sent out notifications. Maddeningly, with different laws in different states, none of the companies really knew their legal responsibilities, so they just blanketed their email lists with notifications.

Everyone agrees, the goal of the various data breach notification laws, beside their attempt to entice companies to prioritize security, is to make consumers more cautious about the information they disclose. Unfortunately, the laws and their murky requirements have resulted in so many notifications that they are having the exact opposite effect on consumers, while saddling IT professionals with extremely time-consuming responsibilities.

Admittedly, the emergence of a business model where companies offer a free-service in exchange for personal data may spur a federal breach disclosure law, or even more expansive legislation. Consumers are already allowing these companies to peddle their personal data to third parties. One significant overstep in personal data privacy, and that may bring about much stricter regulations than those that are currently on the books.

Worsening the problem is that consumers tend to trust the larger, more well-known companies. And it’s true, these organizations have more rigorous processes for vetting third parties. But, invariably, it’s just a matter of time until they sell customer data to a wolf in sheep’s clothing.

Furthermore, a generation of internet users has grown up sharing much more personal information than their wary elders would. If data disclosure laws are burdensome now, they’ll overrun IT departments when the Facebook generation enters the workforce.

Regulation isn’t always the answer. Yet, here, the fragmented approach taken by the states has made notifications meaningless, expensive and time-consuming. Current data breach laws simply don’t provide users with understandable guidelines for how to adjust their behaviors. Simple, actionable rules would ensure data breaches get the gravitas they deserve.

Ultimately, the standard of care for data is evolving, and measures once considered high security are now easily bypassable. And while social norms concerning online privacy and security are dynamic, a practical, actionable vigilance can be engrained in consumers and businesses alike with the appropriate approach to data breach notifications.

Jeff Schmidt is the founder and chief executive officer of JAS Global Advisors, and a two-decade veteran of the information security industry.

Can your network security stop APTs? FireEye can.

Over 95% of networks are compromised as advanced attacks easily evade traditional and next generation signature-based firewalls, IPSs, AV and gateways.

The best and brightest across every industry are protecting themselves from zero-day and APT attacks with FireEye.

FireEye... the leader in stopping zero-day and APT attacks!

Contact FireEye now for a free assessment.
www.FireEye.com/StopAPTs
World’s No. 1
Antivirus and Internet Security

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

Virus Bulletin Awards  Success ratio (%)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>25</th>
<th>50</th>
<th>75</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET</td>
<td>97</td>
<td>91</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td></td>
<td></td>
<td></td>
<td>79</td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
<td>76</td>
</tr>
<tr>
<td>Sophos</td>
<td></td>
<td></td>
<td></td>
<td>68</td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td></td>
<td></td>
<td>67</td>
</tr>
<tr>
<td>GDATA</td>
<td></td>
<td></td>
<td></td>
<td>68</td>
</tr>
<tr>
<td>McAfee</td>
<td></td>
<td></td>
<td></td>
<td>67</td>
</tr>
<tr>
<td>TrendMicro</td>
<td></td>
<td></td>
<td></td>
<td>67</td>
</tr>
</tbody>
</table>

Selected Antivirus Vendors (not a complete list)

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