How secure is the cloud and the use of social networks? What’s up with mobile malware? We take a backward glance at 2011’s major developments. As well, we pick the year’s top luminaries and call out the products and events that shaped the IT security field.
CAN YOU SEE EVERYWHERE AT ONCE?
You can’t stop threats if you can’t spot them. That’s why HP Enterprise Security offers proven solutions that deliver context-aware visibility into security risk. There’s no better way to proactively detect security issues and drive situational awareness across your applications, operations, and infrastructure. The HP Security Intelligence and Risk Management platform provides integrated correlation, application protection and network defenses that can secure modern IT environments from sophisticated threats.

For more information go to www.hpenterprisesecurity.com

Advanced protection against advanced threats.

Copyright ©2011 Hewlett-Packard Development Company, L.P.
Editorial

Summing up the year that was

I’m a Johnny Cash fan. One of his coolest tunes is a duet with Merle Haggard during which they sing, “That ole’ wheel, it’s gonna roll around again…”

They were singing about karma, of course, but the idea of things coming full circle, of trends being cyclical, can be inferred here.

This thought could be applied to the information security industry this year. However, in my mind, there does seem to be a new development. So, this left me thinking: If I were to write a headline to sum up 2011, what would be the right fit? Hacktivists wreak havoc in 2011. 2011: The year of the data compromise. Data security goes mainstream in 2011.

Perhaps all these ideas work. After all, we had a mightily busy year.

Arguably, more than any year before, we saw over the last 12 months a few prominent groups rise up to call out what they perceived as questionable practices adopted by government and private entities alike. Their compromises seemingly had no end, and often strived to promote their various political ideologies.

This year also saw organizations of all sizes across all markets hurling countless data breach notifications through cyberspace to warn millions of customers about some compromise of their personally identifiable information. To say it has been a difficult year for IT security pros is an understatement.

So, could 2011 be coined the year of the breach? Sure. Many experts say, however, it’s bound to get worse given the volume of electronic data and the many cybercriminals who are continually honing their skills to get at it.

And this brings me to my last point. At no time in our history have we seen individuals and organizations so dependent on IT. Let’s count the ways.

There’s the bring-your-own-device movement, along with an astronomically growing number of endpoints. Companies and government agencies are looking for cost-savings in a dark economy through cloud computing and paperless operations. Every walk of life is tethered to some social networking application. Meanwhile, legislators are worried about protecting electronic records, with compliance mandates becoming finetuned to integrate security technologies, policies and requirements.

Has cybersecurity gone mainstream? I think, yes. As a matter of fact, I think I’ll tweet this as I imbibe my margarita at this year’s holiday party and further ponder what this might mean for us all in 2012. Here’s to you and yours for a prosperous and data security-filled New Year!

Illena Armstrong is editor-in-chief of SC Magazine.

IT made easier with EdgeWave

We know there are things you’d rather be doing. Spend less time managing your information security with EdgeWave’s award-winning iPrism Web Security and ePrism Email Security Suite. We believe in developing innovative solutions that meet the needs of our customers now, and in the future. With EdgeWave SCM solutions:

• Simple deployment has you up and running in 30 minutes or less
• Easy to configure and fully-hosted solutions mean low-to-no maintenance
• Revolutionary real-time defense against botnets and emerging threats
• Fully integrated email security services for threat protection, DLP, Encryption, Continuity and Archive
• Live, 24/7, US-based support team with customer satisfaction rates over 95%

As a special offer for SC Magazine readers, for a limited time, we’ll give you $100 just for trying our Web or Email security solutions. Already have a solution in place? We’ll make it very easy to switch.

Visit www.edgewave.com/SCMag for more information or call us at 1-800-782-3762 and mention SC Magazine Innovator.

Has cybersecurity gone mainstream? I think, yes.”
Mobile security
To safeguard handheld devices used by business execs is a constant trial — one that rarely is satisfactorily remedied. Businesses must leverage people, processes and technologies to enable systems to be resilient. We learn from experts.

APTs
Some say advanced persistent threats (APTs) are a combo package of attack types complete with long-term information-siphoning that can bring companies to their knees. Others, however, believe APT has become a type of well-funded marketing term used by vendors to scare nervous or confused executives into buying their products. We take a deeper look at this term used by vendors to scare nervous executives into buying their products.

Desktop Virtualization. A better way to minimize risk without compromising business productivity.
You need a security approach that can evolve to adapt to the ever-changing threat landscape. Citrix desktop virtualization is a better way for companies to fortify security without freezing business productivity. It provides the foundation for a layered security strategy that enables desktops, applications and data to be delivered securely, on demand, to any device.

Traditional thinking about security can have a chilling effect on your business.

SC WORLD CONGRESS
Dec. 8
eSymposium: Fending off attacks from all sides
The rate at which attackers have breached enterprise systems has risen rapidly. Whether spearheaded by cybercriminals, hacktivists, state-sponsored offenders or insiders, these assaults highlight the need to be proactive and adaptive. Having the most robust risk management programs is critical. In short, such programs must leverage people, processes and technologies to enable systems to be resilient. We learn from experts.

WHAT IS SCWC 24/7?
SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

ON DEMAND
APTs
Some say advanced persistent threats (APTs) are a combo package of attack types complete with long-term information-siphoning that can bring companies to their knees. Others, however, believe APT has become a type of well-funded marketing term used by vendors to scare nervous or confused executives into buying their products. We take a deeper look at this term used by vendors to scare nervous executives into buying their products.

Mobile security
To safeguard handheld devices used by business execs is a constant trial — one that rarely is satisfactorily remedied. Businesses must leverage people, processes and technologies to enable systems to be resilient. We learn from experts.

APTs
Some say advanced persistent threats (APTs) are a combo package of attack types complete with long-term information-siphoning that can bring companies to their knees. Others, however, believe APT has become a type of well-funded marketing term used by vendors to scare nervous or confused executives into buying their products. We take a deeper look at this term used by vendors to scare nervous executives into buying their products.

Desktop Virtualization. A better way to minimize risk without compromising business productivity.
You need a security approach that can evolve to adapt to the ever-changing threat landscape. Citrix desktop virtualization is a better way for companies to fortify security without freezing business productivity. It provides the foundation for a layered security strategy that enables desktops, applications and data to be delivered securely, on demand, to any device.

Traditional thinking about security can have a chilling effect on your business.

Visit www.citrix.com/security
India was top producer of zombie IP addresses

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

DataBank

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

- **HIGH-LEVEL ACTIVITIES**
- **MEDIUM-LEVEL ACTIVITIES**
- **LOW-LEVEL ACTIVITIES**

**WILMINGTON, DEL.** – Three unencrypted backup tapes containing the names and Social Security numbers of 1.6 million individuals went missing from Nemours, a children’s health system.

**ATHENS, GA.** – The personal data of 18,931 staff and faculty members at the University of Georgia in 2002 was found accessible online. An administrative file was placed on a publicly available web server where it remained from at least 2008 until 2011.

**DOMINICAN REPUBLIC** – Hackers defaced the government website, likely in protest of alleged police killings and torture uncovered in an Amnesty International report.

**MONTANA** – Authorities in the Treasure State warned users to be on alert for smishing attacks, in which victims are called or contacted via SMS and asked to provide credentials or personal data.

**TENNESSEE** – Thieves planted skimming devices on ATMs around the Nashville and Chattanooga areas to capture users’ debit card numbers. Two men were arrested and charged in connection with the crimes.

**TANZANIA** – The East African Community organization, based here and made up of members Kenya, Uganda, Tanzania, Rwanda and Burundi, is expected to adopt uniform laws addressing cybercrime. The plan for common legislation comes as the nations are experiencing a boost in e-commerce and e-government services.

**FINLAND** – The Nordic nation is planning to build an offensive cyberspace capability, possibly as a means of launching counterattacks against future threats. The project’s purpose now, however, is to conduct penetration tests against its own networks to evaluate its protection level.

**U.K.** – The head of the Ministry of Defense’s cybersecurity program told The Daily Telegraph that cyberattacks pose the largest risk to the nation’s security, given that hackers are regularly making off with intellectual property. He placed much of the blame on “poor cyber hygiene.”

**PALESTINE** – Distributed denial-of-service attacks struck servers here, knocking out web service to the West Bank and Gaza. Officials said they don’t know the motive, but the attacks began soon after Palestinians won UNESCO membership.

**JAPAN** – Hackers targeted both houses of the nation’s parliament in an attempt to access internal documents. In their raid on the lower house, intruders stole data by tricking users into loading malware. Upper house members also reported receiving suspicious emails, but officials said no data was taken.

**MONTANA** – Authorities in the Treasure State warned users to be on alert for smishing attacks, in which victims are called or contacted via SMS and asked to provide credentials or personal data.

**TENNESSEE** – Thieves planted skimming devices on ATMs around the Nashville and Chattanooga areas to capture users’ debit card numbers. Two men were arrested and charged in connection with the crimes.

**DOMINICAN REPUBLIC** – Hackers defaced the government website, likely in protest of alleged police killings and torture uncovered in an Amnesty International report.

**WILMINGTON, DEL.** – Three unencrypted backup tapes containing the names and Social Security numbers of 1.6 million individuals went missing from Nemours, a children’s health system.

**ATHENS, GA.** – The personal data of 18,931 staff and faculty members at the University of Georgia in 2002 was found accessible online. An administrative file was placed on a publicly available web server where it remained from at least 2008 until 2011.

**MONTANA** – Authorities in the Treasure State warned users to be on alert for smishing attacks, in which victims are called or contacted via SMS and asked to provide credentials or personal data.

**TENNESSEE** – Thieves planted skimming devices on ATMs around the Nashville and Chattanooga areas to capture users’ debit card numbers. Two men were arrested and charged in connection with the crimes.

**DOMINICAN REPUBLIC** – Hackers defaced the government website, likely in protest of alleged police killings and torture uncovered in an Amnesty International report.
ThreatStats

There were 1,861,656 foreign attacks last month.

**Spam**

World’s most prevalent 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>hostrec.net</td>
<td>78</td>
</tr>
<tr>
<td>2</td>
<td>telecomitalia.it</td>
<td>74</td>
</tr>
<tr>
<td>3</td>
<td>telecomrica.com.ar</td>
<td>59</td>
</tr>
<tr>
<td>4</td>
<td>unicom-cn</td>
<td>54</td>
</tr>
<tr>
<td>5</td>
<td>unicom-hl</td>
<td>44</td>
</tr>
<tr>
<td>6</td>
<td>hinet.net</td>
<td>43</td>
</tr>
<tr>
<td>7</td>
<td>iliad.fr</td>
<td>41</td>
</tr>
<tr>
<td>8</td>
<td>telecomrica.com.br</td>
<td>41</td>
</tr>
<tr>
<td>9</td>
<td>chinaren-rj</td>
<td>41</td>
</tr>
<tr>
<td>10</td>
<td>shawcable.net</td>
<td>39</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

- 300% Education (v)
- 154% Food & beverage (v)
- 127% Retail & wholesale (v)
- 108% IT & telecom (v)
- 92% Government (v)
- 81% Banking & finance (v)
- 69% Health care (v)

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 nearly 40%

- India 18.6%
- Brazil 7.8%
- Russia 6.5%
- Other Europe 12.9%
- Other Asia 18.7%
- Vietnam 8.6%
- China 4.7%
- Pakistan 4.9%
- Indonesia 4.1%

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

Source: Commtouch Software Online Labs

**Top breaches of the month**

Data loss

- Tricare (San Antonio, Texas): The car theft of backup tapes resulted in the exposure of protected health information from patients of military hospitals and clinics. 4.9 million records.
- Nemours (Wilmington, Del.): Three unencrypted computer backup tapes were reported missing. 1.6 million records.
- Neurological Institute of Savannah (Savannah, Ga.): The car theft of a computer hard drive may have exposed patient information. 63,425 records.

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

542,361,948

Source: RSA Anti-Fraud Command Center

**Top 5 attacks used by U.S. hackers**

1. Clampi trojan
2. Downloader trojan
3. Zeus trojan
4. TDSS Downloader trojan
5. Sinowal trojan

**Top 5 attacks used by foreign hackers**

1. Butterfly bot
2. Downloader trojan
3. Zeus trojan
4. SpyEye trojan
5. Sinowal trojan

There were 1,066,947 attacks in the United States last month, primarily originating from New York; Cambridge, Mass.; Atlanta; Dallas; and Chicago. There were 1,861,656 foreign attacks last month, primarily originating from Moscow; Toronto; Beijing; Guangdong, China; and Amsterdam, Netherlands.

**Top 10 spyware threats**

Trojans still on top

1. Trojan.Win32.Generic: trojan 33.37%
2. Yontoo (v) Adware (General): adware (general) 1.77%
3. INF.Autorun (v): trojan 1.30%
4. Trojan.Win32.Adware: adware (general) 1.23%
5. Worm.Win32.Downad.Gen (v): worm/W32 1.02%
6. Trojan.Win32.Jmpframe (v): trojan 0.98%
7. Backdoor.Win32.Cybot.crg (v): backdoor 0.98%
8. Pinball Corporation. (v): adware (general) 0.88%
9. Trojan-Spy.Win32.Zbot.gen: trojan 0.84%
10. Virus.Win32.Sality.at (v): worm/W32 0.84%

ThreatNet statistics revealed that trojans continue to make up a large portion of the most prevalent threats, taking four of the top 10 spots. The majority of these threats propagate through stealth installations or social engineering. (v) is a detection that has come directly from VIPRE. Source: Sunbelt Software

**Spam rate**

Compared to global email

- 80%
- 70%
- 60%
- 50%
- 40%
- 30%
- 20%
- 10%
- 0%

Spam rate indicates the accumulated emails tagged as unsolicited.

Source: Fortinet Threatscape Report

**Top 10 spyware threats**

<table>
<thead>
<tr>
<th>Threat name</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan.Win32.Generic: trojan</td>
<td>33.37%</td>
</tr>
<tr>
<td>Yontoo (v) Adware (General): adware (general)</td>
<td>1.77%</td>
</tr>
<tr>
<td>INF.Autorun (v): trojan</td>
<td>1.30%</td>
</tr>
<tr>
<td>Trojan.Win32.Adware: adware (general)</td>
<td>1.23%</td>
</tr>
<tr>
<td>Worm.Win32.Downad.Gen (v): worm/W32</td>
<td>1.02%</td>
</tr>
<tr>
<td>Trojan.Win32.Jmpframe (v): trojan</td>
<td>0.98%</td>
</tr>
<tr>
<td>Backdoor.Win32.Cybot.crg (v): backdoor</td>
<td>0.98%</td>
</tr>
<tr>
<td>Pinball Corporation. (v): adware (general)</td>
<td>0.88%</td>
</tr>
<tr>
<td>Trojan-Spy.Win32.Zbot.gen: trojan</td>
<td>0.84%</td>
</tr>
<tr>
<td>Virus.Win32.Sality.at (v): worm/W32</td>
<td>0.84%</td>
</tr>
</tbody>
</table>
**NEWS BRIEFS**

- An annual study on internet crime, conducted by Telus Corp. and the University of Toronto’s Rotman School of Management, indicated that publicly traded Canadian companies experienced 50 percent more cyberattacks in 2011 than in the previous year. On average, public companies were hacked 18 times, compared with a dozen times in 2010. Over the longer term, breaches at public companies have increased 600 percent since 2008. The study’s authors said that the most surprising finding was that 42 percent of hacker intrusions into government computers came from inside the organizations.

- Initiated in 2008, the study queried 600 Canadian IT professionals across government, public and private industries.

- The Supreme Court of Canada heard arguments seeking to overturn a lower court ruling on so-called fair dealing of copyright-protected works, looking to achieve a consistent application of the Copyright Act. The court’s rulings are expected sometime in early 2012.

- The Canadian Broadcast- ing Corp. (CBC) reported that the massive Chinese-based hacker attack on the Treasury Board of Canada and other federal government agencies late in 2010 was aimed at uncovering information about the takeover bid for Potash Corp. of Saskatchewan. The broadcaster cited evidence gathered by cybersecurity expert Daniel Tobok, who discovered that the spear phishing attack also targeted a number of large law firms who did business connected to BHP Billiton’s unsuccessful bid for Potash Corp. — a deal valued at $38 billion. One of the world’s largest consumers of potash-based fertilizer, China opposed the takeover bid, which would have put the Canadian company into the hands of BHP, an Australian conglomerate.

- Proposed federal government legislation could shutter many of Canada’s smaller internet service providers (ISPs). As written, the legislation would give law enforcement agencies sweeping powers to access internet subscriber information without a judicial warrant. ISPs would be required to maintain technology to provide real-time data surveillance. “If a smaller ISP has to make publically available exploits, which means they only need to worry about delivery mechanisms. While most public exploits have patches available, organizations aren’t patching as they should. Should I be worried? It is hard to find an organization that isn’t affected by patch management failures. This should be the highest priority because patches address the root cause of security holes.

**Debate**

The Stuxnet authors are behind the Duqu trojan.

We are certain Duqu was created using the same source code as Stuxnet. This is because roughly 50 percent of the code in Duqu is reused from Stuxnet. It would be nearly impossible to reverse engineer Stuxnet’s binary and achieve code so similar, not to mention impractical. Because the same source code was used, Stuxnet and Duqu share remarkable similarities: Duqu’s method for loading modules into memory has only ever before been observed in Stuxnet; both threats’ encryption algorithms are nearly identical; both store their two primary files, an executable and a configuration file with a unique .pnf extension, in the same subdirectory; and both are stored in a single file with all other components included therein. The organizational structure of the components within these files is identical. So, who has access to the Stuxnet source code? The truth is only Stuxnet’s authors do. All these facts taken into account leave no doubt Duqu was created by, at the very least, Stuxnet-affiliated attackers.

**THE SC MAGAZINE POLL**

Is Duqu, the so-called son of Stuxnet, something to care about?

- 27.59% No, its impact has been minimal.
- 72.41% Yes, any trojan that carries Stuxnet code is worrisome.

**THE STAT**

Oct. 28

Mumbai officials seize equipment from Web Works, suspected of hosting a Duqu C&C server

30 days: threat is configured to run by default before automatically removing itself from an infected system.

Source: Reuters/Symantec

**FOR**

**AGAINST**

Liam O Murchu / Security manager, Eurocontrol, Spain

Jules Polonetsky / President and CEO, U.S.-Canada Council for Cybersecurity

**THE QUOTE**

Designing to meet the nuanced needs of all web users is really hard.

— Jules Polonetsky, director and co-chair of the Future of Privacy Forum, commenting on a Carnegie Mellon report that found web users wishing to stop advertisers from tracking their online behaviors face major hurdles.

**THE MONTH AGAINST**

**FOR**

**2 minutes on...**

The 2012 election and cybercrime

**P14**

**P15**

**P15**

**P15**

**P15**

**Update**

**Face off**

The hacktivist group Anonymous made good on its promise of digital retaliation against the Oakland Police Department for the force it used against protesters following the clearance of an Occupy Oakland encampment. Members of the collective launched a denial-of-service attack that took down the department’s website, and also released employment details on a number of police officers.

*“Optpria” came in retaliation for Oakland police action against protesters.*

**Skills in demand**

Whose vendor risk is in high demand.

**Me and my job**

Assessing security postures to meet regulations.

**NEWS BRIEFS**

**THE SC MAGAZINE POLL**

Is Duqu, the so-called son of Stuxnet, something to care about?

- 27.59% No, its impact has been minimal.
- 72.41% Yes, any trojan that carries Stuxnet code is worrisome.

**THE STAT**

Oct. 28

Mumbai officials seize equipment from Web Works, suspected of hosting a Duqu C&C server

30 days: threat is configured to run by default before automatically removing itself from an infected system.

Source: Reuters/Symantec

**FOR**

**AGAINST**

Liam O Murchu / Security manager, Eurocontrol, Spain

Jules Polonetsky / President and CEO, U.S.-Canada Council for Cybersecurity

**THE QUOTE**

Designing to meet the nuanced needs of all web users is really hard.

— Jules Polonetsky, director and co-chair of the Future of Privacy Forum, commenting on a Carnegie Mellon report that found web users wishing to stop advertisers from tracking their online behaviors face major hurdles.

**THE MONTH AGAINST**

**FOR**

**2 minutes on...**

The 2012 election and cybercrime

**P14**

**P15**

**P15**

**P15**

**P15**

**Update**

**Face off**

The hacktivist group Anonymous made good on its promise of digital retaliation against the Oakland Police Department for the force it used against protesters following the clearance of an Occupy Oakland encampment. Members of the collective launched a denial-of-service attack that took down the department’s website, and also released employment details on a number of police officers.

*“Optpria” came in retaliation for Oakland police action against protesters.*

**Skills in demand**

Whose vendor risk is in high demand.

**Me and my job**

Assessing security postures to meet regulations.

**NEWS BRIEFS**

**THE SC MAGAZINE POLL**

Is Duqu, the so-called son of Stuxnet, something to care about?

- 27.59% No, its impact has been minimal.
- 72.41% Yes, any trojan that carries Stuxnet code is worrisome.

**THE STAT**

Oct. 28

Mumbai officials seize equipment from Web Works, suspected of hosting a Duqu C&C server

30 days: threat is configured to run by default before automatically removing itself from an infected system.

Source: Reuters/Symantec

**FOR**

**AGAINST**

Liam O Murchu / Security manager, Eurocontrol, Spain

Jules Polonetsky / President and CEO, U.S.-Canada Council for Cybersecurity

**THE QUOTE**

Designing to meet the nuanced needs of all web users is really hard.

— Jules Polonetsky, director and co-chair of the Future of Privacy Forum, commenting on a Carnegie Mellon report that found web users wishing to stop advertisers from tracking their online behaviors face major hurdles.

**THE MONTH AGAINST**

**FOR**

**2 minutes on...**

The 2012 election and cybercrime
The 2012 election & cybercrime

The cyber worries Obama’s campaign faced in 2008, however, likely were just an opening salvo. Not only have attack tactics gotten more sophisticated since 2008, but there also has been a meteoric rise of politically motivated hacktivism, particularly by the Anonymous collective, which has made no qualms about its interest in going after individuals or organizations with which it disagrees.

And with the Iowa caucuses, the first major electoral event related to the 2012 presidential nomination, set for early next month, the digital fight may soon get going, said Steve Livingston, a principal at Deloitte and lead of the company’s power and utilities security practice. “Campaign organizations don’t have CISOs,” he said, “but they’re calling them soft targets.” The incentive to show the American people what someone is really thinking, not just what their talking points are, I think there’s too much return on investment there for a hacktivist to ‘pass up.’ Already, in a video posted to YouTube in early November, Anonymous asked viewers to “occupy” the presidential candidates’ campaign offices in Des Moines, Iowa on Dec. 27, and then “peacefully shut down” the polls on Jan. 3. “The primaries and caucuses put on by these parties are part of an elaborate scam that deceives the public into voting for candidates that serve the private interests of the mega corporations,” said a computer-generated voice in the video. The two-minute clip does not explain how Anonymous plans to accomplish this action, whether it’s on the ground or in cyberspace – perhaps by way of a DDoS attack – but some have suggested the video is a hoax. Regardless, its mere existence underscores the possibility that the race to next November may be far unlike any other in presidential history.

– Dan Kaplan

$500m Amount of money President Obama raised online in his 21-month campaign in 2008 – The Washington Post

JOBS MARKET
Me and my job

David McGuire
senior security researcher; Veris Group; and vice chair of the operational security testing panel, National Board of Information Security Examiners (NBISE)

How do you describe your job to average people?
At Veris Group, I build and run security assessment programs to help customers assess their security posture and meet regulatory requirements in a way that is cost effective and repeatable. At NBISE, I extend that work into a community effort to define competency models for security testers with the goal of enhancing education.

Why did you get into IT security?
I got into IT security while in the Marine Corps because breaking into computer systems seemed cool. I ended up as a technical lead for a large Department of Defense Red Team and decided to stay in the field because being a part of the solution for securing our critical IT systems is a rewarding experience.

What was one of your biggest challenges?
Many of the organizations we work with are high-security environments with a large number of regulatory requirements, but constrained IT budgets. Our greatest challenge is designing assessments and training programs within these environments.

What keeps you up at night?
We are facing an increasing number of cyberattacks. Yet, our ability as an industry to assess systems against these threats is not keeping up.

– The Washington Post

What it takes
Candidates who can create and manage a comprehensive vendor risk program are in high demand. They must understand the risk of dealing with vendors; have a basic understanding of vendor risk management.

Compensation
The ability to drive policies, practices, tools and metrics is the key to success. Salary: $300,000 to $500,000 plus.

– Joyce Breen, CEO, AFA Associates, and founder, Executive Women’s Forum

Skills in demand
Companies are relying on vendors for the achievement of their business objectives through outsourcing of development, creating products and services, consulting and augmenting staff.

The Security Industry Association has named Don Erickson CEO. In his prior role, as director of government relations at SIA since 2006, he served as the lead advocate when appearing before Congress and other government agencies. www.siaonline.org

Kevin Engelhardt, VP of security operations at Diebold, maker of security systems, has been named interim VP of security solutions until a replacement can be found. He takes over for Bradley Stephenson, who retired from the post. Stephenson joined Diebold in 1973 and played a major role in the firm’s security business. www.diebold.com

Kevin Engelhardt, VP of security operations at Diebold

Follow us on Facebook and Twitter
Implement cultural change in 2012

Justin Somaini
CISO, Yahoo!

The end of the year is a really important time for me and my team. It’s one of those rare situations when I feel reflection is forced upon us. The business starts to slow down for end-of-year finances, IT shuts down for end-of-year finances, and core principles by which I operate, I believe, very deeply, that security is critically important to each and every one of us in our personal and professional lives. To that point, it’s important to do this reflection to make sure we are not off target.

I believe that transparency, openness and data are critical to obtaining people’s understanding and enrollment into security. We will never explain “why” to people and have them support our cause unless we are transparent, open and using data. Only 14 percent of respondents believed they had metrics that predict trends and allowed them to respond. In addition, none (0) respondents sent metrics to all employees. If we don’t show our metrics of security to employees, how can we ever expect them to support our implementation of controls? Also, the constant maturity of our metrics is important to ensure we are focusing on the right things. In industry, key performance indicators (KPI) are seldom used, if ever correct. Driving to this level of maturity is significant to ensure we have a robust data driven approach.

The method in which we implement controls is important to the defense of our environment. However, it’s our ability to implement culture change that is critical. Over 78 percent of respondents said culture change was most important compared to technical controls. Yet, the data shows that we don’t focus on it. Instead we focus on converting a subset of employees and executives, and leaving it at that. If we believe in culture change, we should change our behavior to meet it.
Social networking, hacktivism, advanced persistent threats, cyberespionage, mobile malware, the entry of portable, handheld devices (smartphones, tablets) into the enterprise environment...these are just a few of the most prominent challenges security professionals must contend with each day. This year-end special section focuses on people who represent the highest degree of professionalism in the security space, individuals who stand out for their technical skills, managerial prowess, insight and advocacy. As well, interspersed are some of the highlights in the year’s strongest trends, including top breaches and threats, merger and acquisition activity and legal developments, as well as some of the nuttiest news stories in the cybersecurity world.

TOP 5 INFLUENTIAL IT SECURITY THINKERS

SAMEER BHALOTRA

Age: 35
Occupation: White House deputy cybersecurity coordinator
Personal: Married, two children
College: B.S. chemistry and physics, Harvard University; Ph.D., physics, Stanford University
Recent accomplishments: executive branch development of cybersecurity legislation proposal, National Strategy for Trusted Identities in Cyberspace, and cybersecurity management reform

he three weeks from the end of April to the middle of May was a memorable time for Sameer Bhalotra, the White House’s deputy cybersecurity coordinator. Bhalotra, along with his boss, White House Cyber Coordinator Howard Schmid, oversaw the release of not one, but three major initiatives on cybersecurity. For Bhalotra, who signed on in July 2010, this was the outcome of long days facilitating lengthy meetings with two dozen executive agencies.

Along with Schmid, Bhalotra is the architect of the administration’s cybersecurity legislative proposal, released on May 12. But there was more. Four days later came the first International Strategy for Cyberspace. Previously, on April 26, his office released its National Strategy for Trusted Identities in Cyberspace (NSTIC), which seeks to establish clear privacy rules and greater security within a proposed identity ecosystem.

Accolades abounded for the 35-year-old Bhalotra, whose meteoric rise has taken him from a doctorate in physics at Stanford into the intelligence community, the Senate and his current post.

He achieved what no one in the Department of Homeland Security or the White House was able to do before by bringing the players together and getting them to work harmoniously. Alan Paller, research director for the SANS Institute, says of Bhalotra’s work on the legislative blueprint.

Bhalotra was sought for that mission. Soon after his appointment, Senate Majority Leader Harry Reid, D-Nev., asked the administration to weigh in on cybersecurity considering the 50-plus bills floating around the Hill. With this golden opportunity, Schmid’s office decided on a comprehensive approach. It was a minefield – within the executive branch, as well as between government and industry – but Bhalotra navigated it skillfully.

But, Bhalotra prefers to deflect attention from himself. “I’m proud to be yet another hard working member of the White House staff,” he says. “This was a team effort. Our leadership in the West Wing takes cybersecurity seriously.”

“He’s a little publicity shy, actually more than a little,” says Robert Rodriguez, a friend of Bhalotra’s and the founder of the Security Innovation Network. “He likes to work under the radar. But he’s the man behind all of it... Those were three huge accomplishments.”

On the legislative proposal, Bhalotra coordinated massive intergovernmental collaboration among such agencies as the FBI, National Security Agency and departments of Defense, Commerce, Justice and Homeland Security.

“Managing that process was a great experience,” Bhalotra says. The goal was to come up with recommendations to give Congress, of which securing America’s critical infrastructure and information sharing between DHS and industry stand out. Its release “was a great and clear end to a very rigorous process,” he says.
Bhalotra’s training for this process came during his nearly four years in the Senate. In 2007, he was brought onboard in a unique bipartisan role as a top staffer for the Senate Select Committee on Intelligence. He quickly seized on cybersecurity as a major issue and became an expert among Beltway staffers on the topic.

Bhalotra found few colleagues there dedicated exclusively to cybersecurity. So he began an informal group, where staffers on the Senate and House worked to discuss cybersecurity and bring new people into government. He quickly onboard in a unique bipartisan role on cybersecurity as a major issue in the Senate and House. He has mentored many young staffers on the Hill. With his distinguished resume, Bhalotra has cut the model. He hopes others in academia and industry will follow.

One of his personal interests is trying to bring new people into government,” he says. “We need to tap into the best minds in the country to solve these problems and move forward.”

== Eric Goldberg

**ERIC COWPERTHWAITE**

*Occupation: chief information security officer, Providence Health & Services*

**Age:** 44  
**Personal:** Married, four children  
**College:** B.S., computer engineering, California State University-Sacramento

Something of a perfect storm for privacy and security is converging in the health care industry. As part of last year’s Patient Protection and Affordable Care Act, companies are now required to digitize their medical records, but with this push come greater threats and challenges.

Eric Cowperthwaite, the chief information security officer of Providence Health & Services, which employs 54,000 people in Washington, Oregon, California, Alaska and Montana, is facing these challenges proactively. Providence, which operates 214 physician clinics, 27 hospitals, a health plan and many other services, has a model for securing health care organizations in protecting patients’ information from an increasing number of breaches.

This was borne out of necessity: in 2008, Providence was the first organization to enter into a resolution agreement with Health & Human Services (HHS) to resolve allegations of violating the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. Cowperthwaite, 44, has overseen the successful implementation of that agreement.

“They have the most mature program that I’m aware of in health care delivery,” says Gartner analyst Paul Proctor. “Eric has a program that rivals those in financial services.”

The federal government and business side of the industry, Cowperthwaite says, are “pushing us down the road of 100 percent electronic records. All patient information has to be accessible, open systems.”

“So we set up a one-stop shopping center for all the information you could want about a single person.”

However, confidential information—personal and financial in nature—is incredibly valuable for those who want to steal it. Breaches cost the health care industry $6 billion a year, according to the Ponemon Institute, and the majority of these intrusions currently come from insiders. At the same time, HIPAA and 2009’s Health Information Technology for Economic and Clinical Health Act, or HITECH Act, levy heavy fines for the loss or misplacement of information.

At Providence, protection of that data begins with recognition and emphasis. By design, Cowperthwaite reports to the chief risk officer instead of the chief investment officer. He believes he’s the only one among his peers at Catholic health organizations who does this.

“I think it’s a recognition that information security is a critical function of the business,” he says. “It’s not just an IT issue, but it touches the whole business. Providence did not have much of a security program to speak of before Eric, Gartner’s Proctor says. “They brought Eric in to build that program up.”

What began with just employees not well versed in information security has become a staff of 19 who report to Cowperthwaite directly, and another 33 people assigned in a matrix role. He is professional, but also has the energy to get briefings from officials, their work. These “cyber jams” allowed monthly to discuss cybersecurity and his gathered Senate and House staffers on the topic.

“Reboot 2011”

For Sesame Street was briefly hijacked by hackers who swapped out educational gene, one of the wealthiest businessmen in Russia. There’s little time to rest for Bhalotra says. “And I find cybersecurity so sophisticated, complicated, in an interesting way, and important to the country.”

Thereto little time to rest for Bhalotra, who is already meeting with Congress on the administration’s legislative proposal. In addition, he is also focused on bringing others into public service to meet cybersecurity’s fresh challenges. He has gathered Senate and House staffers in the House to discuss cybersecurity and the move forward.”

== Ryan Goldberg

**TOP 3**

**Weirdest news items**

Taste of one’s own medicine: A hacker in October who received a scam email had the last laugh when he took control of the phishing page and turned it into a public service announcement around phishing awareness.

Happy ending: Ivan Kaspersky, who was kidnapped for a ransom of $4.3 million, was rescued following a police operation. He is the son of IT security mogul and Kaspersky Lab founder Eugene, one of the wealthiest businessmen in Russia.

Mean streets: The YouTube channel for Sesame Street was briefly hijacked by hackers who swapped out educational videos with X-rated pornography. Not long after, Microsoft’s YouTube channel was also compromised, but not to display erotic video.

DigiNotar

In March, another CA revealed that hackers gained access to its system and fabricated nine certifi cates for some top-tier sites. Experts believe the Iranian government could be behind the Comodo, and more recent DigiNotar, attacks to spy on private communications.

RSA SecurID

In March, the security company revealed that sophisticated hackers launched a spear-phishing attack that exploited an Adobe Flash zero-day vulnerability to successfully infiltrate its systems and steal information related to its SecurID products. Such products include hardware token authenticators, software authenticators, authentication agents and appliances. Millions of customers worldwide use SecurID to protect access to sensitive assets, such as web servers, email clients and VPNs. Subsequently, hackers leveraged stolen information about SecurID in an attack on U.S. defense contractor Lockheed Martin. RSA President Art Coviello issued a warning for customers to be more vigilant and issued a list of recommended actions.


**TOP 10 breaches of 2011 (by records)**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Organization</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Sony Pictures</td>
<td>1 million</td>
</tr>
<tr>
<td>2.</td>
<td>WordPress.com</td>
<td>18 million (blogs)</td>
</tr>
<tr>
<td>3.</td>
<td>Tricare</td>
<td>4.9 million</td>
</tr>
<tr>
<td>4.</td>
<td>Health Net</td>
<td>1.9 million</td>
</tr>
<tr>
<td>5.</td>
<td>Nemours</td>
<td>1.6 million</td>
</tr>
<tr>
<td>6.</td>
<td>New York City Health and Hospital Corp.</td>
<td>1.7 million</td>
</tr>
<tr>
<td>7.</td>
<td>Sega</td>
<td>1.29 million</td>
</tr>
<tr>
<td>8.</td>
<td>Office 35</td>
<td>0.5 million</td>
</tr>
<tr>
<td>9.</td>
<td>Reboot 2011</td>
<td>0.1 million</td>
</tr>
<tr>
<td>10.</td>
<td>Eisenhower Medical Center</td>
<td>0.9 million</td>
</tr>
</tbody>
</table>

---

Suzanna Schmeelk is a woman on the frontlines of computer science, attempting to tear down the remnants of an old system that, she says, hasn’t been updated to meet the needs of today’s new computing environment. Her criticism is that students nowadays are not being taught to think independently. “Divergent thinking is being lost,” she says. “The ability to assert innovative, conceptual ideas is stilled in favor of procedural exercises.” As an example, she points to the evolution in attack vectors where an engineer has to think about what the next criminal entryway might be. The future of protecting online commerce depends on encouraging this type of open questioning, she says.

For Schmeelk, thinking conceptually began early. Her grandfather and father were both math professors. Her dad, she says, was a “liberal” math person who encouraged her efforts “within ethical boundaries.” Her mom provided vision. “She said everything is going to be computers some day,” Schmeelk recalls. “I knew that the explosive growth of computing was going to be an incredible thing.”

While Schmeelk believes computer science, as it is currently taught, is too narrowly focused, there are shining lights who manage to think outside the box. She points to Apple’s recently deceased co-founder Steve Jobs, and Joseph Nadan, a professor of management technology and business innovation at Polytechnic Institute of New York University (NYU-Poly), a research institution affiliated with NYU, where she is currently teaching. What she admires about them is their ability to see the big picture by combining engineering acumen with business needs. It’s a matter of being goal-oriented and being able to envision an end result: “It’s more about the value, not the process,” she says.

At NYU, Schmeelk is working as a cybersecurity consultant on a number of start-up projects, including collaborating with a number of hospitals and gaming companies. She serves as a resource as these incubating projects attempt to build websites, focused on applications-related challenges, such as...
TOP 8 legal actions

1. In what was termed the largest identity theft trial in U.S. history, 111 individuals were charged for their part in a New York-based organized crime operation responsible for more than $13 million in losses.
2. Six men believed to be behind a massive click-fraud scheme, all of whom are Estonian nationals, were arrested last month following a two-year, international police investigation, dubbed Operation Ghost Click. The racket led to the infection of more than four million computers in 100 countries with malware.
3. Running an online business that sold counterfeit credit cards embedded with stolen account information led to a 14-year prison sentence for Tony Perez III, 21, of Indiana.
4. The U.S. point person for one of the largest phishing rings ever to be brought to justice, John Cornish, 29, of Lang Beach, Calif., was sentenced nearly 13 years in prison for his part in stealing more than $1 million from victims.
5. Cameraman Tien Truong Nguyen, 34, of Long Beach, Calif., was sentenced to 11 years in prison for embedding stolen account information with malware.
6. Using stolen credit card numbers to conduct fraudulent transactions totaling more than $36 million resulted in a 10-year prison sentence for Rogelio Hackett Jr., 25, of Lithonia, Ga.
7. Former IT employee Jason Cornish, 37, of Smyrs, Ga., faces 10 years in prison for crippling his ex-employer’s network and causing hundreds of thousands of dollars in damages.
8. A nine-year sentence was handed down to former Dallas hospital guard Jesse William McGraw, 26, after he broke into hospital computers, planted malicious software, and planned a DDOS attack.

TOP 3 hacktivist attacks

The victim: Sony Pictures
The motive: The company has pursued legal action against alleged copyrighters.
The result: The now-disbanded LulzSec group exploited a SQL injection vulnerability to gain access to internal Sony networks and websites. The hack yielded the passwords, email addresses, home addresses, birth dates, and other account information belonging to more than one million users.

The victim: PBS
The motive: LulzSec sought revenge against the network for airing what they considered an unfair documentary about WikiLeaks.
The hack: The intruders compromised the website of PBS NewsHour to post a fake story that rapped Tupac Shakur was still alive. In addition, they published the usernames and passwords to staff at the public TV station, as well as those working at other networks affiliated with PBS.

John Streufert
Occupation: chief information security officer, U.S. Department of State
Age: 55
Personal: Wife, three children
College: Maxwell School of Public Affairs, Syracuse University, M.P.A.; St. Lawrence, B.A.
Recent accomplishments: Reduced measured risk on PCs and servers by a factor of 20; his tools guided critical patch coverage to the 84-percent level in seven days and 93 percent in 30 days at State; gives away software and speaks widely to promote continuous monitoring across the economy; served in 17 federal civilian roles across military, civilian and foreign affairs organizations.

John Streufert doesn’t like three-ring binders. Not because they remind him of a coldhearted teacher, but because of what their presence has come to symbolize in the government security world.

As chief information security officer of the U.S. Department of State since the summer of 2006, Streufert has seen more notebooks filled with compliance paperwork than he cares to remember. “A three-ring binder generally has little to do with information security,” Streufert says.

But, it’s not just a matter of transmitting data and details. While she’s reluctant to discuss gender issues, she does admit that being that she was often the only female in her computer science classes, she enjoys her new role encouraging women in the sciences. “There’s a choice a teacher makes,” she says, “to either encourage or discourage.”

Before her present activities, she interned at The Team for Research in Ubiquitous Secure Technology (TRUST). She has high praise for the consortium of academic and industry partners funded by the National Science Foundation to address issues affecting security, privacy and data protection.

“They’re not average people,” Schmeelk says. “Working there, you realize these are people who are making the impossible possible.” A similar consortium is now being formed within NYU, she says.

She is also a prolific writer of research papers, which often focus on how one can manage a project by developing a prioritization schema. Here too she envisions how a project can build to an end result. Schmeelk presented papers on prototype tools for testing open source coding at security conferences for Yahoo! and eBay.

“I like thinking about a lot of different problems,” she says. – Greg Masters

How best to protect health care data and online privacy?

“I am more geared to management and understanding the computer science aspect of online efforts,” she says.

This involves more studying of human nature. “A lot of this needs to be analyzed from a perspective of motivation. Why is this person doing this?” she asks, referencing hackers and cyberbullying.

“Suzanna is someone who makes a difference,” says Marjory Palis, associate director of The Robert B. Davis Institute for Learning at the Rutgers Graduate School of Education in New Jersey, where she teaches mathematical reasoning courses.

“I think she does it by bringing outstanding personal qualities to bear upon her work,” Palis says. “Suzanna is bright, worldly, compassionate and highly creative. She is an innovative thinker who eagerly explores novel situations and applies focus, imagination and perseverance to solve problems and develop new techniques.

Schmeelk was writing her doctoral dissertation at Rutgers as Palis and her colleagues were launching the Video Mosaic Collaborative (http://videomosaic.org), a portal to enable teachers and researchers to analyze and use classroom videos in math education. Schmeelk’s dissertation was the first to incorporate multimedia, inserting video stills in support of her findings of children’s mathematical learning as they built understanding of rational numbers as fourth graders, says Palis.

“The videos she analyzed for her research were among the earliest video clips for which we prepared metadata, with the help of Suzanna, in order to catalog and make them freely accessible to educators worldwide to support math learning, teaching and research,” Rutgers’ Palis says.

Schmeelk brings these qualities as fourth graders, says Palius. “Suzanna is someone who makes a difference,” Streufert says. “She is an innovative thinker who eagerly explores novel situations and applies focus, imagination and perseverance to solve problems and develop new techniques.”

A nine-year sentence was handed down to former Dallas hospital guard Jesse William McGraw, 26, after he broke into hospital computers, planted malicious software, and planned a DDOS attack.

“Working there, you realize these are people who are making the impossible possible.” A similar consortium is now being formed within NYU, she says.

“John Streufert doesn’t like three-ring binders. Not because they remind him of a coldhearted teacher, but because of what their presence has come to symbolize in the government security world.”

As chief information security officer of the U.S. Department of State since the summer of 2006, Streufert has seen more notebooks filled with compliance paperwork than he cares to remember. “A three-ring binder generally has little to do with information security,” Streufert says.

But, it’s not just a matter of transmitting data and details. While she’s reluctant to discuss gender issues, she does admit that being that she was often the only female in her computer science classes, she enjoys her new role encouraging women in the sciences. “There’s a choice a teacher makes,” she says, “to either encourage or discourage.”

Before her present activities, she interned at The Team for Research in Ubiquitous Secure Technology (TRUST). She has high praise for the consortium of academic and industry partners funded by the National Science Foundation to address issues affecting security, privacy and data protection.

“They’re not average people,” Schmeelk says. “Working there, you realize these are people who are making the impossible possible.” A similar consortium is now being formed within NYU, she says.

She is also a prolific writer of research papers, which often focus on how one can manage a project by developing a prioritization schema. Here too she envisions how a project can build to an end result. Schmeelk presented papers on prototype tools for testing open source coding at security conferences for Yahoo! and eBay.

“I like thinking about a lot of different problems,” she says. – Greg Masters
## TOP mergers and acquisitions activity

<table>
<thead>
<tr>
<th>Company</th>
<th>Purchased</th>
<th>Gains</th>
<th>Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check Point</strong></td>
<td>Dynasec</td>
<td>adds GRC software to help with regulatory requirements</td>
<td>undisclosed, but estimated at $20 million to $20 million</td>
</tr>
<tr>
<td><strong>Dell</strong></td>
<td>SecureWorks</td>
<td>adds managed security and consulting services</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>EMC</strong></td>
<td>NetWitness</td>
<td>adds network security analysis solutions</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>HP</strong></td>
<td>Autonomy</td>
<td>adds infrastructure software</td>
<td>$30 billion</td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>Q1 Labs</td>
<td>adds security software and services</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>Platform Computing</td>
<td>adds cluster and grid management software</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>Algorithmics</td>
<td>adds risk management</td>
<td>$387 million</td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>i2</td>
<td>helps clients harness data to combat fraud and security threats</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>IronKey</strong></td>
<td>IronKey's secure data storage hardware business</td>
<td>augments position in data storage and device management</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>McAfee</strong></td>
<td>NitroSecurity</td>
<td>will boost the SIEM capabilities in McAfee's Security Connected Framework</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>McAfee</strong></td>
<td>Sentirgo</td>
<td>adds database security and compliance products</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>Oracle</strong></td>
<td>RightNow</td>
<td>bolsters its cloud computing portfolio</td>
<td>$1.5 billion</td>
</tr>
<tr>
<td><strong>Oracle</strong></td>
<td>Endeca Technologies</td>
<td>adds software for unstructured data analytics and business intelligence</td>
<td>up to $1.075 billion</td>
</tr>
<tr>
<td><strong>Red Hat</strong></td>
<td>Cluster</td>
<td>adds open-source software for cloud storage</td>
<td>$136 million</td>
</tr>
<tr>
<td><strong>SAP</strong></td>
<td>Astara</td>
<td>delivers combination of endpoint protection with UTM</td>
<td>undisclosed</td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
<td>Clearwell Systems</td>
<td>adds e-discovery solutions</td>
<td>$390 million</td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
<td>Shavlik Technologies</td>
<td>adds traditional and cloud-based management products for SMBs</td>
<td>undisclosed</td>
</tr>
</tbody>
</table>

## TOP 5 threats

**Duqu:** An information-stealing trojan that shares much of its code with the notorious Stuxnet worm, and has impacted roughly five Europe-based manufacturers of industrial control systems.

**Zeus:** The insidious banking trojan, which continues to be used to siphon millions of dollars from U.S. bank accounts, became even more prolific this year when its source code was leaked on at least two underground forums.

**DroidDream:** The malware, which is capable of harvesting data, was discovered this year in more than 50 apps offered in Google's official Android Market, and illustrates that cybercriminals are focusing more of their efforts on mobile platforms.

**Operation Shady RAT:** A five-year-long advanced persistent threat and cyberespionage offensive that plundered intellectual property from some 72 organizations across 14 nations, including the U.S. government.

**Mac OS X scareware:** While still much-less prevalent than those seen in the Windows world, rogue anti-virus malware scams targeting the Mac platform grew increasingly nefarious this year, leading to a significant uptick in infections.

---

*Image 33x102 to 105x125*

*Image 34x140 to 105x159*

*Image 34x207 to 106x230*

*Image 34x258 to 106x274*
Reboot 2011

TOP 5 research revelations

BIOS fuel Researchers discovered the first-in-the-wild rootkit that targets BIOS, the built-in software responsible for booting up a computer. The discovery of Melbrom, the root kit, should not induce panic, though, as the complexity of a successful attack on the motherboard is high.

CA, MIA Mosix Malensis released Convergence, an add-on for Firefox, which essentially inverts the existing (and much maligned) certificate authority (CA) system, giving more power to users. They take their pick of so-called “trust notaries,” which authorize their web communications by default.

Pumped up Jay Radcliff demonstrated at Black Hat how he is able to send commands to and wirelessly disable the insulin pump he has been wearing since he was 22, when he was diagnosed with the autoimmune disease after dealing with extreme weight loss. He was right, Zatko remembers.
2012 is almost here. What security and privacy trends can Canadians expect during the coming year? Danny Bradbury checks in.

T he new year is here. Canada’s businesses and consumers alike have 12 months of security and privacy issues to navigate. What trends can they expect? We spoke to some experts to help map out key issues throughout the coming year.

**Consumerization will be a bigger driver**

Consumerization will be a big driver in 2012. The rise of smartphone and tablet devices allowing employees to plug in their own devices, and this is an overwhelming demand for people to plug in their own devices, and this is as true among Canada’s gadget-hungry population as elsewhere.

“As organizations move into allowing employees to plug in their own devices, it will open up a whole new area for risk mitigation,” says Nick Galletto, partner and national leader for information and technology risk solutions at Deloitte Canada. “How do you ensure that the right level of security controls are implemented on devices that don’t belong to the organization?”

Expect to see companies putting policies in place to manage the introduction of these devices. One potential solution could be a policy requiring users to hand over partial control of their devices to the company, so that encryption and VPN software can be added. Employees might agree to have their devices wiped and locked, should they be lost. Is Canada’s predominantly small-business-based community ready for that?

**Mobile threats will increase**

This rise in mobile usage will coincide with an increase in mobile threats, warns James Quin, lead research analyst at London, Ont.-based analyst firm Info-Tech Research Group. He says that we are seeing a perfect storm developing for mobile threats.

First, mobile phones are increasing in power. “No one was doing anything significant on them, so the payback was pretty small,” he says. Today, however, dual-core phones are enabling consumers and businesses alike to store and manipulate vast amounts of useful data, including contacts, financial and location information.

The second factor driving the threat is the increasing popularity of Android, he warns. “Previously, the market was really fractured, so any threat created would only affect a small subset of the population,” he says. “Now that business is using mobile devices, and Android has become the market share leader, we’ll see a lot more mobile threats.”

The open source nature of Android makes it particularly vulnerable. Fifty malicious Android apps were discovered on the Android Marketplace last year, all of them created using malicious code called DroidDream. If Quin is right, we can expect more of the same.

**Tracking will be a bigger problem**

Not all mobile threats are created by malware authors. Watch out for greater tensions over tracking technologies in 2012, says Anne Cavoukian, information and privacy commissioner of Ontario.

2011 saw several tracking incidents that worried privacy advocates and consumers, such as the revelation in April that Apple devices were logging users’ whereabouts. More recently, researchers from Duke University, Penn State University and Intel Labs found that an alarmingly high proportion of Android Apps send sensitive data back to corporate servers.

“You have this attraction to businesses to conduct this detailed tracking,” Cavoukian says. “The prevailing force against that will be consumer discontent.”

These conflicting drivers must be resolved, and Cavoukian predicts that the two can be reconciled by good design. “We always say that privacy isn’t anti-marketing, it’s pro-choice,” she argues, calling for anonymous data. “You can use it for market research purposes or with the consent of the data subject. Lots of people want information sent to them. They just don’t want the default to be identifiable tracking.”

**Whaling and spear phishing to grow**

Conventional phishing may be a smaller threat, says Cavoukian. “As organizations move into allowing employees to plug in their own devices, and this is an overwhelming demand for people to plug in their own devices, and this is as true among Canada’s gadget-hungry population as elsewhere.”

“Whaling is a very serious and difficult to counter type of fraud that is going on, and many people, especially high-wealth individuals, are getting whaling messages,” says David Jacobson, director of emerging technology consulting and deals at PwC Canada.

**Lawful access: Trigger point**

Lawful access — the legislation under which law enforcement can access information about internet users via ISPs without a warrant — was an issue in 2011. The Canada Consumer Product Safety Act (Bill C-22) was on the ballot, but was swept away by the May elections. It threatened to reappear in the Omnibus Crime Bill, but didn’t. Expect to see it all arise again in 2012, says Cavoukian.

“I wish they would call these lawful access bills something else, because there’s nothing lawful about them,” she says. “I am disturbed by these.”

Eleven fields of subscriber information are up for grabs, including IP, email addresses, mobile identification numbers, and others. “They will enable the ready identification through data linkage to the tracking of individuals,” says Cavoukian.

She expects lawful access legislation to be reintroduced in February. “Unless we raise our voices very loudly right now, this form of warrantless access may become a reality in 2012,” she warns.

**Hacker land grab**

Advanced persistent threats (APTs) are nothing new. Heavily orchestrated, sustained hacking attacks with a clear goal in mind have been happening for decades. So when SC Magazine’s panel of experts predicted their ongoing rise in 2012, perhaps what they were really envisioning was an escalation of APTs with a focus on intellectual property.

“APTs will continue to grow,” warns Tony Ritolip, partner and Canadian leader in Ernst & Young Canada’s IT risk and advisory service. “These are organizations trying to get intellectual property from governments and corporations.”

Deelstra’s Galletto warns that traditional anti-malware defences won’t be able to detect this kind of malicious code. “Those that used anti-virus and perimeter defences must now get more sophisticated and do more proactive monitoring in their environment,” he says.

This applies to the Canadian government just as much as Canadian companies. In February, it was revealed that Canada’s Treasury Board, Finance Department and Defence Research and Development Canada had been attacked using spear phishing techniques.

**Regulators will get teeth**

Regulators will play a greater role in security and privacy issues in Canada in 2012, predicts Galletto. “Self-regulation hasn’t worked, and there have been numerous breaches,” he warns. “The mandate for proper regulation will be there.”

The main instrument for privacy regulation in Canada is the Personal Information Protection and Electronic Documents Act (PIPEDA). Historically, this has been a relatively toothless piece of legislation, and the federal privacy commissioner hasn’t been given a great deal of room to act on violations.

This legislation, which is reviewed every five years, is up for discussion again in 2012, and the commissioner is already on the record with a promise to push for a greater enforcement agenda. “The second issue is that we live in a global marketplace with other jurisdictions,” says Galletto. “They will put pressure on Canada to comply with those global legislations, too.” A lot of privacy and security regulations in financial services in the U.S. will inevitably trickle down into Canadian institutions if they want to do business in the U.S., he says. 2012 promises to be a busy legislative year for Canadians, then, but the proliferation of new technologies will present new issues for those living north of the border. Let’s hope that Canada is ready for the challenge.
Financial institutions’ leaders must come together to deal with data security risks and compliance requirements, says Illena Armstrong.

CEOs, government regulators and IT security pros sometimes may have disparate views on information protection, and government regulators often confound the most ideal data security outcomes and the methods used to achieve these. Especially among CEOs, concerns about compliance and regulation rule, said Leigh Williams, who spoke at the event as CEO of BITS, a division of an umbrella organization called the Financial Services Roundtable, which is made up of about 100 various financial organizations, including banks, insurance providers, investor firms and others. (Williams has since left BITS to serve as director at the Office of Critical Infrastructure Protection and Compliance Policy at the U.S. Department of Treasury. Paul Smocer, former technology risk manager at Bank of New York Mellon and CISO at Mellon Financial, who first joined BITS in 2008, is now the organization’s president.)

Because the financial crisis led to everything from the creation of the Consumer Financial Protection Bureau (CFPB) to myriad regulations, CEOs want assurance from IT and executives that data security and data reporting standards put forth in these rules are upheld, Williams explained during the SC Magazine Roundtable, sponsored by HP Enterprise Security.

“Foremost in their minds, for better or worse, is this avalanche of regulation,” he said. “You can argue about whether that’s a good thing or a bad thing, but it absolutely crowds out some of their thinking about opportunities and customer service, and I know they’re frustrated about that.”

Many SC Roundtable attendees agreed, noting that while their CEOs don’t necessarily get into the detail of how they’re keeping compliant with regulations, they do have firm expectations.

“From a compliance and risk management perspective, they’re very, very tuned in, and I think it’s generating a lot of the push down in terms of action amongst our teams...” said one attendee who asked to remain anonymous.

Multifactor authentication is of particular interest, agreed many SC Roundtable participants, especially given the updates earlier this year to the Federal Financial Institutions Examination Council (FFIEC) guidelines, which pushed for use of such technologies in 2005 to combat such attacks as phishing. Revisions specifically address corporate bank account takeovers, which have become more common, as have corporate system must be able to assign different actions together, the overall corporate system must be able to assign these varying identity attributes to a particular customer, he said.

Indeed, the monitoring and protection of confidential data, ultimately resulting in preventing its exfiltration, is yet another employee-related concern for SC Roundtable participants.

“Since the financial crisis, I’m hearing a lot of stories about how people leave companies and take the data with them,” said the Roundtable participant, reviewing legal options to address the loss of data through mobile devices. When considering customer security, issues become even more convoluted—especially again considering widespread use of mobile apps, said Ryan Kalember, director, solutions marketing at HP Enterprise Security. Citing the example of technologists earlier this year using Bluetooth-enabled devices to hack into a car’s computerized system to stop it from mid-drive, he said to the SC Magazine group: “If they can change fuel ratios that prompts the bank to ask customers to approve transactions; or the bank’s procurement of a list of approved payees from customers.

Another SC Roundtable participant—working for a large bank and who asked for anonymity—said mobile security was proving exceptionally tricky given the variety of devices traded and other executives use. Because of Federal Communication Commission (FCC) regulations, which mandate that exchanges via these devices be monitored, the time and costs currently dedicated to this task is high. And, currently, he has found little help from security vendors.

To support organizations in addressing the countless ways data could be compromised and to tie together the sometimes contrasting viewpoints on ways to get there, Williams said BITS has created some 17 working groups to address data security and the many other requirements put forth in legislative mandates, such as the Dodd-Frank Wall Street Reform and Consumer Protection Act.

He further noted that whatever the differences of opinion concerning data security among CEOs, security professionals and legislators, information protection is center stage. It’s imperative, then, that budgets and associated risk management plans must stay focused on this objective.

“There are enormous amounts of data being reported to every agency now, to every examiner, to every banking agency,” he said. “It’s important that we safeguard them. This creation of the CFPB is a reminder that we’re not just talking about the safety of our organizations and institutions, but we’re talking about the safety of and service to customers, too. That’s an important piece to senior execs. They’d like to ensure that customers are being well served.”

A more extensive version of this article is available at www.scmagazineus.com
Q&A

We asked a few of our most trusted sources to peer into the crystal ball and formulate some predictions for what we all can expect in 2012.

OUR PANEL OF PROGNOSTICATORS
Craig Spiezle, executive director & president of Online Trust Alliance (OTA)
Randy Sanovic, owner of RNS Consulting; former general director, information security of General Motors
Rich Mogull, founder of Securosis
Gerhard Eschelbeck, CTO & SVP at Sophos
Daniel Kennedy, research director, TheInfoPro, a division of The 451 Group

What threat vectors will be most prominent? Why?
Spiezle: I expect to see continued targeting of the trusted supply chain, such as certificate authorities, content providers and the ad supply chain and others. For example, Epsilon is just the tip of the iceberg. Email marketers are being attacked at increasing velocity. If they can compromise these trusted providers, it is game over downstream. I also expect a continued focus on the compromising of ad servers to serve malicious ads, which are unknowingly served by high trafficked websites (aka “malversting”).
Sanovic: My first worry would be malicious hackers and bots. The environments that concern me most are mobile computing and social technology. For example, to somewhat secure Facebook could require at least 103 clicks, and most people, including the more technical-oriented, will not get it done. Because of the pervasiveness of mobile computing, and the fact that technologi- 
cal advances continue to outpace reason-
able and prudent security fixes, I feel we will not be able to get “user friendly/ capable” security solutions implemented in a timely fashion.
Mogull: What’s prominent in terms of attacks? The same stuff as today: email and web phishing/social engineering. In the press releases? Whatever the vendors want to sell that you probably don’t need: a lot of mobile device and cloud hype. I expect a lot of iOS headlines this year, and a lot of Mac hype. Not that Macs are immune, but the hype will far outweigh the number of people being compromised. And, while cloud security is important, most of what you’ll see is “cloudwashing” of traditional security stuff. People will really have to keep hunting for the innovation (which is there, just not from your usual vendors).
Eschelbeck: The web is today’s platform of choice for communication and interaction, and will undoubtedly continue to be the most prominent vector of attack. Cybercriminals tend to focus where the weak spots are, and use a tech-
nique until it becomes far less effective, as we saw with spam mail (which, while still present, is less popular with cyber- criminals, as people have deployed highly effective gateways). The web remains the dominant source of distribution for malware – in particular malware using social engineering or targeting the browser and associated applications with exploits. Social media platforms and similar web applications have become hugely popular with the bad guys, a trend that is only set to continue over 2012.
Kennedy: Enterprises are concerned about trends associated with IT consum-
erization – personnel bringing in their own devices – and how to handle that in all of its manifestations (smartphones, laptops, etc.) while still protecting custo-
dial and intellectual property data.

What security solutions/services will see increased adoption? Why?
Spiezle: Email authentication and hard blocking will gain, as will walled garden/blocking of unprotected PCs.
Sanovic: I think cloud security services will be more in demand, and that will help determine the extent of security technologies applied. The main issue will be cost, and how onerous the computing overhead of such technologies will be.
Mogull: Mostly things we’ve been spending on for the last five years, which still don’t work like they should. I’d like to say we’ll see increased spending on tools better suited to today’s targeted attacks, but I suspect only the leading edge of the market will actually drop cash on those.
Eschelbeck: The rapid inflow of consumer-owned smartphones and devices is causing significant security challenges for many organizations. IT departments are being asked to connect devices to corporate networks and to secure data on these devices, over which they have very little control. Due to the high degree of mobility, security requirements are plentiful, including enforcement of use policies, corporate data encryption, secure access to corporate networks, productivity/content filtering, and, of course, malware protection. Mobile security and management solutions will likely see significant adoption in 2012. The global nature of these mobile security challenges makes them prime candi-
dates for solutions delivered as services in the cloud.
Kennedy: Both flavors of data leakage prevention (DLP), endpoint and net-
twork, top the in-plan implementations we see in our user-based research for 2012. Application-aware, or next-genera-
tion, firewalls are a close third.

Cloud security services will be more in demand.”
—Randy Sanovic, owner of RNS Consulting

The web...will continue to be the most prominent vector of attack.”
—Gerhard Eschelbeck, CTO & SVP at Sophos

Which will see declining adoption rates? Why?
Sanovic: I think we will see an increasing adoption rate based primarily on the above noted factors.
Mogull: Nothing. We’re too scared to drop even worthless products.
Eschelbeck: In 2012, we will continue to see the evolution from traditional Windows-based endpoints to a new genera-
tion of form factors, including very lightweight endpoints and tablets. While some development will be incremental, part of this will also come at the cost of traditional desktops, notebooks and laptops. Security technology will follow the same paths, and traditional endpoint security mechanisms will reach their physical limits on these new platforms. The unique nature of these modern form...
factors requires rethinking of security and defense mechanisms, whereby cloud-based delivery models will play an important role.

Q: Which security lesson will organizations be forced to learn this year? Why?

Spiezle: I see more focus on looking at security and privacy by design in a concerted effort, with a mindset of completing a security impact statement for every business process. Further, data minimization efforts will increase, and data incidents will be required to be reported by the U.S. Securities and Exchange Commission and the Sarbanes–Oxley Act, increasing C-level accountability.

Sanovic: Organizations will be forced to concern themselves with true data protection mechanisms/technologies.

Eschelbeck: Security really is about accountability.

Rapid fire: What’s ahead in 2012?

<table>
<thead>
<tr>
<th>Question</th>
<th>Increase</th>
<th>Stagnant</th>
<th>No</th>
<th>Yes</th>
<th>N/A</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will security budgets increase, stay stagnant or decrease?</td>
<td>Craig Spiezle</td>
<td>Yes</td>
<td>Yes, misinformation and leaks.</td>
<td>n/a</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Will any significant security-related legislation become law?</td>
<td>Randy Sanovic</td>
<td>None that I’m sure of.</td>
<td>Yes, I think they may.</td>
<td>SCADA systems are still subject to severe damage.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Will cyberthreats play a role in the presidential election?</td>
<td>Rich Mogull</td>
<td>Yes, but it won’t help.</td>
<td>Yes, the election. I have money on that one.</td>
<td>The election. I have money on that one.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>What “emerging threat” will finally break out and become a real risk?</td>
<td>Gerhard Eschelbeck</td>
<td>Yes</td>
<td>Yes, marginal. A subject that will be given lip service.</td>
<td>Mobile device spyware/malware will continue to grow.</td>
<td>Yes, the ball moves forward a little every year.</td>
<td></td>
</tr>
<tr>
<td>Will we be more any more secure by Dec. 31, 2012?</td>
<td>Daniel Kennedy</td>
<td>Increase, but at a lesser percentage.</td>
<td>No, though some lesser legislation might go through.</td>
<td>Mobile device spyware/malware will continue to grow.</td>
<td>Mobile device spyware/malware will continue to grow.</td>
<td>Mobile device spyware/malware will continue to grow.</td>
</tr>
</tbody>
</table>

What will be the most surprising security-related development?

Sanovic: The focus on mobile security will force and drive security solutions in the mobile and social media arenas.

Mogull: If I told you it wouldn’t be a surprise. It would also be wrong, so I try not to predict the unpredictable.

Eschelbeck: We are currently seeing daily news of security incidents and exposure of corporate data, whereby the even more troublesome security issues could be in critical infrastructure systems. This could easily create alarming surprises in the coming year. We saw attacks on the critical network infrastructure, as well as control systems, but there are many other types of systems, including aviation networks, which could come under focus of cybercriminals. We also continue to integrate and connect technology more and more into our lives—for example, smart grid infrastructure—and such systems could yield attacks that have a new “personal” impact on us.

You’ll never know who’s plotting the next cyber attack on your business. But with F5, you’re protected.

Unlike traditional or so-called “next generation” firewalls, F5’s award-winning security solutions identify the nature and source of digital traffic and quickly adapt to threats.

Learn more at f5.com/smartersecurity.
CASE STUDY

For a company that supplies vending machines and arcade games across the southeast United States and South America, it’s far from amusing when a “tilt” alert goes up on its network operations. When the Brady Distributing Co. began operations in 1944, delivering Wurlitzer jukeboxes involved some paperwork, a few trucks and strong backs. Now after 70 years, it has added pool tables, vending machines and pinball and video games to the mix – all operated out of a 84,000 square-foot facility in Charlotte, N.C., with branch offices in Memphis, Tenn., and Miami and Orlando, Fla. Brady works with more than 70 manufacturers, making it the second largest distribution company in the amusement games and vending machine industry. There are about 120 employees throughout the organization.

But, a new game came to town that threatened the day-to-day operations of the enterprise and its branches: malware and distributed denial of service (DDoS) attacks. And despite an IT staff consisting of only one person, infrastructure support must reach all of its far-flung offices, as well as its customers – who span from Texas to Oklahoma to the East Coast and into the Caribbean and South America, says Rick Baird, the company’s IT department manager.

“Our remote offices are not very large, so we use a multiprotocol label switching (MPLS) network and Citrix gateway to route our satellite branches into our main network where we host our business software and applications,” he says. Baird had installed a firewall on the company’s MPLS network and a content-filtering appliance to block undesirable websites, but these just didn’t provide enough security, he says. In particular, content filtering by domain name was inadequate. As soon as he would block a site containing malicious content, another one would pop up. Brady has anti-virus software, but its desktops – especially the ones in the remote offices – were still getting infected.

“We rely on technology to connect our offices and service to those customers around the world,” he says. “As well, malware and viruses could result in a customer information breach, and reduces our employee productivity by creating a lot of extra work for our IT staff, which has better things to do than deal with infected PCs.”

Baird also was concerned that a DDoS attack could disrupt the business, especially as it expands its online presence. Brady had experienced SYN flood attacks (wherein an attacker attempts to overload a system by repeatedly sending SYN requests), but its network firewall can’t stop everything, Baird says. Taken together, Baird decided another defensive layer was needed to block malware on the network and mitigate against DDoS attacks.

He and a team of executives considered a number of intrusion prevention systems (IPS). The choice was a solution from Corero Network Security, based in Hudson, Mass.

“Corero was the only solution we found that provides true, three-dimensional protection – from malware defense to firewalls to anti-DDoS,” says Baird. He says he was thrilled with the deployment. Within an hour, Corero had the solution set up, and then customized the configuration to meet Brady’s environment and specific needs. Within days the system was tweaked and running by itself.

“They walked us through the entire process, and continue to support us from soup to nuts,” Baird says. “That has made all the difference.”

The IPS includes hardware and software components that are shipped to the customer’s data center, where the IT department deploys it as an inline network device, says Mike Paquette, chief strategy officer at Corero (formerly Top Layer Security). “A few quick configuration steps later, their clients and servers are protected against remote exploits, malware and other network-borne cyber-attacks that might occur.”

What differentiates the Corero solution from the competition, says Paquette, is that its IPS provides network- and application-layer DDoS defense, policy-based stateful firewall filtering, and two-stage protection and immunity to advanced evasion techniques, in a reliable, integrated, “green” platform.

Baird says that at Brady, he continues to apply the updates and advisories that Corero distributes, but beyond that no other changes have been needed. “Since we installed the solution, securing the network has gotten so much easier, and I can focus on work that helps the business rather than firefighting things, like malware infections,” he says.

Corero provides Brady with the protection it needs, and regular updates keep the game distributor ahead of the curve, says Baird. “Our network is more secure than ever.

Further, the solution assists with compliance requirements. The company’s online transactions and personal information handling fall under the Payment Card Industry Data Security Standards requirements, as well as multiple state data breach notification laws. “Corero provides a reporting and audit trail to help us document the protection we have,” Baird says.

Brady expects to expand its use of the product as the company grows its operations. To achieve that, it soon will be hosting a new website to handle more orders. Currently, five percent of its business comes from online orders, but that will grow to 15 to 20 percent once the new site is in place, Baird says. “This will be worth millions of dollars to us, and if something like a DDoS attack were to disrupt our business, we could lose a lot of revenue.”

And as the company relies more heavily on the internet, and threats grow more frequent and represent an increasingly greater threat to the business, “good enough security isn’t good enough anymore,” Baird says.

Corero’s IPS provides significant out-of-the-box attack protection, says Paquette. In addition, customers subscribe to the company’s Secure-Watch threat update service to receive Protection Packs that include new and updated rules and signatures to protect against new vulnerabilities, or detect and block the latest exploits. The packs also include internet topology and IP address-based filtering information.

Because IPS sits inline, Baird says he was concerned about latency and its impact on employees and the business, particularly since all of Brady’s offices are connected through the main corporate network. “It’s absolutely critical that we have the internet connections and all security systems up and running as fast as possible so that everyone can work as smoothly as possible,” he says. “With Corero, we have experienced no slowdowns or delays on the network.”

Keeping the network operations going at an amusement game company takes more than a roll of quarters, reports Greg Masters.

GAME PLAY

36 SC • December 2011 • www.scmagazineus.com
Imagine yourself as a burglar choosing a target to enter. You have a variety of structures before you: some tremendously large buildings with vast stores of valuables within them, others smaller outposts with slightly fewer rewards for your efforts. Most of the places with the biggest treasures are going to be better guarded than those in the smaller buildings, so common sense might tell you that the smaller places are a better place to start. Fewer security measures to break through or to outsmart potentially means more bang for your burglary buck.

The obvious advice to any owner of the smaller premises would be to increase their security, so taking that metaphor and applying it to network security means considering what can be done to maintain a perimeter that is secure enough to put off the more casual thief or criminal. This is where unified threat management systems (UTMs) come in – they seek to increase the firepower of the protection used in those smaller outposts, making them less vulnerable.

Small to medium businesses in particular have a unique set of circumstances, as they may have fewer monetary and personnel resources than an enterprise business. These business owners can feel a false sense of security, as they consider themselves to be lower-profile and less valuable a target than larger businesses. But this is not how cyber-criminals view the situation. The stakes of loss of reputation and, therefore, business for SMBs can be significantly higher, given their smaller customer base and profit margins, compared to enterprise businesses.

UTMs were designed to deal with precisely these concerns. Security is not something that can be postponed because it seems to be a poor return on investment. Odds are, if you’re reading this magazine, you don’t need to be “sold” on the importance of having a complete security solution to protect a business of any size. You know the magnitude and the complexity of the threat which faces businesses of all sizes and home users alike.

Having a central security and protection device can be an ideal tool for businesses which have a small or non-existent staff dedicated to security. In the early days of these types of solutions, this took the shape of simple anti-virus offerings. Having your security infrastructure reside on a separate device operating at a gateway allows security to be managed centrally so that all updates and settings changes could be done in a single location rather than having to apply them to each endpoint. The evolution of these solutions has led us to the point where UTMs, which can offer a balance of speed, ease of use, transparency and manageability, for a variety of sizes of businesses, are prevalent.

Modern UTMs now comprise a wide toolkit of different security features beyond just anti-virus. At its most basic, a UTM should feature, alongside the anti-malware components, a firewall and virtual private network (VPN) capabilities which means they offer a good range of functionality for smaller businesses.

More full-featured devices can contain various additional modules, such as intrusion detection and prevention systems (IDS/IPS), and spam and URL content filtering. By grouping these tools in a device at the gateway, they can help improve network performance by taking out hostile or unwanted traffic before they reach the internal network. Certainly, having these things centrally located makes it easier to apply updates to network settings and policy changes across an organization.

Because there are so many complex features at play here, all interacting with each other, independent testing plays a vital role in finding the device best suited to a company’s individual needs. A UTM must not just protect a business and its users, it must also not act as a hindrance to doing day-to-day business. Legitimate email must get through. Innocent websites need to be accessible. Clean, non-malicious files should not be blocked. By putting these devices in simulated real-world environments, including malicious and unwanted, as well as innocent activity, their effectiveness can be accurately assessed across the whole spectrum of functionality.

As we have seen with the anti-malware space, the purchasing process has become more of a pure business decision than in the past. Yes, security is the main function and needs to be evaluated. However, it should also be tested in the environment to determine the overall effectiveness specific to total cost of ownership and return on investment.
OVERVIEW

The Unified Security Gateway (USG) range of appliances was developed by the joint venture company, Huawei Symantec. All of the appliances tested in this report are part of the USG series which are tailored to meet the needs of various company sizes – the USG2200 series for SMBs and the USG5500 series for enterprises.

In order to test the full range of security technologies contained within the appliance, Huawei Symantec enrolled both devices into the Checkmark UTM Certification program by West Coast Labs (WCL). This certification has been designed to test the core components of any UTM device with a focus on the following key functions: firewall, VPN, and anti-virus as the baseline and anti-spam, IPS, URL filtering, and anti-spyware as optional components. To demonstrate confidence in their products’ security capabilities, Huawei Symantec opted to test the baseline and all optional components.

TEST NETWORKS AND METHODOLOGY

Initial configuration of each appliance is performed by using the product’s Quick Access Wizard which guides the administrator through configuration of standard networking tasks, such as internal, external, and DMZ IP addressing, virtual private tunnelling, and the operations and management agent.

Once the setup is complete, the final stage is the application of the various module licenses. Huawei Symantec offers greater flexibility by employing licenses for each of its core technologies so companies that are content with their existing anti-spy or URL filtering solutions can continue using them.

The first technology tested in the Checkmark scheme was the anti-virus capabilities of Huawei Symantec’s USG series, which were tested over the SMTP protocol. Before testing could begin, the appliances were configured to forward all SMTP traffic to an internal postfix server. Following this, an anti-virus policy was added to不准 the use of signature-based protection. If a virus were detected, it would be blocked immediately.

Intrusion prevention (IPS) in the appliances is addressed by use of a signature-based system and policy deployment. At the time of testing, there were more than 8,000 detectable attack types in the signature database, which is constantly being updated. During each of the these three network security tests - namely firewall, IDS/IPS, and VPN - the USG appliance was able to correctly identify and block the incoming traffic, while allowing authentic, genuine traffic to continue as would be expected. Given these network security technologies are the raison d'être of UTM appliances, protection in these areas without hampering workflow is key, and the USG appliances deliver on both fronts.

RESULTS REPORTING

In testing the firewall, IPS and VPN features, West Coast Labs (WCL) used various commercial, open-source and custom tools to validate the overall integrity and performance of each feature. Huawei Symantec’s USG series yielded impressive results at high thresholds within the WCL Checkmark Certification.

There is a dashboard that provides an immediate, high-level overview of the solution. Information within this page is displayed through the use of visual data such as charts, “speed dials”, and short tables, providing an accurate and instantaneous appraisal of the system status without the need to study text-heavy logs. For a more in-depth analysis of the system, a separate log mechanism called eLog be setup on a standalone PC. The eLog logging system contains more detailed information on incoming traffic, such as source IP address and port, the respective security zone (e.g., trusted or untrusted), and the security policy responsible for the log entry.

WEST COAST LABS VERDICT

The Huawei Symantec USG2250 and USG5560 are comprehensive, well-rounded security solutions. Each of the package’s security technologies is well designed, with the anti-virus, IPS and anti-spam technologies benefiting from the combined expertise of the joint venture of Huawei Symantec. Firewall, URL filtering, VPN and anti-spyware features have also been well implemented and there is strong commitment to deliver a quick and easy-to-learn user interface. Huawei Symantec has delivered feature-rich and user-friendly UTMs. West Coast Labs recommends Huawei Symantec USG2250 and USG5560 for excellence in both performance and functionality.
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
- Computer Information Systems with an emphasis in Information Security
- Systems and Network Administration (SNAP)
- Information Technology

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.
I t’s time for our “Innovators” issue again. Every year at this time, we roll up our sleeves and start digging for those companies that have the vision, imagination and creative management to become the leaders in our industry through their innovation. The first time we did this – four years ago – leading-edge changes were in short supply. Since then, we have seen mergers and acquisitions, severe economic woes and business failures. Happily, all of that seems to be behind us, but the industry does not look anything like it did four years ago.

Last year, we had several companies pass out of our Hall of Fame. This year, we have one, but it is a real success story. The Hall of Fame is reserved for the most innovative of the innovative. That means that we have vetted the winners several years in a row. We perform that due diligence in a variety of ways. We look at how many times they have been chosen as Innovators. We look at how they fared in our monthly Group Test – leading-edge changes were in short supply. The first time we did this – four years ago – the picture has changed – and radically from four years ago – we believe this is the true spirit of our industry, another innovative – but much larger – company, bought them. It remains to be seen what will happen next, but knowing both of these firms, I’m betting each will continue their winning streaks, together now.

Innovation is not something that comes from sales or marketing alone. It is comprised of the technology, plus the way the business is conceived. We found some interesting trends this year. For example, we found that the majority of our Innovators are stealthy marketers. They prefer to use public relations and word of mouth instead of spending bundles on advertising. That doesn’t mean they don’t advertise. It means they advertise smart. For example, some told us they use online banners and trade shows instead of paying big bucks for display ads. Another major factor in our business has been the emergence of old wine in new bottles. Those of you who follow my writing know I am not a fan of the hype that surrounds “the cloud” and “Web 2.0.” Both of these are, pure and simple, figments of some marketer’s pipe dream. That said, they are with us even though nobody seems to recall that back in the day we were sharing computing resources from time-share services through crude dial-up modems. Web 2.0 is nothing more than the same old stuff married up with active content. The product equivalent of this is a “new release” that really is nothing more than a different color box. So, given this reality, how have these “new” market areas affected us? Depending on your perspective, I think we’d have to admit that they have changed everything, at least for now. They have introduced an entirely new computing paradigm when taken in context with today’s enterprises. A contradiction to my comments above? Not really. Back in the day, we did not have the distributed computing platforms that we do presently. And, most important, we did not have the kinds of virtualization that we do currently. If there is a single true generational innovation, it is virtualization. Clouds and web notwithstanding, without virtualization, these things would never have been economically feasible. So, we may have old wine in new bottles, but that virtualization bottle is a game changer. The combination of the wine and the bottle is a serious challenge for security and forensic investigation. The real Innovative companies are those that have come up with viable technology, have the business foresight to monetize it and the marketing savvy to get the technology to customers. This month, we have, as we used to say in Indiana way back when, a whole passel of ‘em. Though the picture has changed – and radically from four years ago – we believe you’ll find that this issue is a harbinger of what to expect. Things in the computing world have started moving again and they will never be the same as years past. So, hang on… it’s going to be quite a ride!

Cutting edge is alive and well again, says Peter Stephenson, technology editor.

I 2011 Innovators

PRODUCTS | Industry Innovators

PRODUCTS | Industry Innovators

ACCES CONTROL

Access control is a key to securing the enterprise.

G iven out and get a top-

practitioner identity and

access management

(IAM) product and make it

available to the SMB market.

Good idea, right? Except

for one thing: SMB companies

cannot afford enterprise-class IAM

products, no matter how much

they need what those products do.

Along comes this Innovative

who lights the way to a solution.

Lighthouse took the core

IAM technology from partner

IBM, added its own shell to

make it accessible and configu-

rable to users in SMBs that do

not have quite the resources

that big enterprises do, and

provided a vastly better, easier-

to-deploy product – called Lighthouse Gateway.

Cost $2,995 per month

GREATEST STRENGTH: The vision to see what the market

needs and figuring out a creative way to

support.

Lighthouse Gateway

IVATION: Making IBM “big

Iron” capabilities in IAM avail-

able to smaller organizations

at an affordable price and within

their means to support.

PRODUCTS

www.scmagazineus.com • December 2011 • SC 45

PRODUCTS

www.scmagazineus.com • December 2011 • www.scmagazineus.com
Insightix

Insightix is an Israeli company that has experience – especially in consulting – in what they refer to as the "jungle problem." By that they mean a jungle is a jumble, and nobody really knows everything on the network. The implication is that there is a need for complete, real-time, contextual network intelligence in order to secure the network.

Insightix is seven years old with 120 employees. The company is well-balanced between marketing and technology, but is focused on technology to support the customer and integrate with vertical applications. To make that work, it seeks technology partners and provides a platform for partners’ products.

The Insightix tool – called Insightix Business Security – is designed to detect, identify, profile, audit and control all devices connected to the network in real time. That's a pretty big order. But, that is what BSA is designed to do. And this provides first-rate support for compliance.

From the business perspective, Insightix understands where it brings value to the marketplace. That value could be an end-user or technology partner. Because it provides the total intelligence in real time to the appropriate delivery target, it addresses the business need directly. Because this is an agentless approach, it is more efficient and lightweight at the endpoint. From a features delivery perspective, the product does discovery of all network assets, audit, compliance, risk analysis, user identity profiling, remediation, control and enforcement. That makes BSA a full, closed-loop access control tool.

Assurance (BSA) product suite – is designed to help customers.

EyeLock

Biometrics tools – real biometrics of the kind that one can use reliably in a high-security environment – are relatively rare. Add the need for rapid and reliable identification and one has a requirement for a very rare bird indeed. EyeLock enters the picture here with its approach and we would present them with “The Better Mousetrap Award” – if such a prize existed.

EyeLock was founded five years ago in response to several industry trends carefully, and watches relationships within specific geographic regions, develops partnerships with OEMs [original equipment manufacturers] that are pre-loading WinMagic products. It’s a good strategy and one we’ve heard before, but in the hands of WinMagic, it does seem to work quite well.

Encryption

Encryption, arguably, is the mainstay of information protection. We would be hard-pressed to find many product categories in the security space that did not have some encryption component associated with them. Whether it is raw encryption – file and folder or whole disk, for example – or some form of public key infrastructure (PKI), encryption makes the information-protection world go round.

Also, it is pretty hard to find anything new under the encryption sun. But, we’ve done that this year. Again, as with many of our Innovators, it is not so much what they’ve done that impresses us, but how they’ve done it. Addressing a problem that we all know about, but don’t think about – the complexity of encryption from the perspective of the end-user – poses a problem that may be greater than those posed by the mechanics of encryption. This year’s Innovator focused on solving a problem with a technology that people actually can use. The company got there first and it never looked back. Many of us can remember when Phil Zimmerman introduced the early versions of Pretty Good Privacy (PGP). Great stuff, to be sure, but like many products of the time, PGP required a proficiency with the command line, and it came at a cost that was not the average user’s bailiwick. I recall many years ago, telling a client that he needed to employ encryption for sensitive emails. What did I suggest? PGP, of course. My client just laughed and asked me who I thought would be able to use the product? He got me there. Once you leave the IT shop, users who could make it work were few and far between.

However, times have changed. Today, encryption is commonplace, and this year’s Innovator played a significant role in achieving that status. Happily, it is still innovative and bringing encryption ever more into the mainstream for users who need to employ their computers, not tinkering with them to make them work.

And, while encryption is about mathematics and technology, our Innovator believes that it also should be usable by the broadest possible audience.

EyeLock

EyeLock is an Israeli company that focuses on IrisLock – formerly the Hoyos Group – did, and the partners’ products.

But, it was not just any full disk encryption product. The company was, in fact, the first full disk encryption (FDE) provider to introduce true key management by using a key labeling design. Not satisfied with that, WinMagic introduced the client design using cryptographic token interface standard [PKCS#11] from the ground up. The following year, it became the first FDE provider to introduce encryption for floppy, ZIP drivers and USBs. And since those years, this Innovator never has looked back.

Over the years, it has introduced secret-level encryption for the U.S. government by means of hardware encryption via the Fortezza card, provided FDE for the U.S. National Security Agency, and received the first-ever NIST certification for advanced encryption standard (AES), among many other accomplishments.

WinMagic’s PBlConnex is based on the premise that typical encryption technology is too complex and disruptive. It should, in fact, behave as if it were not encrypted. That calls for an emphasis on ease of use, as well as effective protection. Encryption done wrong can cause too many disruptions, and that is a weakness that needs to be overcome.

WinMagic’s PBConnext is an Israeli company that has experience – especially in consulting – in what they refer to as the “jungle problem.” By that they mean a jungle is a jumble, and nobody really knows everything on the network. The implication is that there is a need for complete, real-time, contextual network intelligence in order to secure the network.

Insightix is seven years old with 120 employees. The company is well-balanced between marketing and technology, but is focused on technology to support the customer and integrate with vertical applications. To make that work, it seeks technology partners and provides a platform for partners’ products.

The Insightix tool – called Insightix Business Security – is designed to detect, identify, profile, audit and control all devices connected to the network in real time. That’s a pretty big order. But, that is what BSA is designed to do. And this provides first-rate support for compliance.

From the business perspective, Insightix understands where it brings value to the marketplace. That value could be an end-user or technology partner. Because it provides the total intelligence in real time to the appropriate delivery target, it addresses the business need directly. Because this is an agentless approach, it is more efficient and lightweight at the endpoint. From a features delivery perspective, the product does discovery of all network assets, audit, compliance, risk analysis, user identity profiling, remediation, control and enforcement. That makes BSA a full, closed-loop access control tool.

Assurance (BSA) product suite – is designed to help customers.

EyeLock

Biometrics tools – real biometrics of the kind that one can use reliably in a high-security environment – are relatively rare. Add the need for rapid and reliable identification and one has a requirement for a very rare bird indeed. EyeLock enters the picture here with its approach and we would present them with “The Better Mousetrap Award” – if such a prize existed.

EyeLock was founded five years ago in response to several industry trends carefully, and watches relationships within specific geographic regions, develops partnerships with OEMs [original equipment manufacturers] that are pre-loading WinMagic products. It’s a good strategy and one we’ve heard before, but in the hands of WinMagic, it does seem to work quite well.

Encryption

Encryption, arguably, is the mainstay of information protection. We would be hard-pressed to find many product categories in the security space that did not have some encryption component associated with them. Whether it is raw encryption – file and folder or whole disk, for example – or some form of public key infrastructure (PKI), encryption makes the information-protection world go round.

Also, it is pretty hard to find anything new under the encryption sun. But, we’ve done that this year. Again, as with many of our Innovators, it is not so much what they’ve done that impresses us, but how they’ve done it. Addressing a problem that we all know about, but don’t think about – the complexity of encryption from the perspective of the end-user – poses a problem that may be greater than those posed by the mechanics of encryption. This year’s Innovator focused on solving a problem with a technology that people actually can use. The company got there first and it never looked back. Many of us can remember when Phil Zimmerman introduced the early versions of Pretty Good Privacy (PGP). Great stuff, to be sure, but like many products of the time, PGP required a proficiency with the command line, and it came at a cost that was not the average user’s bailiwick. I recall many years ago, telling a client that he needed to employ encryption for sensitive emails. What did I suggest? PGP, of course. My client just laughed and asked me who I thought would be able to use the product? He got me there. Once you leave the IT shop, users who could make it work were few and far between.

However, times have changed. Today, encryption is commonplace, and this year’s Innovator played a significant role in achieving that status. Happily, it is still innovative and bringing encryption ever more into the mainstream for users who need to employ their computers, not tinkering with them to make them work.

And, while encryption is about mathematics and technology, our Innovator believes that it also should be usable by the broadest possible audience.

EyeLock

EyeLock is an Israeli company that focuses on IrisLock – formerly the Hoyos Group – did, and the partners’ products.

But, it was not just any full disk encryption product. The company was, in fact, the first full disk encryption (FDE) provider to introduce true key management by using a key labeling design. Not satisfied with that, WinMagic introduced the client design using cryptographic token interface standard [PKCS#11] from the ground up. The following year, it became the first FDE provider to introduce encryption for floppy, ZIP drivers and USBs. And since those years, this Innovator never has looked back.

Over the years, it has introduced secret-level encryption for the U.S. government by means of hardware encryption via the Fortezza card, provided FDE for the U.S. National Security Agency, and received the first-ever NIST certification for advanced encryption standard (AES), among many other accomplishments.

WinMagic’s PBlConnex is based on the premise that typical encryption technology is too complex and disruptive. It should, in fact, behave as if it were not encrypted. That calls for an emphasis on ease of use, as well as effective protection. Encryption done wrong can cause too many disruptions, and that is a weakness that needs to be overcome.

Further, response to customer needs, including customization, brings value to the customer. That is something we almost never hear. The idea of customi-
Digital forensics is a difficult field to analyze...

NIKSUN

These guys, in the vernacular of some in the tight hand coast, are wizened smart. To be sure, there is a lot of technology in what they do, but what makes them Innovators is not so much what they do, but how they do it. Their flagship product, NetOmní Alpine, is delivered on a hardware platform (up to 2U form-factor) that is deployed in a customer’s network or security operations center, or a similar central location. All distributed NIKSUN appliances deployed in the customer network need to be accessible from the NetOmní system so data can be exchanged. With this approach, the user achieves a pervasive network forensic captures that can be analyzed in real time or after the fact. That is a very important point, by the way. Some forensic tools may claim to be network forensic tools when they mean that they are network aware and can capture platform data over the network. True network forensic tools, however, must be able to capture and analyze network traffic, reconstruct network sessions and provide tracing capabilities for attribution purposes.

All that is interesting, and it certainly has made NIKSUN an innovator, but what comes next? To be an innovator, a company must continue creating better products. When we asked the visionary to whom we were talking, what’s next, he told us that the next challenge is to have a global view of data presented in a user-friendly manner. That means one to two clicks to the data. Also high on the list is improving the efficiency of workflow, looking at how users attack problems, and seeking to make it smoother and more intuitive. It takes curious and knowledgeable people to get these difficult tasks accomplished, so NIKSUN relies on a motivated staff. It doesn’t spend a lot of money advertising, rather it focuses on doing the products right.

Its next step is to make workflow more efficient through automation. The company needs to handle lots of data and lever-age lower-level people in the everything’s operation. This is a more efficient way to do network forensics than forcing all of the analysis to be performed manually by experts. Next step is to leverage the data to be predictive and then feed back into the cycle. Sounds pretty ambitious, but I’m betting this team will pull it off.

AccessData

Here’s another one of the forensic good guys. But, they are substantially different from some of their competitors. For starters, they are one of the oldest companies in the game with a pedigree going back more than 20 years. Last year, we recognized AccessData as a mainstay in the forensic business and, to be sure, they are. But when one has been around a long time, it gets harder and harder to come up with new things. Nowhere is that more obvious than in the digital forensic marketplace.

True, there are some fine companies that are doing very interesting things. Some are quite small. Others are larger, but have focused on continuous improvement in what they have – a notable approach. But true innovation is a tough beast to find, and the folks at AccessData seem to have found it. More and more, they are creeping up on a more comprehensive approach to digital forensic analysis.

One of the powerful things about the AccessData strategy is its view of digital forensic data. It is always about the case at hand. Data collected using other AccessData tools usually slots right into the case so that the analyst can consider the whole picture. We have found that view to be most useful when using the AccessData suite of products.

So, where do you go when you need to develop innovation in what looks like a mature market? First, you acknowledge that it is anything but mature, no matter how other vendors treat it. Then you set about to prove the thesis. One starts by identifying weaknesses in the current crop of products. One major weakness is how relationships between digital forensic data may be visualized. These can be seriously important because they point out subtleties that help solve the case. Malware analysis always has been delegated to third-party tools, and some very good ones at that. But what if one could add that analysis into computer forensic good guys. But, as the “Swiss Army Knife” philosophy. This is the “every-tool-in-one-box” approach. Everything forensic is in a single program. There are some disadvantages to all tools needed to conduct a digital forensic analysis. On the other hand, there is a lot of technology in what they do, but how they do it. Their flagship product, so much what they do, but how they do it. Their flagship product, NetOmní Alpine, is delivered on a hardware platform (up to 2U form-factor) that is deployed in the enterprise at the infrastructure level to pull the protection outside of the network. Capable systems are doing exactly that. Slowly, security services are moving to the internet in shared environments. These shared environments are special-purpose environments to use the current vernacular.

The second issue is compliance. If the infrastructure protection is not policy driven, it will fail in its purpose. The infrastructure is exactly that. It is not just the server farm. It is the servers, the endpoints, the communications devices and, today, it could, for example, be the organization’s telephne system running on VoIP. Coordinating protection of all of that is a formidable challenge, and our entry this year meets the challenge in spades. In prior years, we focused on policy and configuration management tools and other similar solutions for the infrastructure...
MOBILE DEVICE PROTECTION

There is anything that characterizes today’s computing environment beyond virtualization and the techniques that have fostered – it is the pervasiveness of mobile devices. These units, from smartphones to tablets, have introduced to the enterprise a whole batch of new intrusion – and extraction – vectors.

The challenges include new and very different operating environments, as well as the pervasive nature of mobile applications. Many of these are not vetted for malware, backdoors and just plain bad programming. There are limited protection tools for many of these environments and, probably worse, sometimes there is no way to know who is on the network. Moving between Wi-Fi and the wireless telecom network provides opportunities to exfiltrate data from one network onto another without authorization.

Demand for mobile devices within the organization is reaching epic proportions, often precluding proper policy development, testing and configuration of gateways. With all of that in mind, solutions to these challenges become a major challenge in itself. Managing everything from policy to enforcement poses huge challenges by itself. These are the types of challenges that require creative solutions, and they require those solutions quickly. It takes both experience and innovation to step up to the enterprise and become an emerging new and very disruptive technology.

Returning for the moment to the subject of disruptive technology, this year our surveys have uncovered the interesting premise that addressing a disruptive technology, such as the explosion of mobile device use in all quarters, requires an equally disruptive technological solution, along with the creative business and go-to-market approaches to monetize it.

This year’s Innovator is all of those things: experience, creativity, vision and a solid business approach. Taking the framework for security in the mobile environment, adding the dimension of compliance and considering the technological issues all play important roles in successfully addressing smartphones and tablets.
M86

A couple of months ago, we recommended the M86 product to some friends in the banking industry. We had the opportunity to give the product a thorough shake-down, and the results were impressive. First, malware defines the M86 product. And the malware engine defines its innovation. M86 focuses on distinct capabilities that are holistic, rather than any one single capability. Regardless of what the organization is, M86 has deployed its anti-malware tools from small enterprises up to the very large. Read the market, respond and move the product fast. Listen closely to customers and anticipate what that means. And then make M86 tick. And it does in its products and support.

M86 has a very long history. The founders created the current company by merging several world-class companies together. Each was an innovator in its field. Together, they looked for a problem to solve in the market. Over a very short time, they developed a vision of applications that will be a problem in the future. Then they attacked the management of those applications. M86 capabilities are available through the company’s appliance, software or software-as-a-service (SaaS) for web and email security. M86 works with organizations that have a vested interest in keeping its customers safe, so it provides the technology to ensure that safety. These partners become M86’s salesforce, taking its products to their customers, keeping the customer safe and not spreading malware around the web.

M86 products use patented, real-time code analysis and behavior-based malware detection technologies, as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information and ensure regulatory compliance. A tall order, but certainly within the realm of M86’s capability. The strong merging of premises products and cloud services gives M86 customers access to a lot of power.

Trustwave

We’ve said it before, but here we go again. Trustwave is without a doubt the freshest example of a well thought-out cybersecurity product going. It is intuitive, has well-constructed menus and capabilities, and does exactly the job for which it is intended. Trustwave was the result of a merger in 2005. The predecessor company was founded in the 1990s by ex-NSA employees and was mostly a consulting practice focusing on P3I compliance. The current company still does consulting and assessment, plus it has a portfolio of more than 20 products, which it either built itself or has acquired. Trustwave has built a comprehensive security portfolio by actively integrating everything in its kit into a holistic security management system.

The Trustwave strategy is to build and acquire leading products from multiple sources and integrate the mix into what the customer needs, whether on-premises or as a managed security service. The company actively applies both consulting expertise and research. That provides a platform of knowledge and experience. The team also has a unique ability to combine compliance management with compliance enablement by providing all the necessary services and components to allow one stop shopping. From the beginning, it has established relationships with large banks and consortia to provide products and services in bulk. Using its partners to leverage sales, Trustwave has over time established a base of more than one million clients by selling to the customers’ customers and leveraging those relationships.

Recognizing that customers grapple with complexity and compliance, Trustwave set out to simplify this through a comprehensive suite of security products and services. When we asked the visionary what makes the company tick, he answered: “Trustwave is committed to identifying and protecting sensitive data in every form in every environment. Our vision is for a global community in which transactions are safe, and information flows freely and securely.”

That global vision has gone a long way toward putting Trustwave in this year’s Innovator designation.

Cyberoam

Cyberoam is a brand of Elitecore Technologies, an Indian company that started 12 years ago with 10 employees. With all the uproar about offshoring, this company is a real success story. The visionary we spoke with was the founder of the company and spent a lot of time talking about working with American employees and learning the cultural difference so that his Indian employees could make a global success out of Cyberoam. And a global success it is.

In 2004, the Cyberoam product was born and is now globally strong with 5,000 sales partners and 70 distributors worldwide. It always has been profitable, selling mostly to SMBs. With about 700 employees, half are dedicated to Cyberoam and most of the company’s revenue comes from Cyberoam. The visionary told us that transparency (strategy always is clear) and collaborative culture around the world (business) are hallmarks of its corporate personality. It is cautious on marketing spending. It makes sure that its products are established in all other markets before the United States to ensure the credibility of the product in what it considers the most important market in the world. The key, we were told, is brand recognition. Cyberoam is one of two largely foreign Innovators this year, the other one being based in Israel.

The Cyberoam product line is quite broad, consisting of 19 models. These can be fully customized to meet the security requirements of enterprises across verticals. And, the company recently launched a network security product targeting the home segment, called NetGenie-Home.

“So, what really makes Cyberoam stand out?” we asked the visionary. “What one single thing defines the Cyberoam value statement?” The answer was clear, and it explained why this precious start-up, which began with only 10 employees now has a global operation with more than 700. “Value for money,” he told us. “Add strong research and development, strong company commitment to innovation, many features – all while the cost stays reasonable and then maintain hardware compatibility without requiring new hardware.”

Yep. That should do it.
VIRTUALIZATION

We began 2011 with the most significant change to computing since the introduction of client-server computing: virtualization. Virtualization has been with us in one form or another for a long time, but now that it is a staple of the systems world, it really has come into its own. Virtualization not only has changed the way we build our data centers, it has gone beyond that to change the way we do computing. All sorts of companies are competing for specialized niches, coining new buzzwords and addressing new problems – mostly economically related – by providing the computing power in a centralized data center reached securely (one hopes) over the internet. Some of the offerings are solutions looking for a problem, but a significant number – an ever-increasing number – are legitimate business opportunities. It is important to recognize that there are at least three important trends driving the explosion of cloud offerings – cost, green initiatives and compliance. Serious computing power costs money. Pulling together several customers who are willing to share a community resource is one way to address that. The catch is that these several customers don’t want the others sniffing out their business. So, the concept of sharing this way could not progress without adequate security. That has opened serious opportunities for innovative companies.

Our two companies – one is in the Hall of Fame section – this year are visionaries. They have seen the future and, in true paranoid fashion, have sought out and addressed challenges. These companies model their solution to virtual problems after similar paranoia in the non-virtual world. Their premise is: If it works in the physical data center, it should work in the virtual one. That, of course, requires significantly different technology, a business model that is sustainable, and a go-to-market plan that can foster confidence in potential customers. The virtual world is a scary place when one starts thinking about security in the context of the cloud – public or private – and compliance.

**Virtualization has...changed the way we do computing.”**

---

**VULNERABILITY TESTING**

Vulnerability testing has changed markedly over the past few years. Hall of Famers in this space have contributed mightily to these changes, which largely dealt with redefining what we mean by vulnerability assessment (VA) tools. That term – vulnerability management (VM) – is a Holy Grail for this product space. There are good vulnerability management tools available. Some even do both automated VA and pen testing. However, as a genre, these tools have a way to go to be fully baked.

What we have now, in addition to some capable vulnerability management tools, are some very capable VA and pen testing tools. What we don’t yet have is everything in a single tool. This year’s Innovator is approaching that Nirvana from the VA/pen testing perspective. VA is not rocket science to perform automatically. VA scans, after all, are pretty automated from the beginning. The scan starts and then reports back its findings in the form of a report – and that’s it. Done. Pen testing can be automated, and there are times when automated pen testing actually doesn’t work as well as automating VA does because there always is the necessary human intervention. But what if one wanted to combine VA and pen testing, automate the process, and make the human less necessary? That would approach the pot of gold and, if one could add the right workflow for remediation and retesting, the goal would be attained. That’s where this market needs to go, and this year’s Innovator has played a key role, along with other Hall of Famers, to get us to this promised land.

---

**Catbird**

It’s good to be in the Catbird seat, and this Innovator certainly is. This 10-year-old company has an interesting history. Its original business was doing security monitoring from the cloud, even though there wasn’t a cloud yet. It solved a problem for banks by remotely checking the data center, so it put sensors inside so it could do both internal and external monitoring. Then it customers wanted them to check inside the data center, so it put sensors inside so it could do both internal and external monitoring.

There is a virtual appliance (sen- sor) that sits on the hypervisor and reports back to a cloud-based monitoring center so that either the customer or Catbird can monitor: Sensors are free, but Catbird charges the control center that does monitoring and analytics, and then quarantines virtual machines, based on user definitions. The product suite includes a firewall, access control, intrusion prevention (IPS), vulnerability assessment and what the company believes is the most important, compliance based on the user’s selection of regulations. Why does this company position itself as an innovator? Its technology provides in-depth compliance monitoring in a virtual environment. This leads to helping its customers as trusted advisors in the virtual security space. Catbird sells through a value-added reseller (VAR) channel and its market strategy is to put virtual security monitoring on the map by educating the market and being seen as thought leaders. Since people who purchase Catbird are already comfortable with security experts – the VARs – Catbird adds the tools for those experts. There is no doubt that Catbird has taken a decade of experience and morphed it into a viable virtual security suite of capabilities. Does the company still do the external monitoring? Certainly, although that is not its mainstream business anymore. But, just think of its mix of monitoring. We did, and we made them our Innovator in virtualization security this year.

**AT A GLANCE**

**VENDOR:** Catbird
**www.catbird.com**
**FLAGSHIP PRODUCT:** vSecurity
**COST:** $1,995 per socket

**INNOVATION:** In-depth compliance monitoring while providing useful functionality for virtual security, especially in cloud environments.

**GREATEST STRENGTH:** Experience from the data center to the virtual center.

---

**Saint**

Saint is back this year for its second bite at the Innovator apple. This is only proper since Saint has a very long history – one of the longest, in fact, of all the vulnerability assessment tools. Over that history – which began formally in 1998, although Dan Farmer and Wietse Venema actually released the open source version of its predecessor, Security Adminis- trator Tool for Analyzing Networks (SATAN), in 1995 – Saint has won numerous awards, innovated in many ways, and, in general, helped change the way we test our enterprises for vulnerabilities. The Saint website gives a good view of what drives the company. “Since its inception in 1998, Saint Corp. has been developing software products to make network security easy and affordable.” Ease of use and affordability have been the company’s hallmarks since its inception. However, that has not been an easy road. First, Saint started out running in a “thin environ- ment, rather than on a Windows box. Many novice penetration testers had some difficulty with that, but Saint persisted. Linux is the primary tool for system hacking. All of the best scripts run on it, and developing new tools is easier than in Win- dows. The code also tends to be more compact. Today, Saint has added the Mac to its arsenal and that, too, should be no surprise. With its “two roots, the current Mac operating system is so good for system testing that Macs are now being used primarily for pen tester in general. One of Saint’s major innovations was the integration of penetration testing and vulnerability assessment. Since the network assessment process usually begins with automated or semi-automated vulnerability scans, and progresses to attempting to exploit weaknesses found by those scans, a product that does both – and integrates both results and reporting – is a powerful tool indeed.

Overall, the company’s objectives are to develop technology that is more useful for the customer. Saint’s vision is to be a leader. That’s what drives them. Striving to figure out what the next need is going to be and then producing it. The company is small and agile enough to run with something new very quickly, achieving a speedy turnaround on new products and ideas.
HALL OF FAME

The 800-pound gorilla in the room, Hall of Famers go through a rigorous evaluation, not once, but over a space of years. They have to be creative, well-managed, forward-looking and successful. Don’t forget that last one, either. Success is the yardstick by which we measure the worth of these creative companies.

We pick our Innovators each year based, in part, on our experience with them during the intervening year between December issues. After two to three years, depending on the company and how it fares in our Group Test reviews and First Looks, its road map for the future, and its performance against its earlier road maps (including turn-on-a-dime responses to unavoidable changes, such as market conditions or the economy), we push the best of the best into the Hall of Fame.

Getting to the Hall of Fame requires innovation, staying power and demonstrated success. Last year, we inducted several companies into our inaugural Hall of Fame. This year, there is only one, but it is an interesting story because it is the amalgam of two companies, both of which have, over time, demonstrated the characteristics that we look for in Hall of Fame candidates.

There is a notion that getting votes in the Reader Trust Awards, part of the annual SC Awards, equals Hall of Fame status. Because of the way the Reader Trust Awards are granted, however, they only count for part of the total picture. Reader Trust Awards, for example, may equate in part to market share, which, in turn, may equate to company size and age.

There are a couple of Innovators this year that might very well win a Reader Trust Award. That would be a very good thing given that the designation bestowed by us would tend to validate the kudos presented the winner by our readers. And that sums up the whole idea nicely. It is the well-rounded company with appropriate products in the right place at the right time that wins Hall of Fame honors.

Today’s technology companies ought not to win by brute force, but, rather, by a combination of attributes that define excellence in their respective fields.

Organizations are learning that meeting regulatory requirements usually isn’t enough.”

Juniper

This is the third year that we have looked at Altor, the company that burst on the scene with the first product to firewall individual virtual machines in a VMware environment. At the time, we asked the company’s visionary what the company was going to do when VMware decided to build its own similar product. “That’s our business,” he replied. Altor’s approach is still hot, and it’s not Altor anymore.

This year, Altor became part of the Juniper family. We cannot think of a better marriage. Both companies as the cream of the crop. Deserve to join other Hall of Fame candidates.

The vGW Virtual Gateway is Juniper’s positioning for securing virtualized data centers and clouds. The centerpiece is a hypervisor-based stateful firewall that secures inter-VM traffic at wire speeds. Layers of defense include application monitoring, integrated intrusion detection, VM compliance assessment, image enforcement and now integrated, high-performance anti-virus. This functionality makes the vGW much more than a virtual firewall. It really is a true gateway that joins the physical and virtual environments for generalized security. And that is worthy of a spot in our Hall of Fame.

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

As we increase our social connectivity, we also increase our exposure to an ever-changing array of exploits by criminals seeking to steal personal information via active online communities. By banding together to protect and defend ourselves we can stop enemies in their tracks. At RSA® Conference 2012, you will tap into the power of the collective as you learn from the best and brightest in the industry, exchange effective and valuable strategies with your peers and become stronger in the face of persistent security threats.

RSA Conference 2012 is the premier event where you will find the insights and resources you need to thwart socially engineered attacks and keep your kingdom safe from threats.

BUILD YOUR STRENGTH

Connect with cutting-edge solutions.

CONQUER YOUR CHALLENGES

Get insights on today’s hottest topics.

REFINE YOUR STRATEGIES

Participate in over 220+ expert-led sessions.

SHARE YOUR KNOWLEDGE

Create networks with industry experts and peers.

To register before Friday, January 27, visit Register Now!
We are our own worst enemy

To avoid past mistakes, one should appeal to outside experts, says Kyrus CTO Michael Tanji.

It is tough being in cybersecurity. Defense is a cost center, and it’s hard to find meaningful metrics to demonstrate success. Interest in security is also cyclical: Major breaches stir action, but as time passes, interest and resources wane, though the threat is still there. Yet the biggest problem with cybersecurity is ourselves. Before we can succeed, all of us must agree to change.

We can start by getting a handle on our language and defining our terms. Just about every adjective applied to malicious activity or code is subjective. There are no widely accepted definitions for what is “advanced,” “sophisticated” or “complex.” Why does security get short shrift? Because it is hard to take people seriously when their words can mean anything and they’re so hyperbolic.

Related to our language problem is the desperate need to end the use of war analogies. The stupidity of phrases like “digital Pearl Harbor” doesn’t require further elaboration. “Cyber deterrence” only makes sense if there were any meaningful analog between the lasting impact of using nuclear weapons versus digital ones. “Digital arms control” is such a non-serious idea as to be laughable. Legacy futures make for great newspaper copy and think-tank literature, but proposing solutions for a world that doesn’t exist isn’t helping the world that actually does.

We desperately need to do more critical thinking. So much cybersecurity analysis is pseudo-scientific, sometimes to the point of being on par with astrology. There is nothing more intellectually lazy than pointing to an IP address as “proof” of a source of evil. It’s not that others aren’t stealing our ideas and property, but no country has a death-grip on every byte that enters or exits systems within its borders. Any country that is advanced wouldn’t need to steal secrets. Yet in every report about cyberespionage there is a line akin to “all signs point to this being the work of country X” – without any critical analysis. There are 20 (G-20) “major economies” in the world, 31 “high income” Organisation for Economic Co-operation and Development (OECD) member nations, and 35 “advanced economies” per the International Monetary Fund – all of which could benefit greatly from the intellectual output of American engineers and scientists. But since we’re so heavily invested in preparing for a conventional war with just two adversaries, that’s who we blame.

When presented with the opportunity to discuss cybersecurity problems, we should actively campaign against the use of false authorities. Our world is filled with security celebrities whose Q scores are disproportionate to the breadth of their actual expertise. When we launch people into space, we seek comments of former astronauts, not glider pilots. Yet no one thinks twice about asking an expert in cryptography what they think about botnets.

One suggestion: When asked about an issue outside of one’s area of expertise, offer access to a true expert instead. We need less commentary from the most glib, and more insight from the most knowledgeable.

Finally, and I can’t stress this enough, we need to appreciate and promote our history. I have computer security books that were printed in the 1970s. If you didn’t know The Cuckoo’s Egg (which details a computer hack) took place 25 years ago, you’d think it was documenting events that happened last month. In fact, everything Cliff Stoll did ad hoc – computer network defenses, honeypots, public-private information sharing – are things we’re still struggling to get right today. The echoes of history should inform, not haunt us, if we’re to succeed.

Michael Tanji is a former intelligence officer and the CISO at Kyrus.

Virtualize more with WebSphere.
Or pay more with WebLogic.

Over 400 highly logical reasons to choose IBM WebSphere® over Oracle WebLogic®:
1. Save 57% on first-year licensing and support.
2. Choose from more virtualization options (including VMware and Xen).
3. Pay only for cores you use (not always true with Oracle WebLogic).
4–404. Be in good company (last year, over 400 Oracle WebLogic clients chose IBM WebSphere).

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

<table>
<thead>
<tr>
<th>Vendor</th>
<th>25%</th>
<th>50%</th>
<th>75%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET NOD32</td>
<td>93</td>
<td></td>
<td></td>
<td>97</td>
</tr>
<tr>
<td>Symantec</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td>79</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sophos</td>
<td></td>
<td></td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td></td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>G DATA</td>
<td></td>
<td></td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>McAfee</td>
<td></td>
<td></td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>TrendMicro</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Selected Antivirus Vendors (not a complete list)

World’s No.1 Antivirus and Internet Security

1 year FREE
Buy two years, get the third free

Offer valid on 25 seats or more of ESET NOD32 Antivirus Business Edition and ESET Smart Security Business Edition

PROMO CODE: 2011Q4PROMO
10/4-12/31/11. For terms, visit www.eset.com/q4promo

www.eset.com