Professor James Holderman is leading an effort to improve the e-discovery process for lawyers and IT teams. P20

Will Canada go cashless? Residents respect the dollar, but it’s time to weigh the risks of the next generation of payments. P21

Streamlining defenses Countless organizations have built their own situation rooms to protect data and respond to threats. P28

Federation 2.0 Standards are maturing just in time for identity federations to aid cloud and mobile access. P30
Real-Time Log Analysis for Proactive Network Defense

Logs have to be analyzed. Regulations such as PCI, HIPAA, NERC CIP, SOX and GLBA require it, but let’s face it - traditional log analysis is reactive. You have a choice: You can pick a product that is forensically focused: gathering logs, storing them in a database and offering search and reporting, OR you can choose TriGeo SIM. TriGeo SIM is the ONLY log analysis solution that combines real-time log analysis with active response for true Proactive Network Defense.

Real-time, in-memory, analysis is the key. TriGeo’s enterprise-wide view of the network makes it possible to capture, correlate and actively respond to network attacks and insider threats - at network speed. For proactive network defense, there is only one choice.

See the webinar where you will see TriGeo SIM in action under real-world conditions. Watch as we capture, correlate and respond to network attacks and policy violations - all in real-time. Join us for a live webinar where you’ll see TriGeo SIM in action under real-world conditions.

Cover photo by Susan Andrews

© 2010 TriGeo Network Security, Inc. All rights reserved. TriGeo SIM is a trademark of TriGeo Network Security, Inc.
You might be next

We’ve seen a tsunami of data breaches crashing over numerous large corporations lately, from Sony’s PlayStation Network and Google to Epson and, most recently, Citibank and the International Monetary Fund. It seems cybercriminals have been mighty active these last few months.

What such activity may indicate is anyone’s guess. And, there are plenty of industry folks looking to predict just who might be in the path of this still raging wave of online criminal activity, or just what types of information could be compromised next.

My thought: Pretty much everyone is a potential victim. That’s obvious, right? So much so that large enterprises would have, at minimum, a CISO in place to manage a sound risk management and incident response plan. Yet, Sony, a publicly traded, multinational conglomerate with assets in the billions, was prompted to hire a CISO only after the loss of millions of customers’ data and endless bad press coverage over its bungling reaction to now multiple breaches.

And while most pros would agree with Sony Executive Deputy President Kazuo Hirai’s comments that “no system is 100 percent safe,” its various networks being victimized by hackers in quick succession underscores just how lax its corporate security practices have been. Hirai acknowledged as a “realization” that his company, the world’s fifth largest media conglomerate, must undertake “constant monitoring and constant vigilance.” From my perspective, though, to have that realization after experiencing multiple breaches is unacceptable.

As the company strives to rebuild both the integrity of its various systems and its reputation, other organizations are taking notice. According to Intel CISO Malcolm Harkins, who was recently quoted in a news item on website BankInfoSecurity.com, the many breaches that have prompted Sony to take some steady steps to restore its company name and IT infrastructures are reminders to other sectors’ information security leaders that they are potential foils for cybercrime groups. All the risks they face, therefore, must be managed diligently. And, as part of these deeply considered and well-planned mitigation efforts, both CISOs and their executive leaders must concede they eventually will see their infrastructures compromised.

Core to this long-existing reality, of course, is having a knowledgeable, tireless and resolute CISO on your payroll in the first place.

Ilenna Armstrong is editor-in-chief of SC Magazine.
Professional face on a regular basis. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

Vectors being used by cybercriminals, the promotion of a defense-in-depth strategy, and focusing on the ‘soft’ inside, which has led to a shift in how the outside of a network that protects critical information is viewed. This has been described as the ‘hard shell’ on the company’s security architecture, but more importantly, it is the firm’s strong foundation. Security is no longer just about perimeter security.

ON DEMAND

Implementing fixes

What can companies do to protect their valuable resources? How do they do so without adding overhead or slowing down business efficiency? How can companies build a robust defense-in-depth strategy that reduces risk while meeting the needs of today’s cybercriminals?

SC MAGAZINE EDITORIAL ADVISORY BOARD 2011

Rich Baich, principal, security & privacy, Deloitte and Touche
Greg Ball, global information protection and security lead partner, KPMG
Christopher Burgess, senior security adviser, corporate security programs office, Cisco Systems
Jaime Chanaga, managing director, CSO Board Consulting
Rufus Connell, research director - information technology, Frost & Sullivan
Dave Cuillinnane, chief information security officer, eBay
Mary Ann Davidson, chief security officer, Oracle
Dennis Duvlin, chief information security officer, Brandeis University
Gerhard Eschelbeck, chief technology officer and chief information security officer, Symantec
Maurice Hampton, information security & privacy services leader, Clark Schaefer Consulting
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
Kris Lovejoy, vice president of IT risk, office of the CIO, IBM
Tim Mathew, director, information protection, KPMG
Stephen Northcutt, president, SANS Technology Institute
Randy Sanonivo, former general director, information security, General Motors
* Howard Schmidt, cybersecurity coordinator, U.S. White House; chief executive officer, Information Security Forum
Justin Sommestad, chief information security officer, Yahoo!
* Sylvek, former chief information security officer, Symantec
* Varghese, former director of information security, Verizon
Craig Spieles, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
W. Hord Tipton, executive director, (ISC)²; former CIO, U.S. Space Force at the Interior
Amit Yoran, chief executive officer, NetWitness; former director, Department of Homeland Security’s National Cyber Security Division
* omissions

WHO’S WHO AT SC MAGAZINE

EDITORS

EDITOR-IN-CHIEF Ilona Armstrong
Ilona.armstrong@haymarketmedia.com
EXECUTIVE EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
SENIOR EDITOR Angela Moscaritolo
angela.moscaritolo@haymarketmedia.com
TECHNOLOGY EDITOR Peter Thompson
peter.thompson@haymarketmedia.com
SC LAB MANAGER Mike Stephenson
mike.stephenson@haymarketmedia.com
DIRECTOR OF SC LAB OPERATIONS John Aitken
john.aitken@haymarketmedia.com
SC LAB EDITORIAL ASSISTANT Judy Traub
judy.traub@haymarketmedia.com
PROGRAM DIRECTOR, SC CONGRESS CANADA Eric Green
eric.green@haymarketmedia.com
CONTRIBUTORS Deb Rackoff, Beth Schult, Stephen Lawton
DESIGN AND PRODUCTION ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com
VP OF PRODUCTION & MANUFACTURING Louis Marini
louis.marini@haymarketmedia.com
SENIOR PRINT AND DIGITAL CONTROLLER Krisie Vardaman
krisie.vardaman@haymarketmedia.com
SEVENTEEN
SENIOR EVENTS MANAGER Natasha Mulla
natasha.mulla@haymarketmedia.com
SENIOR EVENTS COORDINATOR Anthony Curry
anthony.curry@haymarketmedia.com
U.S. SALES
ADVERTISING DIRECTOR David Shuman
(646) 638-6208 david.shuman@haymarketmedia.com
EASTERN REGIONS SALES MANAGER Mike Shemesh
(646) 638-6202 mike.shemesh@haymarketmedia.com
WEST COAST BUSINESS MANAGER Matthew Allison
(425) 346-6140 matthew.allison@haymarketmedia.com
National Account Manager - Event Sales Mike Alessie
(646) 638-6016 mike.alessie@haymarketmedia.com
ACCOUNT EXECUTIVE Dennis Kostriver
(646) 638-6203 dennis.kostriver@haymarketmedia.com
SALES/EDITORIAL ASSISTANT Roo Howar
(646) 638-6204 roo.howar@haymarketmedia.com
UK ADVERTISING DIRECTOR Mark Gordon
(020) 8287-4672 mark.gordon@haymarketmedia.com
LICENSE & REPRINTS SALESEXECUTIVE Kathleen Moriarty
(646) 638-6101 kathleen.moriarty@haymarketmedia.com
EMAIL LIST RENTAL EMAIL, SALES ACCOUNT EXECUTORS
Frank Capella, Edith Riesz
(408) 730-3832 francisc@pacificdirect.com
CHICA GO
GROUP CIRCULATION MANAGER Sherry Common
(646) 638-6003 sherry.common@haymarketmedia.com
SUBSCRIPTION INQUIRIES CUSTOMER SERVICE:
(800) 558-1703 EMAIL: circ@haymarketmedia.com
WEB: www.scmagazineus.com
MANAGEMENT CHAIRMAN William Passover
PRESIDENT Lisa Kirk
DEPUTY MANAGING DIRECTOR Tony Kuefl

Key Benefits of Attending

• Discover thousands of cutting-edge security solutions from 700+ exhibitors.
• Expand your career network, face-to-face.
• Examine peer-tested strategies that really work.
• Build your leadership, increase your knowledge and productivity by attending any of the 200 conference sessions.
• Save time and money by researching products/services on the show floor.
• Take home a wealth of indispensable tools that will re-energize your career and your organization.
• Earn recertification credits for your ASIS board (or (ISC)² certifications.

Threat Report

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

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

SARNA, ONTARIO – City police are seeking extra funding to increase internet crime prevention and enforcement. The Sar-nia Police Service Board applied for a nearly $200,000 grant to update police software and train more officers to deal with online fraud and cyberbullying.

VANCOUVER – Canadian web-hosting provider Islandnet.com was hit with a DDoS attack that blocked access to 5,000 customers’ websites for more than 24 hours. An anonymous source, who had a problem with a blog Islandnet.com was hosting, claimed responsibility.

WOOLINGTOM, N.C. – Police gathered at a summit to raise aware-ness about cybersecurity. FBI agents briefed attendees on high-profile hacking incidents and how law enforcement agencies around the globe are working to track down and arrest criminals.

WORONUCK, N.C. – A hacker from North Carolina was sentenced to 37 months in federal prison for attempting to embezzle more than $200,000 from three dozen Texas ATMs. Thor Morris, 20, of Jackson-ville, N.C., confided to an FBI informant that he planned to reprogram the ATMs to make them issue $20 for every $1 requested.

U.K. – U.S. President Barack Obama said it is up to U.K. officials to decide whether accused NASA and U.S government hacker Gary McKinnon should stand trial here. McKinnon could face up to 60 years in prison if convicted of charges that in 2001 he hacked into 97 computers operated by the U.S. government and military.

SOUTH KOREA – Police charged two men with hacking into lender Hyundai Capital’s database to steal personal information of 13,000 clients and then threatening its exposure unless the company paid them nearly $500,000. Hyun-dai Capital, meanwhile, is being investigated by regulators for its apparent lax security practices.

AUSTRALIA – The federal government will draft its first-ever Cyber White Paper, which will detail how the public and private sector and individual users can collaborate to manage risks in cyberspace. The paper will address crime, security and national defense, and is scheduled to be published next year.

Norway – The military was targeted after it joined other NATO forces in air strikes against Libya. Newspaper VG reported that several hundred defense personnel received a socially engineered email that contained a malicious attachment enabling attacker access. No confidential data was stolen, however.

Estonia – The U.S. Secret Service opened an office in Tallinn that is tasked with fighting cybercrime. The four-person outpost will work to train Estonian, Latvian and Lithuanian au-thorities about crimes such as money laundering and identity theft. Estonia was victimized by fierce DDoS attacks in 2007 after relocating a Russian war memorial.

Australia – The federal government will draft its first-ever Cyber White Paper, which will detail how the public and private sector and individual users can collaborate to manage risks in cyberspace. The paper will address crime, security and national defense, and is scheduled to be published next year.

Sweden – The military was targeted after it joined other NATO forces in air strikes against Libya. Newspaper VG reported that several hundred defense personnel received a socially engineered email that contained a malicious attachment enabling attacker access. No confidential data was stolen, however.

Estonia – The U.S. Secret Service opened an office in Tallinn that is tasked with fighting cybercrime. The four-person outpost will work to train Estonian, Latvian and Lithuanian au-thorities about crimes such as money laundering and identity theft. Estonia was victimized by fierce DDoS attacks in 2007 after relocating a Russian war memorial.

Norway – The military was targeted after it joined other NATO forces in air strikes against Libya. Newspaper VG reported that several hundred defense personnel received a socially engineered email that contained a malicious attachment enabling attacker access. No confidential data was stolen, however.

Estonia – The U.S. Secret Service opened an office in Tallinn that is tasked with fighting cybercrime. The four-person outpost will work to train Estonian, Latvian and Lithuanian au-thorities about crimes such as money laundering and identity theft. Estonia was victimized by fierce DDoS attacks in 2007 after relocating a Russian war memorial.

Norway – The military was targeted after it joined other NATO forces in air strikes against Libya. Newspaper VG reported that several hundred defense personnel received a socially engineered email that contained a malicious attachment enabling attacker access. No confidential data was stolen, however.

Estonia – The U.S. Secret Service opened an office in Tallinn that is tasked with fighting cybercrime. The four-person outpost will work to train Estonian, Latvian and Lithuanian au-thorities about crimes such as money laundering and identity theft. Estonia was victimized by fierce DDoS attacks in 2007 after relocating a Russian war memorial.
ThreatStats

A virus infected computers at various Massachusetts state departments.

Top 10 malicious programs

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Change</th>
<th>Number of infected computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AdWare.Win32.HotBar.dhn</td>
<td>0</td>
<td>783,931</td>
</tr>
<tr>
<td>2</td>
<td>Trojan.JS.Popupper.aw</td>
<td>0</td>
<td>739,998</td>
</tr>
<tr>
<td>3</td>
<td>AdWare.Win32.FunWeb.id</td>
<td>4</td>
<td>472,777</td>
</tr>
<tr>
<td>4</td>
<td>Trojan-Downloader.JS.ISlBarcx</td>
<td>New</td>
<td>364,197</td>
</tr>
<tr>
<td>5</td>
<td>AdWare.Win32.FunWeb.ip</td>
<td>1</td>
<td>243,612</td>
</tr>
<tr>
<td>6</td>
<td>Trojan.JS.Agent.hxw</td>
<td>New</td>
<td>233,868</td>
</tr>
<tr>
<td>7</td>
<td>Exploit.HTML.CVE-2010-4452.h</td>
<td>New</td>
<td>182,193</td>
</tr>
<tr>
<td>8</td>
<td>Trojan.JS.Agent.bun</td>
<td>New</td>
<td>180,370</td>
</tr>
<tr>
<td>9</td>
<td>Trojan-Downloader.JS.Iframe.cew</td>
<td>New</td>
<td>172,075</td>
</tr>
<tr>
<td>10</td>
<td>Exploit.CVE-2010-1885.k</td>
<td>New</td>
<td>150,738</td>
</tr>
</tbody>
</table>

The number of incidents involving attempts to infect computers with rogue anti-virus software via the web was 109,218. However, the decrease in the amount of rogueware does not mean that this type of malware has ceased being developed.

Source: Kaspersky Lab

Phishing

33 percent spike in May

May marked a surprising 33 percent increase in attacks on the global scale. The composition of attack methods remained nearly unchanged — 82 percent of phishing sites used hijacked websites to launch their attacks. Commercial hosting, free hosting and hijacked computers represented hosting methods used in lower ratios through last month.

Source: RSA Anti-Fraud Command Center

Zombie IPs

The biggest increases in month-over-month zombie activity occurred in India, Brazil and Pakistan.

Source: Commtouch Software Online Labs

Top 5 attacks used by U.S. hackers

1. Barnloit trojan
2. Zeus trojan
3. TDSS Downloader trojan
4. Sinowal trojan
5. Alureon trojan

Top 5 attacks used by foreign hackers

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

Top 10 spyware threats

1. Fraudtool.Win32.FakeRean: Rogue security program
4. Gozi trojan
5. ZeuS trojan

DataBank
Update

NEWS BRIEFS

After it was learned that hackers had compromised classified federal documents, the head of Canada’s intelligence agency made it clear: “Cyber-based spying is the fastest growing form of espionage.” The statement was contained in the Canadian Security Intelligence Service’s (CSIS) annual report to Parliament, which was tabled in early June. In the report, CSIS Chief Richard Fadden noted that “hostile actors” are targeting a wide range of organizations, including government, business and education and home users. The goal, he wrote, is the acquisition of “technology, intellectual property, military strategy and commercial or weapons-related information.”

CS Industry Canada employees may have infected his computer with dangerous malware by looking at porn sites, according to an investigative report. QMI Agency obtained a copy of a security report that detailed inappropriate surfing activity by the worker at Industry Canada’s Ottawa office. The employee, who may not have been disciplined, also allowed his computer to be infected with trojans.

Despite the major compromise of intellectual property related to its SecurID product line, RSA had implemented a process that limited what the hackers could get away with, the company’s security architect told an audience at June’s SC Congress Canada.

The Quote

Security and usability are sometimes at odds.

— Maxim Veytsman, security consultant at Security Compass, speaking during a session on mobility at SC Congress Canada in June.

Award winners

Some of the country’s brightest security stars were recognized at the 2011 SC Awards Canada. Part of the second annual SC Congress Canada, the event honors the achievements of groups and individuals striving to protect the privacy and critical data belonging to Canadian businesses and customers. “These individuals and companies are fighting the good fight,” said Ilenna Armstrong, SC Magazine Canada.

Speaking on a panel focused on how a properly implemented risk program can help defend against specially targeted attacks known as advanced persistent threats, Robert Griffin explained how RSA’s process of dynamics, adaptation, analytics and assessment prevented further damage.

Employee emails, contact lists, authentication credentials and sensitive company documents are some of the primary assets that must be protected on mobile devices, audience members said during a standing-room-only mobile session at SC Congress Canada. “The more portable the device, the more likely it is to be stolen, and that is the biggest mobile threat,” said speaker Sahba Kazerooni, director of professional services and training at application security firm Security Compass. Besides lost mobile devices, security practitioners must think about how they can stem the growing tide of mobile malware and man-in-the-middle attacks, Kazerooni said.

With ready-made exploit kits and classes of vulnerabilities that date back to the 1990s at their disposal, hacker groups are finding easy pickings. A string of breaches has cemented the notion that these attacks may not be able to be fully stopped, but contained enough to prevent a massive compromise, Derek Manly, senior security strategist at Fortinet, told a crowd at SC Congress Canada in Toronto. “It’s really inevitable that more of these attacks are going to occur,” he said. “A lot of these attacks are age-old.”

Debate

The federal breach notification law, proposed by President Obama, should replace existing state laws.

For

David Seltzer, founder and executive director of Cyber Security Strategies, who specializes in cybersecurity.

AGAINST

Neal O’Farrell, executive director, York Council.

The SC Magazine poll

Should SCADA (control) systems be connected to the public internet?

5.56% Either way is fine. This issue is overblown.

13.89% Yes, but securely, as web connectivity helps drive the business.

80.56% No, this risks attack or sabotage.

To take our latest weekly poll, click on www.scmagazineus.com.

The stats

34 zero-day vulnerabilities detected in four SCADA products in one advisory

75% of polled global energy organizations sustained at least one intrusion over the last year

Source: Laura Auerwoma/O’Farrell.

P15

2 minutes on...

A new cybersecurity index aims to capture CSO wisdom.

Me and my job

This pro monitors networks for security indicators.

Skills in demand

The project manager has risen to the top of the food chain.

P14

P15

For more on this issue, see the June 13, 2011 issue of the SC Magazine on newsstands now or download the July 2011 issue of SCMagazineUS.com.

Threat of the Month

AndroidOS/Sm-spaccem

What is it?

Mobile malware which leverages Trojan, bot and “logic bomb” tricks.

How does it work?

Infection requires the installation of a trojaned app called “Holy King’s Bible.” Following installation and a reboot, a rogue service is started that queries a remote location for command-and-control instructions while attempting to communicate the device’s phone number to another host-based service. An SMS listener is controlled via the logic bomb and only starts when the system time reaches May 21, 2011. A doomsday message is then spammed via SMS to all contacts. On May 22, a new message is sent out, and the wallet gets charged.

Should I be worried?

It illustrates that tricks employed against the PC platform will be repackaged against the Android.

How can I prevent it?

Installing only Android Market apps is a start, but we recognize the openness of the Android platform is tempting, so a mobile security app is recommended.

Source: Dan DeFiore, director of threat research, CA Technologies (CBA).
Indexing risk perception

In the complex world of cybersecurity, it often is difficult to know which threats pose the most risk.

A new index developed by leading security thinker Dan Geer and risk management consultant Mukul Pareek aims to tackle that issue by measuring security practitioners’ perceptions of various cyber risks. The Index of Cybersecurity, launched in April, is based on a monthly survey of 300 security pros, who are asked whether threats, as well as their own defenses and the extent of information-sharing among peers, are falling, static or rising compared to the previous month.

The index, which has been on a steady ascent since March, provides a baseline to which others can compare their own views, said Geer, chief security officer of the Central Intelligence Agency’s investment arm, In-Q-Tel. “That allows me to make decisions,” Geer said. “My peers see the world as getting better or worse. [The index] is decision support for those outside the survey.”

Some have questioned the effort, however, for measuring perception rather than actual risks, such as the number of individual attacks or vulnerabilities. “I’m not sure how useful it will be for aiding decision-making,” said Jon Gossels, president and CEO of consultancy System Experts. “You want to make decisions based on real statistics.”

Even the best security practitioners, who are time-strapped and inundated with vendor hype, lack a complete knowledge of the threat environment, said Joshuaorman, research director of the enterprise security practice at analyst firm The 451 Group.

Also, risk is not consistent across the board, said John Pescatore vice president and research fellow at consultancy Gartner. “The risk for a bank in Bombay is always going to be different than the risk for a video game manufacturer in Mountain View,” he said.

But Geer pointed out that others have, for some time, been measuring actual cyber risks — with mixed results. Usually such efforts are hampered by disagreements about the definition of reality, such as what constitutes a unique vulnerability. This instead constitutes a wisdom-of-crowds-type approach.

“The reason for creating a sentiment-based index is to say experts are of the following opinion — how ever they came to it,” Geer said. — Angela Moscaritolo

1,043.2
Index of Cybersecurity value for May 2011, indicating an increase in the perception of risk from the base value of 1,000 for March

2 MINUTES ON...

Jobs market

Me and my job

Peter Morin

How do you describe your job to average people?

I am responsible for a specialized team that monitors our network for security indicators which may suggest an attack, responds to incidents and provides metrics to management regarding the security posture of our organization. I am also responsible for assisting project teams to better understand their information security risks and recommending improvements to the security of their applications, systems and processes to mitigate those risks.

Why did you get into IT security?

Like many, I started working in the field of enterprise networking, dabbling in security whenever needed. Eight years ago, the opportunity to specialize in the emerging field of cybersecurity was presented to me. I found security engaging, challenging and rewarding and couldn’t see myself doing anything else from that point on.

What is one of your biggest challenges?

One of my biggest challenges is the constant battle to be one step ahead of attackers. With an increase in persistent and complex attacks, we have to ensure that we are as agile as the attackers. Having the proper people, tools and processes to defend our network is a necessity.

What keeps you up at night?

Not knowing what new threats attackers may have up their sleeves, how these threats will affect our organizations’ business, and what type of defenses are needed. Even more frightening, do we have the ability to detect these new attacks?

Of what are you most proud?

I am most proud of the skilled, dedicated team I work with. The success of any information security program is reliant on a group of well-trained, experienced and motivated professionals. I work hard to stay abreast of current trends and pass this knowledge onto others through speaking engagements and training.

Christopher Brenton, cloud security architect at CloudPassage

CloudPassage, maker of server security and compliance solutions for the cloud, has hired Christopher Brenton as CloudPassage’s cloud security architect. Brenton previously served at Dell. He also was one of the founders of The Honeyynet Project, a security research organization, and among the first holders at the SANS Internet Storm Center.

www.cloudpassage.com

Charlie Miller, best known for his zero-day vulnerability discoveries in Apple products, has been named principal research consultant at security firm Accuvant. He previously worked as principal analyst at Independent Security Evaluators. Miller continued his streak at Pwn2Own this year when he exploited the iPhone 4.

www.accuvant.com

Avenda Systems, maker of identity-based network access solutions, has partnered with Meraki, a cloud networking provider. The alliance enables customers to deploy enterprise-wide, context-aware policy services, network access control and advanced guest access across all access methods.

www.avendasys.com, meraki.com

Bob Walder has joined independent network testing facility NSS Labs as chief research officer to drive research and consulting.

www.nsslabs.com

HippTrust, maker of botnet and malware detection solutions, has hired Chris Davis as director of malware research. Davis formerly worked at Morrigan, an Ottawa-based security research firm. Davis, who is known for his discovery of the Mariposa botnet, will lead iTrust’s malware and security intelligence research.

www.iptrust.com

Deli SecureWorks has named Doug Steelman as chief information security officer. He will be charged with defending Dell SecureWorks’ networks. His most recent position was director of the U.S. Department of Defense’s Dynamic Network Defense Operations for the U.S. Cyber Command.

www.dell.com/secureworks

Mu Dynamics, maker of botnet and malware research. Davis formerly served as senior VP of sales for Asia Pacific. The pair is responsible for driving regional go-to-market strategy. Olson formerly was VP of worldwide sales at Mu DynamiCS, and Rowland served as senior VP of sales at Workbrain.

www.mudynamics.com

Blue Coat Systems, provider of web security and WAN optimization solutions, has named Gary Olson VP of sales for the Americas, and Steve Rowland VP of sales for Asia Pacific. The pair is responsible for driving regional go-to-market strategy. Olson formerly was VP of worldwide sales at Mu DynamiCS, and Rowland served as senior VP of sales at Workbrain.

www.bluecoat.com

JOBS MARKET

Me and my job

Peter Morin

How do you describe your job to average people?

I am responsible for a specialized team that monitors our network for security indicators which may suggest an attack, responds to incidents and provides metrics to management regarding the security posture of our organization. I am also responsible for assisting project teams to better understand their information security risks and recommending improvements to the security of their applications, systems and processes to mitigate those risks.

Why did you get into IT security?

Like many, I started working in the field of enterprise networking, dabbling in security whenever needed. Eight years ago, the opportunity to specialize in the emerging field of cybersecurity was presented to me. I found security engaging, challenging and rewarding and couldn’t see myself doing anything else from that point on.

What is one of your biggest challenges?

One of my biggest challenges is the constant battle to be one step ahead of attackers. With an increase in persistent and complex attacks, we have to ensure that we are as agile as the attackers. Having the proper people, tools and processes to defend our network is a necessity.

What keeps you up at night?

Not knowing what new threats attackers may have up their sleeves, how these threats will affect our organizations’ business, and what type of defenses are needed. Even more frightening, do we have the ability to detect these new attacks?

Of what are you most proud?

I am most proud of the skilled, dedicated team I work with. The success of any information security program is reliant on a group of well-trained, experienced and motivated professionals. I work hard to stay abreast of current trends and pass this knowledge onto others through speaking engagements and training.

Christopher Brenton, cloud security architect at CloudPassage

CloudPassage, maker of server security and compliance solutions for the cloud, has hired Christopher Brenton as cloud security architect. Brenton previously served at Dell. He also was one of the founders of The Honeyynet Project, a security research organization, and among the first holders at the SANS Internet Storm Center.

www.cloudpassage.com

Charlie Miller, best known for his zero-day vulnerability discoveries in Apple products, has been named principal research consultant at security firm Accuvant. He previously worked as principal analyst at Independent Security Evaluators. Miller continued his streak at Pwn2Own this year when he exploited the iPhone 4.

www.accuvant.com

Avenda Systems, maker of identity-based network access solutions, has partnered with Meraki, a cloud networking provider. The alliance enables customers to deploy enterprise-wide, context-aware policy services, network access control and advanced guest access across all access methods.

www.avendasys.com, meraki.com

Bob Walder has joined independent network testing facility NSS Labs as chief research officer to drive research and consulting.

www.nsslabs.com

HippTrust, maker of botnet and malware detection solutions, has hired Chris Davis as director of malware research. Davis formerly worked at Morrigan, an Ottawa-based security research firm. Davis, who is known for his discovery of the Mariposa botnet, will lead iTrust’s malware and security intelligence research.

www.iptrust.com

Deli SecureWorks has named Doug Steelman as chief information security officer. He will be charged with defending Dell SecureWorks’ networks. His most recent position was director of the U.S. Department of Defense’s Dynamic Network Defense Operations for the U.S. Cyber Command.

www.dell.com/secureworks

Mu Dynamics, maker of botnet and malware research. Davis formerly served as senior VP of sales for Asia Pacific. The pair is responsible for driving regional go-to-market strategy. Olson formerly was VP of worldwide sales at Mu DynamiCS, and Rowland served as senior VP of sales at Workbrain.

www.mudynamics.com

Blue Coat Systems, provider of web security and WAN optimization solutions, has named Gary Olson VP of sales for the Americas, and Steve Rowland VP of sales for Asia Pacific. The pair is responsible for driving regional go-to-market strategy. Olson formerly was VP of worldwide sales at Mu DynamiCS, and Rowland served as senior VP of sales at Workbrain.

www.bluecoat.com

JOBS MARKET

Me and my job

Peter Morin

How do you describe your job to average people?

I am responsible for a specialized team that monitors our network for security indicators which may suggest an attack, responds to incidents and provides metrics to management regarding the security posture of our organization. I am also responsible for assisting project teams to better understand their information security risks and recommending improvements to the security of their applications, systems and processes to mitigate those risks.

Why did you get into IT security?

Like many, I started working in the field of enterprise networking, dabbling in security whenever needed. Eight years ago, the opportunity to specialize in the emerging field of cybersecurity was presented to me. I found security engaging, challenging and rewarding and couldn’t see myself doing anything else from that point on.

What is one of your biggest challenges?

One of my biggest challenges is the constant battle to be one step ahead of attackers. With an increase in persistent and complex attacks, we have to ensure that we are as agile as the attackers. Having the proper people, tools and processes to defend our network is a necessity.

What keeps you up at night?

Not knowing what new threats attackers may have up their sleeves, how these threats will affect our organizations’ business, and what type of defenses are needed. Even more frightening, do we have the ability to detect these new attacks?

Of what are you most proud?

I am most proud of the skilled, dedicated team I work with. The success of any information security program is reliant on a group of well-trained, experienced and motivated professionals. I work hard to stay abreast of current trends and pass this knowledge onto others through speaking engagements and training.
Got something to say?

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

From the online mailbag

In response to a June news story, Gmail users targeted by Adobe Flash exploit:

Sounds like a serious flaw which can turn a script into executing social networking posts not authorized by a user/member!? Ernie Hernandez

Why can’t we get Flash on iPhone? I want hackers to take actions on my behalf. Sounds like a real concierge service when you put it that way.
Anonymous

In response to the June feature, Eliminating Trust:

Your story leaves untouched the human factor – people want to be personally known and trusted. I’m aware of a model employee whose behavior was brought under suspicion, audited and found to be blameless. However, the scrutiny itself was so demoralizing that they no longer trust their employer and now take great pains to shield their network activities from further analysis.
Paul Landers

In response to Illena Armstrong’s editorial in the May issue, What to learn from the RSA breach:

Good piece. As you said, I doubt we have heard the last of this incident or its repercussions. I remember a number of years ago at InfoSecurity London, RSA conducted a social engineering attack at Victoria. They gave out free pens to people in exchange for their account and password. It seemed more of a marketing stunt than anything else, but they sure made a big deal out of it. Oh the irony. The biggest problem with social engineering is keeping it on people’s radar.
Richard Starnes

In response to a May news story, Sony delays PSN restart as third breach is discovered, we received quite a big response:

Sony, Every “update” so far has been the exact same thing they’ve said since day one, except worded just a little different. I understand that it takes time to fix this kind of thing. Bringing the network up a little bit at a time sounded promising. So why do we have to wait until the end of May for the whole network to come back online? Why wouldn’t Sony at least get the multiplayer gaming back up? Just bring back the multiplayer gaming for now.
Darsynjyin_1

They just decided to get a security officer? They should have had one years ago.
Jrod919

This is very annoying, but I am somewhat grateful that the breach has been found and someone is taking the blame and working on correcting the problem. I have taken a setback because I signed up for GameFly, and I am not able to play the games that I rent online. Being an active and supportive user, will Sony do anything about people in my situation?
Nathannewton

Sony, you should have encrypted the data anyway. When PSN is back up, I think we deserve more than 30 days free PlayStation. Plus, get your act together.
Ummar_sajid

The opinions expressed in these letters are not necessarily those of SC Magazine.
Signing on the dotted line of HIPAA

Bryan Cline, CSO and director of information security at Catholic Health East

G
iven that a misrepresentation of the facts during attestation could result in civil and criminal penalties, what does a health care executive need to feel comfortable about before signing on the dotted line?

Since the meaningful use objective for security and privacy requires a HIPAA Security Rule-based risk analysis, we know the examination must include scoping, data collection, identification and documentation of potential threats and vulnerabilities, as well as an assessment of current security measures.

To achieve this, scope the assessment to the electronic health record (EHR) technology implemented to support “meaningful use,” defined as achieving large improvements in care. Ensure you assess the EHR system; and people, processes, policies and standards related to their control.

When assessing, try to focus on high-risk areas, which can be determined by examining recent breach data, and conduct a top-down control analysis. Collect only enough information to support your assessment of a control’s effectiveness and then move on. It doesn’t take much to determine if a control is absent or not working as intended.

Also, formally report control deficiencies and corrective action plans to executive management. Failure to take reasonable and appropriate measures to remediate identified deficiencies is contrary to the intent of the HIPAA Security Rule and could make an entity subject to penalties for making false statements during attestation. Further, track your control status and remediation progress against industry benchmarks, which also helps determine the relative priority of various corrective actions. Too, consider using a health care-specific assessment methodology which incorporates these recommendations.

Obtain and use a governance, risk and compliance tool to manage the workflow associated with assessment and remediation, retain assessment data and provide automated reporting.

And, above all, make sure the executive attesting to meaningful use is kept informed about ongoing risks, control updates and remediation status. It is their signature on the dotted line.

30 seconds on...

> Assessment strategies
  > There are some basic guidelines to consider when shopping for an assessment, says Bryan Cline. First, make sure the methodology demonstrates reasonable practices.

> Best practices
  > To achieve that, it is vital to select a sound risk assessment methodology that aligns control decisions with industry standards and best practices, he says.

> Serious efforts needed
  > Assessments should be efficient, as well. “Meaningful use” focuses on certified EHR systems. Use sampling techniques for similar facilities and take remediation seriously.

> Managing the portfolio
  > This can be done by developing sound corrective action plans, but don’t over- or under-commit, says Cline. Instead, actively manage remediation as a portfolio of initiatives.


Real-world web abuse

Is APT the new FUD?

Frank Andrus, co-founder and CTO, Bradford Networks

A
dvanced persistent threat (APT) is a term with a specific meaning—generally referring to a sophisticated and well-organized cyberattack against a singular entity. These types of attacks are so well-coordinated that the term is generally used in regard to a nation-state or government-sanctioned attack. But, in the security industry, buzz sells, and APT is now becoming synonymous with any form of cyberattack.

In March, RSA announced that it was the victim of an APT attack. Given the stature of the company, the target of the attackers (information to compromise the effectiveness of the company’s SecureID line) and the openness of the post-attack investigation, there is little doubt RSA was indeed hit with an APT.

But it seems the term now is thrown out any ring to a sophisticated and well-organized cyberattack against a singular entity. These types of attacks are so well-coordinated that the term is generally used in regard to a nation-state or government-sanctioned attack. But, in the security industry, buzz sells, and APT is now becoming synonymous with any form of cyberattack.

In March, RSA announced that it was the victim of an APT attack. Given the stature of the company, the target of the attackers (information to compromise the effectiveness of the company’s SecureID line) and the openness of the post-attack investigation, there is little doubt RSA was indeed hit with an APT.

And, above all, make sure the executive attesting to meaningful use is kept informed about ongoing risks, control updates and remediation status. It is their signature on the dotted line.

It is important that we learn the lessons of each breach...

Kyle Adams, chief architect, Mykonos Software

It is important that we learn the lessons of each breach...
Representing a field that is notorious for being a laggard when it comes to advancing in the digital era, Chief Judge James Holderman knew he was undertaking an ambitious task when he began his formal quest two years ago to reform the practice of electronic discovery.

But there was one fundamental reason that propelled the 65-year-old to want to change the landscape: He believed the onerous and costly nature of e-discovery was limiting the service of justice. In some cases, in fact, plaintiffs were so inundated with pre-trial discovery demands by the claimants’ lawyers that they had no choice but to settle before the case ever made it to trial.

“It was nebulous at best as to what a party had to preserve and, frankly, the law hasn’t advanced,” Holderman says. “It affects justice in the United States because of the cost and burden of electronically stored information.”

As chief judge of the U.S. District Court for the Northern District of Illinois since 2006 – he joined the court in 1985 after being nominated by President Reagan – Holderman believed that if he didn’t take the initiative, the problems would only continue and likely worsen.

“I knew it was a problem when general counsel were coming up to me and saying that it’s a problem and they didn’t even have a case in front of me,” he says. “Frankly, there was no question in my mind that at some point in time all discovery was going to be e-discovery. We needed to do something non-traditional.”

It was May 20, 2009, when Holderman and Magistrate Judge Nan Nolan met with a group of lawyers at the U.S. District courthouse in Chicago – “the best and brightest of the people we knew that were knowledgeable about electronically stored information” – to launch the Seventh Circuit Electronic Discovery Pilot Program, a first-of-its-kind effort in the United States and one that builds on a proclamation from The Sedona Conference to remove adversarial relations from the pre-trial discovery process.

The main issue that came out of the initial meeting was the burden of cost, Holderman says. As the calendar flipped to the 21st century, legal teams began asking for exponentially more information – much of it often
unnecessary – because data proliferated from paper records stored in a filing cabinet to information spread across email and other corporate systems.

“I said, ‘Here’s what we should do,’” Holderman recalls. “We should develop principles and guidelines for lawyers involved in litigation in how they should conduct themselves when dealing with electronically stored information so the burden of asking for everything and providing the minimum is avoided. That way we focus more on what is needed and eliminate some of the discovery that is particularly burdensome.”

Meanwhile, Holderman also sought to educate individual corporations on the need to categorize their data to make the preservation and early-case assessment stages more manageable and efficient.

On Dec. 1, 2006, an amendment to the Federal Rules of Civil Procedure took effect that ordered businesses and their lawyers to, at the start of any lawsuit, meet and discuss the scope of electronically stored information in the case. The updated regulation also mandated that organizations, at the first whiff of a possible legal action, preserve any relevant data.

Even so, nearly five years later, organizations are falling short at properly complying with the new guidelines. In fact, it took until the 2009 America Invents Act that ordered businesses to start archiving electronically stored information for e-discovery purposes.

“From the start of the process it's clear that our approaches needed major improvement...to make the system as efficient as it can be for our clients.”

What we need to do is develop a system in which everyone is not trying to hide something. That is the reason we're proposing Guidelines to Information Sharing and Discovery, Regan says. “I think we need to change the way we focus more on what is needed and less on collecting everything.”

A combination of amendments to the Federal Rules of Civil Procedure – which mandated that organizations, at the first sign of a possible lawsuit, must begin archiving electronically stored information (ESI) – are the result of this focus.

Discovery proportionality:

“[R]equests for production of electronically stored information (ESI) and related responses should be reasonably targeted, clear, and as specific as practicable.”

Meet and confer: “Prior to the initial status conference with the court, counsel shall meet and discuss the application of the discovery process.”

Some of the principles apply more closely to the IT teams at defendant or plaintiff organizations. For example, the completeness requirements for the preservation, search, identification, and production of electronically stored information (ESI).

The program – now in its second phase – has brought together dozens of lawyers, judges and non-legal types, including vendor experts, to develop a set of principles that offer guidance on streamlining the discovery process.

“Lawyers need to have an understanding that everyone is not trying to hide the ball,” Holderman says. “I said the problem is you don't trust each other. What we need to do is develop a system where you can still not trust each other, but you can trust that the system is not going to be able to be manipulated.”

Many of the principles apply more closely to the IT teams at defendant or plaintiff organizations. For example, the completeness requirements for the preservation, search, identification, and production of ESI.

Participants from the Seventh Circuit states of Indiana, Illinois and Wisconsin have placed these principles into some 300 cases already. Holderman says. Violators face contempt of court charges. Initial polling has shown that in most cases, lawyers have said the guidance does not decrease their ability to zealously represent their client.

Moving discovery in-house

Of course, long before Holderman's pilot project ever got off the ground, there have been enough horror stories for IT departments to take note of the risks that come with an inadequate information management and governance program.

E-discovery is a major component of such a program. The landmark case of Zubulake v. UBS Warburg should give pause to businesses. In 2002, Laura Zubulake filed a gender discrimination lawsuit against her employer. It wasn't long after that the defendant was unable to produce relevant emails, due to either negligently or willfully destroying the emails or failing to properly preserve them. Ultimately, the case led to a $29.2 million jury verdict for the plaintiff.

Incidents like this have forced many organizations to recognize the importance of proper e-discovery tools, many of which have significantly matured over the past several years, as well as the need to bring these capabilities into their house. In fact, according to Gartner, the global e-discovery market is expected to hit $1.5 billion in 2013.

Yet, according to an August 2010 Symantec study, less than half of enterprises – 46 percent – have a formal information retention plan in place. And often, says Symantec’s Regan, companies are leaving too heavily on shipping out their archived information to discovery services providers. This presents a two-fold problem: high cost and a potential for compromise.

“High cost is never an excuse,” says Patrick Zeller, vice president and deputy general counsel of Guidance Software, a Pasadena, Calif.-based firm that specializes in forensics and e-discovery. “I can go and tell a judge that this is going to cost me a million dollars, but if you keep that data in a format that is difficult to search, that is not an excuse. Judges are going to order you to produce it.”

And instead of relying on third-party vendors, organizations should consider shifting their e-discovery efforts in-house with software specifically designed for proper categorization, discovery and recovery, Regan says.

“If you don’t bring a process in-house with IT and legal folks working together, you’re exposing yourself to a huge amount of risk,” Zeller says. He cites the Washington state Supreme Court’s $8 million judgment against Hyundai Motor Co. for the carmaker’s failure to comply with discovery demands. E-discovery best practices have ancillary benefits as well. Organizations can identify unnecessary records and get a handle on the type of data they have stored in their systems, say experts. These solutions can assist organizations in realizing they are housing unnecessary confidential information – or help them defend against a patent dispute.

E-discovery also can be used to investigate potential breaches. Zeller referenced a Chicago law firm that traced how many times an inadvertently sent email, containing the pay rates of associate attorneys, was forwarded. Last fall, using the Seventh Circuit pilot program, a subcommittee was formed to help judges and committee members get up to speed on the latest in technology.

“It will help client IT and client legal clear up some of the language barriers and come up with standard wording,” says Jennifer Freeman, co-chairwoman of the subcommittee and a senior legal consultant at Kroll Ontrack, a Minneapolis-based legal technology and consulting provider.

The subcommittee also is seeking to define and assess those technologies that could lend greater efficiencies while lowering cost and risk.

Still, Holderman says that despite software created specifically for e-discovery, tools are not available to “get all the needles out of the haystack.”

“The reason is, electronically stored information is not stored for purposes of retrieval in litigation,” he says. “It's stored for purposes of business...”

Zeller says the preponderance of unstructured data, such as metadata – often defined as data about data – that is necessary for litigation is only adding to the complexity.

Ultimately, Holderman says, the goal of the e-discovery pilot program is to improve cooperation among IT and legal teams and increase education and awareness about the need to wrangle in the costly, time-consuming and argumentative nature that often is associated with the preservation, search, identification, assessment and collection of pertinent data related to legal actions.

“We've said it at every meeting,” Holderman says. “I think we need to change the culture of pretrial litigation in the United States. We are going to make pretrial litigation more reasonable and fair now...Ultimately, companies and readers will have more concrete guidelines so they know they can keep stuff and delete stuff without somehow getting sanctioned by a court.”
Residents respect the dollar, but it’s time to start weighing the risks of the next generation of payments, reports Danny Bradbury.

Canadians have a thing about cash...and about what happens when it disappears. However, a cashless society looms large on the horizon, and civil liberties advocates are bemuseing the potential loss of control and privacy. What’s happening, and how will it play out?

Various projects are afoot to eliminate filthy lucre from the equation. For most big-ticket transactions, of course, credit cards and bank transfers have replaced banknotes for bytes. But those smaller transactions, under $25, have been tough nuts to crack.

The credit card companies have been busy solving that problem. Both Visa and MasterCard have developed systems that use RFID cards. Simply tapping the card against a reader in a suitably equipped point-of-sale system deducts the money from an account without any actual cash being exchanged.

For some, an obvious worry here is that losing the card is not just like losing cash. It’s like losing a debit card with the PIN number written on the back, because purchases don’t require any authentication other than tapping the card. MasterCard’s response, highlighted in its security briefing document for PayPass, the company’s new “contactless” system, is much more interested in smartphone-based, near-field communications technology. Or, as she prefers to call it, “Tap ‘N’ Go” (TNG). “Once you have TNG, that will be the sexy app,” she says.

Google, a company with which Canada’s privacy commissioner has had past run-ins. The tech giant hopes to revolutionize cash transactions with its Google Wallet service. Designed to work with its Android phones, the service essentially embeds the MasterCard PayPass functionality into an RFID-enabled handset. Customers tap the phone against a reader, just as they would normally tap a PayPass card, to pay for an item.

Other cashless systems have developed too. Square, which began life as a mechanism for taking credit card payments with a mobile phone, has since launched a mobile app designed for customers to work with participating merchants. Once a customer has used a credit card with a vendor, he can send a text message to the customer’s iPhone with a link to a downloadable app that then lets them pay virtually through their phone.

From a customer’s perspective, Square is similar to Venmo, a mobile service that lets users link their credit or debit card to their phone number. Customers can then use their Venmo account to exchange money, settling small debts. And, of course, there’s PayPal, which is currently suing Google, claiming that the search baron stole trade secrets when two PayPal employees moved to Google to head up the company’s Wallet initiative. The firm’s president has already predicted that wallets will be defunct by 2015.

“PayPal is positioning itself to become a ubiquitous digital wallet,” says Darrell MacMullin, managing director for PayPal Canada. “If I am the consumer and I play with my Android phone and whatever funding method, and the transaction doesn’t go through, then who do I call? Who is liable and who is protecting the consumer?” On the other hand, PayPal protects buyers and sellers with its established policies, he says.

“There are a lot of background checks that we are doing,” says MacMullin. “We are protecting the customers foremost.” But therein lies the problem. Who polices these new virtual cash companies as they become more widespread? PayPal’s customer base is littered with unhappy users who complain about frozen accounts and other transgressions. With more than 100 million accounts, however, and with a million new accounts every quarter, MacMullin admits that there can be problems.

And what of Google, which was at the sharp end of an investigation by federal privacy commissioner Jennifer Stoddart last October, when it was found to have collected personal communications and network details from Canadian users while gathering data and pictures for Google Maps?

“Google made mistakes, but they understand the question and the strength of privacy, especially when it comes to control,” Cavoukian says. She points to the simplified privacy policy in the firm’s new Google+ social network as an example of how it has changed its ways. “After Buzz, they got the mistakes that they made, and they had to ensure that the designers and code writers themselves had privacy on their radar.”

PayPal, meanwhile, has to hold itself to practices that are higher than nationally-set regulations. “If we relied only on money-laundering standards to manage our business, our fraud rates would go through the roof,” MacMullin says.

He argues that users are verified when they log into their accounts, and transactions are also monitored for suspicious activity. “And we are also monitoring at the network level,” he says. “We are monitoring all of these simultaneously. We do it in a more sophisticated way than simply adhering to regulatory standards.”

For its part, Google outlines specific security and privacy protections as part of its Wallet offering. It does not receive data about which products users purchase, but does record data about transaction amounts and credits used, which are stored locally on the phone. Users can also enable location recording at the time of purchase. In addition, the system uses something akin to a trusted platform module in the Android Nexus handset that supports Wallet. This is supposed to restrict access to Wallet data.

Ultimately, though, most users probably won’t look at the issue of security and privacy much when faced with the dazzling array of features that goes along with Wallet. Google is working to include Offers (its version of the Groupon daily deals service) in Wallet, and will also allow partners to integrate loyalty cards into the system. The result will be a phone that becomes increasingly indispensable, some predict. Like many of the newer systems, Google Wallet is not yet available in Canada, but it is only a matter of time.

Technology always involves a trade-off between convenience and security. If history is any guide, convenience generally wins. The leverage that Google will have with integrated cashless payments will make the outcome pretty certain. Cash is unlikely to be king for much longer – and if anything goes wrong, Canadians may have to live with the consequences.
For many companies that process credit card data, the requirements of the Payment Card Industry Data Security Standard (PCI DSS) are all too familiar. But should companies that do not process credit cards implement the same data security restrictions?

Today there is a veritable alphabet soup of data security standards to which companies can adhere, but because of its prescriptive nature, PCI DSS seems to be catching on as a viable option for companies that do not take credit cards, experts agree. For example, rather than simply stating that a firewall for web applications needs to be in place, PCI DSS describes in detail exactly what is required and how to configure it.

PCI DSS is primarily a contractual agreement between the major credit card companies and enterprises that accept and process credit cards. The standard, defined by the Payment Card Industry Security Standards Council, was put in place as a means of ensuring that personally identifiable information (PII) is protected.

However, some experts argue that PCI should be adopted as a best practice by those not required to comply with the standard. “PCI DSS requires you to continue to monitor [your network],” says Deven Bhatt, CISO in the Washington, DC office of Wright Express, a provider of payment processing and information management services. “It’s not a project with a start and end date.”

Unlike other standards mandating technology usage – such as ISO 27001, which oftentimes uses vague language, such as “appropriate” – PCI DSS is far more specific and not open to “user interpretation,” Bhatt says. Even small or midsize companies that do not process credit cards should consider implementing PCI DSS, he says, because “even small companies have PII.”

Ensuring compliance with the standard can be done in two ways. A qualified security assessor (QSA), who has been certified by the PCI Council as being qualified to assess compliance to PCI DSS, can inspect a company and either certify or deny it. For smaller companies, self-certification is an option. For this, a checklist is used to ensure that all of the key components of the standard have been implemented.

However, Frank Kenisky, a San Antonio-based data security consultant and a former CISO, cautions that a self-analysis is sometimes inadequate. Checklist-based analysis of security is not appropriate for an ongoing process, such as protecting corporate data, he says. A checklist might provide basic information, but it does not take into consideration wider-ranging issues about protecting data, including ensuring that the auditing of the security system is done separately from the team that is responsible for the data security itself. “The checklist mentality treats a business like a board game,” he says.

But, steps must be taken to ensure data is protected. Jeff Hall, a director at consultancy RSM McGladrey, says companies should consider PCI DSS as a viable data security foundation, regardless of the kind of data they are protecting. Instead of thinking of cardholder data, just substitute PII or other company-confidential information, he says, adding that virtually every company has some type of confidential assets, be it human resources, financial trade secrets or a myriad of other data sets, such as Social Security or driver’s license numbers.

Much of today’s data is attainable on the web, he says. “We make everything so searchable, [even] cretins can search for anything.”

Among the information often searched for by ill-intentioned people is personal and company-confidential data, he says. “Competitive information and intellectual property (IP) are as important as PII.” In some companies, he says, IP is siphoned off the server by thieves as soon as it gets there.

Companies of all sizes need to make better decisions about who has access to data, Hall says. If companies make information too accessible or keep PII on servers when it should be archived or destroyed, then they are taking a much greater risk than necessary. Just because a company can do something – like keep data accessible on networked servers – it doesn’t mean it should, Hall says.

But, when it comes to implementing precautions, such as those outlined in PCI DSS, many companies balk because they fear the added costs. “It costs a fortune to get the [appropriate] infrastructure in place,” he says.

Open to breach
In addition to aging hardware, some companies are still using older data security practices that can be breached easily. Even the cloud infrastructure of Amazon S3 – the online shopping giant’s storage web service – had a backdoor that was breached, Hall says. It was fixed soon after.

Experts agree that implementing a proper risk management plan can help organizations better understand IT security priorities. But, at the same time, tighter budgets are forcing CISOs to squeeze more efficiencies out of a company’s security infrastructure. By basing IT security plans on standards like those from the PCI Council, CISOs can go a long way in building a stable foundation for a strong security posture that also accounts for still lingering, industry-wide belt-tightening, says experts.

Hall is a big supporter of standards in general and PCI in particular. “The PCI standards were not developed in a vacuum,” he says in a post on his blog PC7 Guru. “They are a consolidation of a lot of other security standards and guidance gained through root cause analysis of security incidents gathered over the years with the express purpose of protecting cardholder data.”

Shawn Chaput, chief architect and executive consultant at Privity Systems, a Vancouver, BC-based management consulting company, agrees that PCI DSS can help companies protect noncredit card data. Companies that are involved in or considering mergers and acquisitions, as well as those with intellectual property or confidential sales leads and human resource data, should consider protecting their information with more than just minimal data security techniques, he says.

But for some, implementing the PCI standard will provide only a minimal data security framework. Some companies should consider more stringent security measures if their risk assessment indicates greater security is required, experts say.

PCI DSS is not open to user interpretation.”

- Deven Bhatt, CISO, Wright Express

SOMETHING BORROWED

PCI DSS can benefit even those companies not processing credit card transactions, reports Stephen Lawton.

For many companies that process credit card data, the requirements of the Payment Card Industry Data Security Standard (PCI DSS) are all too familiar. But should companies that do not process credit cards implement the same data security restrictions?

Today there is a veritable alphabet soup of data security standards to which companies can adhere, but because of its prescriptive nature, PCI DSS seems to be catching on as a viable option for companies that do not take credit cards, experts agree. For example, rather than simply stating that a firewall for web applications needs to be in place, PCI DSS describes in detail exactly what is required and how to configure it.

PCI DSS is primarily a contractual agreement between the major credit card companies and enterprises that accept and process credit cards. The standard, defined by the Payment Card Industry Security Standards Council, was put in place as a means of ensuring that personally identifiable information (PII) is protected.

However, some experts argue that PCI should be adopted as a best practice by those not required to comply with the standard. “PCI DSS requires you to continue to monitor [your network],” says Deven Bhatt, CISO in the Washington, DC office of Wright Express, a provider of payment processing and information management services. “It’s not a project with a start and end date.”

Unlike other standards mandating technology usage – such as ISO 27001, which oftentimes uses vague language, such as “appropriate” – PCI DSS is far more specific and not open to “user interpretation,” Bhatt says. Even small or midsize companies that do not process credit cards should consider implementing PCI DSS, he says, because “even small companies have PII.”

Ensuring compliance with the standard can be done in two ways. A qualified security assessor (QSA), who has been certified by the PCI Council as being qualified to assess compliance to PCI DSS, can inspect a company and either certify or deny it. For smaller companies, self-certification is an option. For this, a checklist is used to ensure that all of the key components of the standard have been implemented.

However, Frank Kenisky, a San Antonio-based data security consultant and a former CISO, cautions that a self-analysis is sometimes inadequate. Checklist-based analysis of security is not appropriate for an ongoing process, such as protecting corporate data, he says. A checklist might provide basic information, but it does not take into consideration wider-ranging issues about protecting data, including ensuring that the auditing of the security system is done separately from the team that is responsible for the data security itself. “The checklist mentality treats a business like a board game,” he says.

But, steps must be taken to ensure data is protected. Jeff Hall, a director at consultancy RSM McGladrey, says companies should consider PCI DSS as a viable data security foundation, regardless of the kind of data they are protecting. Instead of thinking of cardholder data, just substitute PII or other company-confidential information, he says, adding that virtually every company has some type of confidential assets, be it human resources, financial trade secrets or a myriad of other data sets, such as Social Security or driver’s license numbers.

Much of today’s data is attainable on the web, he says. “We make everything so searchable, [even] cretins can search for anything.”

Among the information often searched for by ill-intentioned people is personal and company-confidential data, he says. “Competitive information and intellectual property (IP) are as important as PII.” In some companies, he says, IP is siphoned off the server by thieves as soon as it gets there.

Companies of all sizes need to make better decisions about who has access to data, Hall says. If companies make information too accessible or keep PII on servers when it should be archived or destroyed, then they are taking a much greater risk than necessary. Just because a company can do something – like keep data accessible on networked servers – it doesn’t mean it should, Hall says.

But, when it comes to implementing precautions, such as those outlined in PCI DSS, many companies balk because they fear the added costs. “It costs a fortune to get the [appropriate] infrastructure in place,” he says.

Open to breach
In addition to aging hardware, some companies are still using older data security practices that can be breached easily. Even the cloud infrastructure of Amazon S3 – the online shopping giant’s storage web service – had a backdoor that was breached, Hall says. It was fixed soon after.

Experts agree that implementing a proper risk management plan can help organizations better understand IT security priorities. But, at the same time, tighter budgets are forcing CISOs to squeeze more efficiencies out of a company’s security infrastructure. By basing IT security plans on standards like those from the PCI Council, CISOs can go a long way in building a stable foundation for a strong security posture that also accounts for still lingering, industry-wide belt-tightening, says experts.

Hall is a big supporter of standards in general and PCI in particular. “The PCI standards were not developed in a vacuum,” he says in a post on his blog PC7 Guru. “They are a consolidation of a lot of other security standards and guidance gained through root cause analysis of security incidents gathered over the years with the express purpose of protecting cardholder data.”

Shawn Chaput, chief architect and executive consultant at Privity Systems, a Vancouver, BC-based management consulting company, agrees that PCI DSS can help companies protect noncredit card data. Companies that are involved in or considering mergers and acquisitions, as well as those with intellectual property or confidential sales leads and human resource data, should consider protecting their information with more than just minimal data security techniques, he says.

But for some, implementing the PCI standard will provide only a minimal data security framework. Some companies should consider more stringent security measures if their risk assessment indicates greater security is required, experts say.
For companies not required to implement PCI DSS, its encryption portion might be one area where savings can be realized, Chaput says. Although, he admits, encryption can be expensive, so many companies, especially smaller ones, might pass on it.

However, there are other advantages to compliance. Companies that provide services to enterprises that fall under PCI DSS requirements might well pass on it. Many companies, especially smaller ones, admit, encryption can be expensive, so might be one area where savings can be realized, Chaput says. Although, he knows of a Canadian company that does processing for a large bank, but does not handle any credit card data, has implemented the PCI standard for its own company. Although it is not required to do so, the company now markets itself as a PCI-compliant data processor for banks, hoping that its adherence to the standard will build its business by attracting companies that need to comply but also prescribe how to do it or do not have the budget. PCI DSS provides them with a roadmap to effective and industry-accepted security procedures that will improve their data security, Chaput says.

Selling the value
The challenge for small and midsize businesses is that many do not necessarily understand what needs to be done to be compliant, they do not know how to implement what they do know and they do not have the IT and security budgets to do the job effectively and efficiently. As well, data security is hardly a stagnant process, but rather a process that is constantly in flux, depending on the whims and cleverness of those trying to steal what a company possesses.

Security best practices from just a few years ago are today becoming mandated by law or part of standards, says Greg Bell, global information protection and security lead partner at KPMG in Atlanta. Companies that are required by their contractual agreement to employ PCI DSS have tools to do so, but those that are not required to comply have a proactive framework for data security that can enhance their business operations.

Although PCI is designed to protect specific types of credit card data across global networks, the same policies and procedures can safeguard employee, customer or supply chain information, intellectual property or medical records just as efficiently for companies that do not use credit cards, Bell says.

“Most mature organizations have a foundation of blocking and tackling in place [for data security],” he says. The piece that is often missing is a formation of action that explains who does what when a breach or other data loss occurs.

That, he says, is the chief benefit of the PCI standard.

As companies try to do more with less – such as fewer staff members doing more work across multiple disciplines – many are starting to migrate to more prescriptive security measures. There is no one-size-fits-all for data security, Bell says. One has to build a foundation appropriate for each company.

From the inside
Bell recommends that companies considering using PCI DSS understand their risks and the various vectors from which the risks might arise. Not all risk is due to criminals and hackers, he says. In some cases, the threat could come from employees, partners or perhaps even something as innocent as a reconfigured server. “Risks are changing faster than the standards,” he says.

So where does that leave an enterprise wanting to adopt some PCI edicts? Emily Mossburg, a principal in the security and privacy practice of Deloitte & Touche, says smaller companies that don’t have full-time data security staffs still can benefit from taking advantage of PCI DSS. Mossburg recommends that all companies employ at least some minimal aspects of the standards. For example, she says it is important to install and maintain a firewall configuration that protects confidential information while blocking attacks from the web. Not all data needs to be on the company’s primary network, she says. A segmented network can be used to protect PII and IP. Access control lists also can secure corporate data. While acknowledging the value of the standard, she says companies should consider the kinds of data they transmit before committing to an expensive data encryption program.

“The standards.”

– Greg Bell, partner, KPMG

Let’s face the facts. You’ve been so dedicated all year. Now it’s time to get the recognition you deserve! We are accepting nominations for the 2012 SC Awards U.S.

Nominations deadline: Aug. 26, 2011
Nominate your products, team members and company today, and come next February you could be taking home the most coveted trophy in information security.

Save the date Tuesday, Feb. 28, 2012
2012 SC Awards U.S. Dinner and Presentation

Visit scmagazineus.com/awards to download your entry kit today.
Countless organizations have built their own situation rooms to protect data and respond to threats. Angela Moscaritolo reports.

From personnel files and student grades to accounts receivable data and cutting-edge research, Virginia Tech University maintains enormous amounts of sensitive information. So it is no wonder that its networks are probed hundreds of thousands of times every day.

Adequately protecting such a complex campus network infrastructure, made up of more 30,000 computing and communication systems across 125 buildings, requires a host of layered defenses, says Randy Marchany, the university’s information security officer, who leads a team of four full-time security analysts in addition to several graduate students.

Marchany and his group have been collecting security-related information from various sources — such as operating system logs, intrusion detection and prevention systems, firewalls and vulnerability scanners — for a number of years. But with such vast amounts of security data being regularly generated and stored on separate, distributed servers, it became too difficult to see the big picture, he says.

So, about two years ago, the team embarked on a project to build a cybersecurity operations center (SOC) to collect, correlate and analyze the data and leverage it to more quickly respond to threats.

Countless organizations have built SOCs for similar reasons. These centers serve to pull together threat and log data from sources, and centralize security monitoring, analysis and response functions within a single unit. In addition, these centers usually provide around-the-clock monitoring and risk management to detect and protect against attacks.

These days, the most state-of-the-art SOCs look like something right out of the movies, says Chris Triolo, vice president of Enterprise Solutions at HP ArcSight, which offers SOC consulting services.

A hardened facility, he says, where an overhead grid of large, flat-screen displays depict real-time attack traffic. Rows of security analysts, each sitting behind multiple computer monitors, watch for trends and anomalies. Other, less elaborate SOCs, meanwhile, may be housed inside a small 10-by-10 room and staffed just two employees.

While each SOC is unique, its main functions often include security event generation, collection, storage, analysis and reaction, according to “Security Operation Center Concepts and Implementation,” a paper written by French computer and network security expert Renaud Bidol, which the Virginia Tech team used as a blueprint.

Electronic Warfare Operations Centers to address threats, such as radio-signal jamming. These centers later evolved to manage the threats introduced by newly deployed networks. Hence, the first modern SOCs were born.

By the late 90s, large, cutting-edge organizations caught wind of the concept and began developing their own SOCs. The model gained widespread support among enterprise IT teams in the early 2000s, driven by an increase in online risks and information regulations.

Counteracting the most advanced threats — such as those using zero-day malware to perpetrate stealthy and often undetectable attacks against a target with the goal of siphoning off valuable information — will likely require organizations to evolve their SOCs in the future, according to experts at RSA, which introduced the concept of an “intelligent” SOC in a paper released in February. (RSA itself was the victim of an advanced persistent threat attack.) As part of this transition, organizations may need to develop new models for mapping risks, attack vectors and threats, the paper said.

The intelligent SOCs of the future may rely on what are now just experimental technologies and theoretical approaches, such as self-learning solutions that continuously monitor an environment to quickly spot anomalous behaviors, researchers say. The most advanced centers may even go a step further, leveraging theoretical, risk-based decision systems to detect unusual conditions and take action on their own to investigate and ultimately mitigate the threat.

While security practitioners wait for these advanced technologies to be developed, there are some key principles of intelligent SOCs that can be adopted today and don’t require the purchase of costly equipment, only a change in focus and behavior.

It is impossible to respond to every threat, so understanding which organizational assets are most valuable and where they reside is important, RSA’s Curry says. By adopting an information-centric approach to risk planning, security teams can selectively mitigate attacks, focusing on protecting what is most important, instead of trying to patch every vulnerability and respond to every attack.

“I sit through presentations from companies and they say, ‘We have 3,400 machines that feed into the SOC,’ and I say, ‘So how much information are you protecting and how many critical systems do you have?’” Curry says.

Security pros should also begin detailing some time to attack-modeling activities to determine potential threat vectors and examine defensive steps to quickly isolate them. By modeling potential attacks, practitioners can be ready with a plan.

Outsourcing the work to managed security services providers is another option, Tridosi of HP ArcSight says.
Identity standards

For years, the notion of federating identities into a single secure identity “ecosystem” to work across multiple applications and entities seemed to gain little traction. That is, until recently, when cloud computing and mobility started placing new demands on access that only a federation could solve.

The reality is, identity federations of hundreds of thousands to millions of business-to-business (b2b) entities are flourishing in the automotive, aerospace, pharmaceutical, government and other sectors. Now, vendors, service providers and enterprises are adopting standards to support single sign-on (SSO) authentication for cloud and mobile access. Meanwhile, Facebook, Google and other social networking giants are poised to become one-stop identity providers for the masses.

“Federation is alive, well and thriving,” says Mark DiDato, research vice president at Gartner. “Most organizations are using federation internally, to connect partners and to connect disparate security and access systems during mergers and acquisitions. Now, federated identity is about SSO and provisioning to resources in the cloud.”

That is not to say that federation is going to be a walk in the park. Standards – responsible for growing adoption of identity federations – are numerous and confusing, experts say. Yet, to comprehendively prepare for federation, enterprises, cloud service providers, as well as identity services and access management vendors, will all have to consider multiple standards based on their – and their users’ – access models.

Another issue is vetting the identities, which brings into question legal issues around privacy, liability and allocation of risk, says Jeremy Grant, program director of the National Strategy for Trusted Identities in Cyberspace (NSTIC), a public-private sector initiative that debuted in April. The agency is charged with creating a trusted, online ecosystem that would designate a single credential to users as a one-time digital password – e.g., software for mobile devices, a smart card or token – to foster secure transactions on the internet.

“There are very large federations out there specific to sectors within the government and in vertical industries,” Grant says, pointing to SAFE BioPharma (a standard used by organizations to verify and manage digital identities), CertiPath (which manages a huge identity federation for the aerospace industry), and InCommon Federation (which supports more than 200 research universities). “The issue is getting identity federation to the next level, which requires a new wave of authentication technologies and rules to govern them that can work in a highly mobile, portable world where smart cards and tokens may not always be the answer.

For example, he cites phone authentication, which can be used as a third factor for one-time tokens via text message. In addition, the phone itself can be used as the additional factor.

Enterprise federations

These, and multiple other SSO and authentication technologies, are enabled by federation, say experts. However, depending on their use, federated networks come in many different flavors, all of which are impacted by what analysts call an alphabet soup of standards. Confusion over these standards has, so far, held up widespread adoption of federation, says Eve Maler, principal analyst with Forrester Research.

She estimates that large-enterprise adoption of federation for business process outsourcing, such as access to human resources web apps, is higher, although there is no formal data available. She adds that adoption will really take off now that the Security Assertion Markup Language, or SAML, became a standard once Microsoft adopted it for its Active Directory Federation Services (AD FS) 2.0, released in mid-2010.

“All vendors, services and enterprises need to get onboard with SAML if they want to federate identities,” says André Gold, senior director of technology and Identity Federation, says Eve Maler, principal analyst with Forrester Research.

“Managing your identities, your PKI certificates, assertions and authentication is complicated in this ever-changing identity federation landscape,” says Dave Miller, CSO of Covintis, which supports nine million users of OnStar, linking vehicle drivers with remote services. “This is why analysts see a growing service industry around identities: These services handle the hard work of standardization and identity management for them.”

American Hospital Association (AHA), based in Chicago, is one company which turned to an identity service after federating the first five of 16 widely used software-as-a-service (SaaS) applications for the cloud. Some of the service applications they are federating include social intranet and collaboration provider Socialtext, document management and collaboration provider Box.net, IT self-service management provider Numara FootPrints, and HR payroll/time entry service UltiPro.

“In one example, we had our own custom SAML adoption for one of our performance management tools, but that tool vendor kept changing the way its login works around the exchanging of public and private encryption keys, and our links kept getting broken,” says Karthik Chakkarapani, the AHA’s IT director of technology solutions & operations. “We didn’t want to do this with 16 applications. And we didn’t want to write our own code to enable the single sign-on to all these applications either.”

Federating to mobility

Synovus Bank, with 30 banks on the East Coast, didn’t want to manage the identities of its approximately 100,000 commercial and 200,000 home-based customers. It also wanted its identity management to occur outside its firewall. So Synovus recently started using Crosscheck Network’s Forum Sentry XML Gateway service between these users and their applications.

“Users and their sessions authenticate on the Forum structure, their SAML assertions are signed by Forum, and Forum also issues their secure tokens,” says Santosh Kokate, head technical analyst with Synovus. “The beauty is I have online banking sitting safely behind the identity gateway and the identities and authentication are established there. I don’t have to manage those identities or write a single line of code to make federation happen.”

Synovus also supports authentication for mobile users through REST (Representational State Transfer), which supports HTTP-based assertions for when Kokate estimates are 8,000 mobile banking customers at this point (and more planned in the future). Because Synovus’ intermediary, Crosscheck, supports these and other standards, Synovus can adapt to different types of identity federation requirements as needed.

In “Architecting a Cloud-Scale Identity Fabric,” a report to IEEE, the world’s largest professional association dedicated to advancing technological innovation, Eric Olden, the founder, CEO and chairman of Simplified, dis-
Identity standards

LEGALITIES: What is required?

The American Bar Association’s Identity Management Legal Task Force is trying to sort out legal and privacy issues surrounding identity attributes and trust. In January, after a series of regional and national meetings, the ABA released version two of its Trust Framework for federated identity networks. The framework describes operational and legal requirements for building trust into these systems, including the use of specifications, standards and rules of operation and enforcement.

and for all their clouds – not just our Box cloud,” Barreto says. “To enable SSO use with multiple clouds, we need to support multiple standards, including legacy SSO standards, current SAML standards and new standards as required.”

Federating to the consumer

In consumer-to-business federation networks, such sites as Facebook, Google and other popular social networks are embracing OpenID and other lighter, more open standards so they can become the identity service providers for their own consumers – and all their non-sensitive online applications, Forrester’s Maler says.

Logging in at Facebook, then, would allow users a single click-through to their other applications, so long as those application providers are participating in the federated network and interoperate with the appropriate standards.

While some organizations feel uneasy about using a Facebook or Google account as the primary login for their customers, employees and partners, others are accepting this as the way of the future. For example, the AHA’s Chakkarapani says many of his mobile, part-time and younger workforce want to leverage social networking for conducting all forms of business.

“We need to be able to support all types of access in order to achieve the 100 percent adoption of our system that we’ve achieved,” Chakkarapani says. “Many of our young people will only work in these types of collaborative environments.”

On the other hand, AutoTrader’s Gold says he worries about the risk of using social networks as the primary identification service for employee, partner and, ultimately, consumer access. For example, in May, 100,000 Facebook applications enabled the leak of millions of access tokens to third parties, and there are myriad examples of social networking consumers being phishing of their credentials or letting in malware that gets in the middle of properly authenticating communications.

This is why vetting the identity provider is important for organizations considering outsourcing their identity management, says NTIC’s Grant.

“Vendors and service providers are picking up the basics of identity now, doing provisioning and directory services management,” says Grant, whose program has been slotted to receive $18 million to support identity pilot programs in 2012. “But the tools for governance and compliance aren’t there yet.”

At the end of the day, it doesn’t matter what the standard is, just as long as it is managed. If a system is working for the businesses and consumers, says Patrick Harding, CTO of Ping Identity, an identity security firm, “A CTO doesn’t care what standards are involved or if it is federated or not,” he says. “CTO’s don’t want lots of passwords everywhere, and they want to seamlessly access all of their applications regardless of where they’re accessing from or where their applications are hosted.”

—Peter Stephenson, technology editor

Endpoints, endpoints... everywhere

This month, it is all about two types of endpoints, one of which is becoming increasingly troubling to security pros.

The easy one – the one with enough of a history to be more or less mature – is the traditional endpoint. This includes such things as desktop computers. The not-so-easy one is the portable device. These little hearts – smartphones and tablets, for example – are proliferating like weeds, and security pros are scrambling to control them.

These devices actually cause more headaches than in the old days when desktop computers were popping up everywhere.

Arguably the biggest problem is data leakage. When devices that cannot be controlled by the enterprise start collecting email, downloading files and connecting to enterprise resources, data leakage prevention challenges cannot be far behind. Those issues are exactly what our portable device section is all about this month.

The good news is that all endpoints – whether desktop or mobile – can be managed because they virtually always are owned by the organization. The endpoint security tools that we look at provide the means to achieve and manage that control.

The bottom line, though, is that these devices, whether they be laptops or smartphones, are becoming increasingly threatening to the security of the information at the enterprise. While they may be misused on purpose, most often they are used by responsible, well-meaning employees to do things in the course of their normal workday. Because we are an increasingly mobile society and because we suffer increasingly heavy workloads, we gravitate toward tools that allow us to have the best of all worlds, and these devices fill that bill.

So, this month, SC Lab Manager Mike Stephenson will take you through the cream of the portable device crop, while reviewer Nathan Oualline navigates the minefields of endpoint security. Between them, you’ll sure get a picture that the sky is not really falling. Instead, there are solutions to the dilemmas we face, even as progress makes surety even more challenging.

—Dave Miller, CSO of Covisint

How we test and score the products

Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a pre-determined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 (or up to 97 on rare occasions) individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University.

We developed the second set of standards specifically for the group test under test and use the Common Criteria (ISO 15484) as a basis for the test plan. Group Test reviewers focus on operational characteristics and are considered at evaluation assurance level (EAL) 2 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

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

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

What the stars mean

Our star ratings indicate how well the product has performed against our test criteria.

★★★★★ Outstanding. An “A” on the product’s report card.
★★★★ Carries out all basic functions very well. A “B” on the product’s report card.
★★★ Carries out all basic functions to a satisfactory level. A “C” on the product’s report card.
★★ Carries out all basic functions to a satisfactory level. A “C” on the product’s report card.
★ Fails to complete certain basic functions. A “D” on the product’s report card.
★ Serious deficiency. An “F” on the product’s report card.

What the recognition means

Best Buy: goes to product with the SC Labs rating of outstanding. Recommended: means the product has shone in a specific area.

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

Whichever the device or wherever the employee, the importance of securing assets that attach to your infrastructure continues to rise, say Nathan Ouellette and Derek Thomas.

**PICK OF THE LITTER**

Check Point Endpoint Security R80 is a modular endpoint security solution that provides flexible and robust protection across many defense-in-depth components. The R80 is our Best Buy.

Sophos Endpoint Security and Data Protection 9.7 is a great value per seat for its many endpoint protection mechanisms. It is worth investigating for any organization looking to add several endpoint technologies to its environment. This is our Recommended product.

**Erratum:** Version and price for the Lightwave product as shown on page 44 of our June issue should be: v4.0.8 with a price of $8,960. Our apologies for the error.

**Whether your company embraces the con-**

- nuerization of IT or your policy states that only organization-managed assets are allowed in the enterprise, protecting the endpoints is probably high on your list. Whichever the device or wherever the employee, the importance of securing assets that attach to your infrastructure continues to rise.

Even if your goals are to incrementally increase the security posture of your endpoints, chances are you’re experiencing all sorts of challenges with regard to making this happen in any sort of expedited manner. With so many security vendors offering varying degrees of encryption, data protection, anti-malware, device control, application whitelisting and other features, you may find yourself looking for one or many endpoint security components based on where you are at with your current product lifecycles. Strategizing on how to cost-effectively implement endpoint security over time can be daunting if you have legacy vendor relationships or if you’re avoiding adding yet another agent.

The good news is convergence keeps moving forward, and licensing models are improving to help reflect the convergence. The more mature enterprise-class vendors seem to have a bit of a headstart, understanding that not every one is going to rush out and replace their current anti-virus or other critical endpoint component they are running today. As the space matures and customers demand more from a unified agent that isn’t terribly bloated, businesses will have an easier time understanding their options and how they can budget and plan for additional endpoint protections.

In this Group Test review, we focus mostly on host-based endpoint security protections. This means that the products had to have some feature to secure a local computer or, at least, secure the impact that any one particular host may have on the environment. Traditional, host-based endpoint security features include anti-virus, firewall, file/folder/disk encryption, application control, protection from local devices (USB, DVD, CD, etc.), web browsing protection, data leakage prevention and other similar technologies. Most products contained one or more of the aforementioned endpoint components. Some contained quite a few features.

Overall, the products that we reviewed in this Group Test reflect the myriad of choices that businesses have in regard to how many features they need and how the solution fits into their environment.

**How we tested**

It is worth noting that all of the products we tested were client/server software applications. We installed the products in either physical or virtual environments based on the products’ various requirements. This included a combination of Windows 2003, Windows 2008, Windows XP, Windows Vista® and various database and web platforms as needed.

As always, the areas we assessed were a combination of features, administration, support offerings, documentation, ease of use, cost and the total value for the money. Every product in this Group Test was installed fairly effortlessly and could be managed through some sort of server-side or web-based console. In many of the technical areas, the solutions scored very similarly. We didn’t encounter any solutions that were difficult to deploy from either a server or client perspective, so, ultimately, the buying decision comes down to cost, features and the overall fit in the environment.

The licensing choices seem to be aligning well with regard to simply unlocking features of the solution with an additional license key. Customers can avoid having to make tougher buying decisions by excluding solutions that offer unneeded components. Whatever the deciding factor may be, there are certainly enough quality choices to warrant a second look or even some long-term planning from organizations that may have tradition-ally shied away from endpoint security altogether.

**Specifications for endpoint security tools**

<table>
<thead>
<tr>
<th>Product</th>
<th>Host IPS</th>
<th>Anti-malware</th>
<th>DLP</th>
<th>Device control</th>
<th>Application control</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit9 Parity Suite</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Check Point Endpoint Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DeviceLock Endpoint DLP</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GFI Endpoint Security</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identity Finder DLP Suite</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lumension Endpoint Management and SecuritySuite</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>McAfee Total Protection for Endpoint</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Novell ZENworks Endpoint Security Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Quarless Protect on Q</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sophos Endpoint and Data Protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SkyRecon Stormshield</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

(✓=yes ○=no)
Bit9 Parity Suite 6

Check Point Endpoint Security R80

DeviceLock Endpoint DLP Suite 7.0

GFI EndPoint Security 4.3

The Bit9 Parity Suite 6 is an endpoint protection solution comprised of a client/server architecture that provides application whitelisting, device control, file integrity monitoring, registry protection and system protection – all within a single agent. The solution is typically installed on Windows computers and the backend is installed on Windows 2003. The solution only uses Bit9’s cloud services for reputation scoring and access to its repository of known hashes for integrity monitoring.

The solution is easy to install. We were up and running within minutes. The Bit9 server console is web-based and fairly easy to navigate. The solution itself is an interesting approach to endpoint protection. Although it does not contain any anti-virus features, the solution itself is a cloud-based reputation scoring to help determine if files and applications are known to be good or if they have been scored as malware by the community.

The heart of the protection and features lies within Bit9’s database of known hashes and reputation scores compiled from various sources, which is then compared to what is installed on local client machines. Reputation scoring includes a specific weighting, which indicates whether the files in question have passed anti-virus checks from at least six vendors. In addition to these features, the solution also performs integrity monitoring and device access control. Security and permissions are granted through various levels of protection, known as SecCon. These levels are based on whether the agent will monitor, block and ask, lock down completely or employ other throttling techniques based on roles or groups of users. Overall, the solution was easy to use and integrates nicely with Active Directory.

Documentation is solid and can be accessed directly from the web-based administrative interface. The solution offers eight-hour-a-day/five-days-a-week phone support, and email support is available 24/7. The product is updated every year. The Bit9 server also provides various types of endpoint security protection.

The method is deployed through a single back-end architecture based on Windows server devices and a database. The solution overall is very modular, and organizations can unlock whichever modules are needed. The available types of protection are abundant and all of them are managed via a single unified agent. The various components include full disk encryption, encryption of removable devices, firewall, antivirus/application control, web browsing protection and remote access VPN.

The features and capabilities across each module are robust, and policies for each are managed through a single administrative interface. The backend architecture is easy to use, and we installed the solution quickly. For example, a separate program is included for packaging agent distributions, as well as a separate executable for developing reports. Overall, this isn’t too cumbersome, as the solution is pieced together very well through an easy-to-use interface.

Documentation is excellent and is available in PDF files or right within the console itself. Standard nine-hours-a-day/five-days-a-week support is included with annual subscription costs. We noted that the solution price point scales very well with the inclusion of more or all of the features.

DeviceLock is a data and device protection solution which controls access to local Windows devices and watches input/output channels for sensitive data flow. The solution integrates with Active Directory and is managed by a Microsoft Management Console (MMC) snap-in. Both the endpoint agents and the server integration are installed on common Windows platforms, and Microsoft SQL Server is used as the repository. Deploying the product is quick and easy. Administrators familiar with Windows-based MMC consoles will appreciate the integration, as all administrative tasks are organized in the familiar MMC display. The user interface isn’t flashy or the most polished we’ve seen, but all the common tasks designed for this solution are easy to navigate.

The product overall serves two purposes: to control local access on the endpoints to ports and devices, and to watch for sensitive data flow through regular expressions and pattern matching. Together these two core principles serve as a device and data leakage layer of protection. The console has templates for the most common devices, and policies are deployed using an inherited Group Policy Objects based on how the admin wants to control user access to removable media, CD/DVD drives, network adapters and more.

Although the documentation was acceptable in most categories, some of the content felt outdated. Standard support is bundled into the purchase and includes 24/7 web and email help. Phone support is only available nine-hours-a-day/five-days-a-week in the United States. However, there are plans to integrate 24/7 phone support later in 2011.

The product overall is very simple. One thing to note is that the solution targets a specific area of endpoint security: access to devices. Since the intent of the solution is focused on a single component of endpoint security, both the backend server and the client computing requirements can be easily met by even the smallest organization. The agent footprint is extremely small, and the solution works well for what it is intended. Ultimately, admins are able to apply granular permissions against Active Directory groups, organization units and users with regard to what kind of access they have to their local devices.

DeviceLock includes any peripheral that can be attached to a computer, USB ports, modems, DVD/CD drives, storage, network adapters and more. Admins can allow or restrict access easily based on existing permission groups or by creating their own. Deploying agents to hundreds of devices at once is very easy and can be accomplished in a short amount of time.

Overall, the product is aimed at organizations that are looking to replace their current anti-virus, client firewall or other protection mechanisms, but may be looking to add a reasonably priced solution for additional device control. The only anomaly we found is that events and audit trails are written to the Windows event log, and enhanced reporting features are not available in the core product. However, a Report Pack add-on is available. Documentation is adequate and supplies most of the information needed to deploy and manage the solution.
Identity Finder DLP Suite 5

Identity Finder Endpoint Management and Security Suite 7.1

McAfee Total Protection for Endpoint – Enterprise Edition

Novell ZENworks Endpoint Security Management 11

**GROUP TEST | Endpoint security**
Quaresso Protect on Q v2.4

SkyRecon StormShield 5.7

S

Sophos Endpoint Security and Data Protection 9.7

For organizations looking to replace traditional host-based security defenses, such as anti-virus and fire-wall, and bolt on encryption, device control, host intrusion prevention and other features, StormShield is definitely worth a look. The endpoint agent also can help to move several common Windows-based protections into the agent, such as managing wireless access. For administrators looking for yet another level of control over hosts, the scripting feature of the solution will be useful.

Documentation should provide all the necessary information to get up and running, but there is a lot to take in given the number of features. Documentation is available in PDF format or as a manual from the console itself. 24/7 phone, email and web support is available at an additional cost of 18 percent of the license fee. Additional levels of support are available.

Defend networks and data. Advance your career.

Every year, data breaches cost companies millions of dollars. That’s why it’s easy to know how to manage risks like cyber attacks, accidental damage and more. Get ahead in this fast-growing field with a certificate or master’s degree from University of Maryland University College (UMUC). Our nationally recognized programs make it possible to turn data loss prevention into career gain.

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and DHS
- Master’s program named as a Professional Science Master’s by the Council of Graduate Schools
- Programs offered entirely online
- Finance an interest-free monthly payment plan available

800-888-UMUC • umuc.edu/data
Portable device security

Smartphones and other mobile devices, along with USB drives, have created a burgeoning category that demands new and effective solutions. We’ve got some, says Peter Stephenson.

O f all the issues that bedevil us, this has got to be near the top of the list. Portable devices are a real security challenge, but the worst are the mobile devices, such as smartphones and tablets. And, don’t forget the other types of portable devices, such as USB flash and thumb drives and the like. Let’s start there.

The tales are legion of people copying sensitive data onto a thumb drive, taking it home to work on, and then losing the drive and thus exposing information. There is now a whole category of not-so-high-tech that poses a real threat of data leakage. The answer, of course, is encryption, but that encryption must be integrated so tightly into the device that it cannot easily be undone by a data thief.

We saw a couple of these simple products this month and, while they don’t have the pizzazz of some of the other tools we tested, they are competent and extremely important to our defense in-depth approach to information protection. Coupled with various endpoint security tools that we discuss in the other Group Test, these simple little tools can perform services as important as other, more complicated, security tools. Bottom line: Don’t forget these tools and don’t forget how important they can be.

Now to the big guys, figuratively – and physically – speaking. These are the tools that are intended to secure those troublesome mobile devices. This is a relatively new category. That, of course, largely is because the devices they protect are a relatively new category. But mobile devices are exploding in the marketplace so we need a way to secure them. The key issue here is that these portable devices are much smaller and do not have 100 percent of the capabilities of full-blown computers. That means that they need their own specialized protection tools. The ones that we use for our laptops just don’t do the trick.

As well, there are additional issues that we find with mobile devices that we do not find with traditional computers. For example, the smaller mobile devices are easier to steal or lose than full-size computers or, even, most laptops. While they can do much of what a full computer can do, they cannot do it all and often use applications – “apps” – to perform their functions.

One buys those apps online and, as a vendor once told me, app stores are the most efficient way of distributing malware known today. This is not shrink-wrapped software, folks. One may know absolutely nothing about the developer of an app. In fact, one probably doesn’t, since there are a zillion of them and some are single individuals, not real companies. Starting again with the little tools, select encrypted thumb drives that use solid, proven encryption. Make sure the user can move the thumb drive among computers without doing a full installation of an application on the new computer. The tool should work by itself. By that I mean one plugs it in, and it does what is needed to work in its new environment. As to the mobile device security tools that address smartphones and the like, start by reading as many of the proliferating articles, sample policies and security white papers about what your mobile device policy should look like. Then, evaluate your organization in light of what you’ve learned. The next step is writing a policy that meets both the enterprise needs and the currently emerging best practices. The last step is to find a device or two that can enforce an entire policy, and then test them.

Some things that admins should be looking for are remote wipe, anti-malware protection, an inability for the user to remove protection, the device’s equivalent of whole disk encryption using a standard algorithm, the ability to authenticate to the admin’s enterprise, and compliance with the rest of the enterprise’s security policies.

All of that said, these are pretty tall orders and I expect that we will see dramatic improvement in these products – and the emergence of others – when we revisit this important category next year.

Mike Stephenson contributed to this Group Test.

### Specifications for portable device security tools

<table>
<thead>
<tr>
<th>Product</th>
<th>IronKey Enterprise v2.0.8</th>
<th>Juniper Networks Junos Pulse Mobile Security Suite v2.0</th>
<th>Kingston / BlockMaster DataTraveler 4000-M w/ SafeConsole v4.1</th>
<th>MAD Enterprise Compliance and Security Server v1.1</th>
<th>MXI ACCESS Management Software v4.0/MXI Stealth Key</th>
<th>Sophos Mobile Control v1.0</th>
<th>Trend Micro Mobile Security v5.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart device security</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/no.png" alt="No" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>USB flash drive security</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Supports iOS platform (smart device)</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Supports Android platform (smart device)</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Supports Windows Mobile platform (smart device)</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Linux compatible (USB)</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Windows compatible (USB)</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Mac OS X compatible (USB)</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Remote lock/wipe</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Custom policy server</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>Cloud-based server</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
<tr>
<td>On-site server</td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
<td><img src="https://example.com/yes.png" alt="Yes" /></td>
</tr>
</tbody>
</table>
IronKey Enterprise

Juniper Networks Junos Pulse Mobile Security Suite

Kingston/BlockMaster DataTraveler 4000-M

Mobile Active Defense MECS Server Solution

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★
**GROUP TEST** | Portable device security

---

**Sophos Mobile Control**

- **Vendor**: Sophos
- **Price**: $65 per device (for 500-1,000 devices)
- **Contact**: www.sophos.com

Sophos Mobile Control offers administrators a way to maintain security across many different devices, including Apple iOS, Google Android, and Windows Mobile. This tool allows secure email access, remote locking and wiping, and Windows Mobile. This solution does offer a lot of functionality and granular policy controls. However, some organizations may find this product to include some features that are quite limited.

**Verdict**

- **Weaknesses**
  - No device support for Apple or Android devices.
- **Strengths**
  - Granular policy controls that are easy to deploy.
- **Overall Rating**: ★★★★✩

**MXI ACCESS Enterprise Management Software/MXI Stealth Key M50 16GB**

- **Vendor**: MXI ACCESS
- **Price**: Software: $12-$26 per license depending; Key: $39
- **Contact**: www.mxiseconds.com

MXI ACCESS Enterprise Management Software/MXI Stealth Key M50 16GB was first seen at the MXI Stealth Key during our biometrics review (January 2013) and was impressed with this version of this flash drive. So impressed, in fact, that we continue to use it in the SC Labs. So when we had the opportunity to look at the non-biometric version, we were quite excited. This product offers up a solid combination of functionality and control. The flash drive can be used on its own or in conjunction with the ACCESS Enterprise Management server for added functionality and control. Deployment of the tool can take a couple of paths, but for this review we looked at it with the ACCESS Management Server. The first thing that needs to be installed is the server itself. The server can be installed on any Windows machine and, once up and running, the Stealth Keys can be self-initialized by the users quickly and easily. After all the pieces are installed, all management is done via the ACCESS Enterprise management console.

When used in conjunction with ACCESS Enterprise, these USB-drives can offer a lot of data security. The drive itself is encrypted at the hardware level and can be used on any operating system without the need for special drivers. Documentation included an administrator guide for ACCESS Enterprise, which we found to be well detailed and easy to follow. MXI includes the first year of support with the purchase. Additional support can be purchased as part of an ongoing maintenance agreement. There is also a small support area available on the website, but resources there are quite limited.

With a price ranging from $12-$26 per device license for ACCESS Management, plus around $200 per device for the 16GB USB drive, this tool can become quite expensive for some deployments, but we do find it to be a good value for the money. The Stealth Key can provide solid data protection, while maintaining functionality to the user through its easy-to-use design.

**SC MAGAZINE RATING**

- **Features**: ★★★★★
- **Ease of use**: ★★★★★
- **Performance**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★
- **Value for money**: ★★★★★

**OVERALL RATING**: ★★★★★

**Strengths**

- Easy to deploy and manage, both from the administrator and user sides.
- Full guides and manuals to various client user guides. We found all guides and manuals to be well-organized.

**Weaknesses**

- Limited support area available online.
- Null.

---

Test facilities in the USA, Europe and Asia. Full details of West Coast Labs product testing, certification and performance validation services can be found at www.westcoastlabs.com

---

**Are you considering deploying a security product or service but don’t have the time to trial it for your type of network?**

- **Yes**
- **No**

Do you want to validate a security vendor’s claims to support a purchasing decision for your organization?

- **Yes**
- **No**

Would you benefit from independent technical data that could help you in deciding which security product is right for your organization?

- **Yes**
- **No**

With extensive experience in testing information security technologies, West Coast Labs can do the job for you by building a test environment that replicates your network environment and give you the data to make the right management and purchasing decision.

---
Keeping an eye on the prize

T

here was a day when a private investigator, or “private eye,” just was a detective. Not anymore. Today the term also applies to a neat program that protects a user’s screen from prying eyes, allowing for an occasional forgetful moment, such as when one fails to invoke the screensaver when headed for the coffee machine. Or it shows you the picture of someone behind you if they are shoulder-surfing at, say, an airport lounge. The thing about this PrivateEye, though, is that it is so simple in operation. That, of course, is one of its beauties. Although the tool seems simple on the outside, it is, of course, pretty tricky under the covers. It comes from some research this young – founded in 2007 – company has done for the government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market. Oculis Labs is a small, privately funded start-up that has government market.

PrivateEye is available as an evaluation version on the Oculis website, and we installed it, used it and uninstalled it with absolutely no pain whatsoever. Our impression of PrivateEye is that it is a cool application that also has significant usefulness. All of us – and, certainly, the folks we support and keep secure – get moving through our days and forget to invoke the screensaver. So at that level, this has solid application.

For those of us who travel, it provides a double benefit. Not only does the screen blur if we set the computer down on the airplane seat while we get up for a stretch, it lets us know when someone is a little too curious about what we’re doing. For all of that, it is easy to use and manage. Well worth taking a look at the eval version. – Peter Stephenson

August

Product: PrivateEye
Company: Oculis Labs
Price: Starts at $3,600 for 50 seats, including first year’s support
What it does: Blurs the computer screen unreadable when the authorized user is not in front of it, and notifies the user when someone is shoulder-surfing.
What we like: This is about the coolest and, at the same time, most useful security product we have seen in a long time. It is simple to use, very effective, and actually serves a real and important purpose. What we didn’t like: None that we found.

PrivateEye is available as an evaluation version on the Oculis website, and we installed it, used it and uninstalled it with absolutely no pain whatsoever. Our impression of PrivateEye is that it is a cool application that also has significant usefulness. All of us – and, certainly, the folks we support and keep secure – get moving through our days and forget to invoke the screensaver. So at that level, this has solid application. For those of us who travel, it provides a double benefit. Not only does the screen blur if we set the computer down on the airplane seat while we get up for a stretch, it lets us know when someone is a little too curious about what we’re doing. For all of that, it is easy to use and manage. Well worth taking a look at the eval version. – Peter Stephenson
Will mobile kill user privacy?

The internet is evolving to deliver individualized experiences, but at what cost to privacy, asks Forrester’s Chenxi Wang.

Innovations in mobile technologies are making the mobile internet increasingly ubiquitous and powerful. Consumers are drawn to the mobile internet because it can be highly contextual and leverages information such as geolocation, proximity and user-specific information to deliver a rich and intensely personal experience.

Already the phone is packed with sensors that can gather more contextual data about its surroundings than anything that we’ve seen before. Sensors such as GPS, accelerometers, gyroscopes, near-field communication (NFC), and high-resolution camera and displays are now commonplace with high-end smartphones. Emerging sensor technologies—like barometer, microbolometers and chemical sensors—will provide even richer user contextual information.

As this is happening, your mobile phone will know more about you than perhaps your closest family members. As more and more of your activities will be tied to the device, it will know where you are, what you are doing, and, if Apple gets its way, the rate your heart beats.

Mobile internet enables the mass-scale collection of such user contextual data. Mining of this data gives rise to transformational business opportunities—interests in location-based services have already sparked a new growth market. In fact, it is not too far-fetched to imagine an intensely personalized internet experience unlike any that we’ve seen before.

Soon, the concept of “going to a website” will become obsolete. Our children will no longer need to surf the internet. Rather, personalized content and services will come to them magically via the little device that is known as the mobile phone. The internet as we know it today will transform into a dark place where everyone can be in the business of user data collection and mining. Just as PCI demands rigorous security practices from those who handle consumer credit card data, regulations can demand a similar level of competence from companies that collect and mine user contextual data. Furthermore, regulations may restrict what a business can and cannot do with users’ private contextual data. For instance, it may be perfectly OK to correlate location and time-of-day information, but it will be deemed unacceptable if a third stream of user contextual data is introduced.

Technology may be another key safeguard. Just as homomorphic encryption allows one to aggregate two functions without knowing the original input, new data-mining technologies may allow meaningful statistical results without access to original raw user data.

It is not clear if or when the regulatory or technological safeguards will be in place. Consumers, lured by the shining promises of the mobile internet, may be blind to the privacy risks.

Right now, technologists and firms in the mobile internet market only have a social responsibility to consider user privacy when they craft their next fancy mobile strategy. Are we headed toward a dark place where everyone is perpetually connected, but none can keep anything private?

What do you think?

One must explore the role of regulatory oversight.

Chenxi Wang is VP and principal analyst of security and risk at Forrester Research.
Our business is to protect your business

With industry-leading proactive malware detection, ESET antivirus solutions intercept and eliminate cyber threats before they can infect your business network.

Our award-winning heuristics technology offers aggressive server-to-endpoints malware defense for multiple platforms and virtual environments. All managed from a single console.


To download your free trial, go to www.eset.com/business_trial

ESET NOD32 Antivirus 4
Business Edition

ESET Smart Security 4
Business Edition

ESET Mobile Antivirus
Business Edition

ESET Gateway Security

ESET Mail Security

ESET File Security

© 2011 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.