FEATURES:

**FOUNTAIN OF YOUTH**

Tech-savvy, Generation Y workers can be an advantage in the enterprise, says James Beeson, CISO, GE Capital Americas

**Defensive strategy**
A report from a Canadian nonprofit finds that awareness and cooperation are required to defend against attackers

**Model behavior**
Informing employees about best practices is still crucial to an organization’s data defense
MOBILE MASTERY

Security and flexibility for the BYOD era.

Imagine an enterprise network with smartphones, tablets, mobile PCs – and no compromises. ForeScout delivers real-time visibility and control over mobile computing devices. Users get the freedom, while you protect the network from data loss and malicious threats. Juggle your primary IT problems like a pro! Download the free Gartner BYOD Case Study at forescout.com/byod.
Editorial

Privacy, please

Just think of all the nifty gadgets that have been commoditized over the years. According to some figures, half of the homes in the United States had television sets by 1955. On the more silly-but-fun side, there were crazy decorative doodads that thrived around this time as well. Remember that 1960s-era Roulette Wheel-inspired cigarette dispenser that made an appearance on Mad Men some seasons back?

These days, we have Google Glasses, iPads, JayBird BlueBuds and, oh, so much more. Satisfying the yearnings of generations salivating over the latest, hottest things, the corporate world has been at the ready to make doggone sure it’s creating and marketing just the right goods and services to get a cut of that American dream, its share of the almighty dollar.

Marketers can cull massive bits of data on you and me to make sure we get served up with whatever product-related links our search habits seem to reveal about our spending habits. Our interactions online can prove advantageous to retailers, telecommunications firms or government entities alike.

That’s why bills, like the one introduced last month by Rep. Hank Johnson, D-Ga., that would require mobile application developers to be more forthcoming with privacy policies and data collection practices, are getting more play. Called the Application Privacy, Protection and Security Act of 2013, and nicknamed the Apps Act, it strives to make national protections, already being enforced through the California Online Privacy Protection Act, by making developers, among other things, get consent from customers before collecting their personal and secure stored data.

Yet, moves like these that endeavor to keep citizens’ rights to privacy somewhat unbroken are not enough. It was only in April that we learned from the privacy rights organization EPIC that the U.S. federal government granted legal immunity from wiretapping laws to at least two internet service providers: AT&T and CenturyLink, which allowed them to monitor their internet traffic to share data with the government on cyber threats.

This and other activities are taking place all in the name of protection from possible terrorist and other coordinated cyber attacks. Other countries, of course, engage in such pursuits as well. Just read SCMagazine.com’s recent news on one of Saudi Arabia’s telecommunications companies contacting security and privacy researcher Moxie Marlinspike for help spying on millions of its subscribers. Unsurprisingly, he declined.

If only privacy was the hottest thing since the 1990s-era Sega Game Gear, we’d all be in much better shape. But it seems disclosure of private details will win whatever governmental/regulatory favors are needed to ensure for private companies that their version of the American dream is reached. It’s our shout to let them know we’re not buying.

Illena Armstrong is VP, editorial of SC Magazine.

A Breach Will Eventually Occur!

IS YOUR ENTERPRISE PREPARED?

MAKE ISACA YOUR ORGANIZATIONS BEST DEFENSE AGAINST CYBERATTACKS. LEARN MORE AT isaca.org/cyber.
Rich Baich, chief information security officer, Wals Fago & Co., former principal, security and privacy, Deloitte and Touche
Greg Ball, global information protection and security head, partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Algea
Jaime Chanaga, managing director, CSO Board Consulting
Rufus Connell, research director, information technology, Frost & Sullivan
Dave Cullumine, CEO, Security Stars; former chief information security officer, eBay
Mary Anne Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president, information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Symantec
Gene Fredriksen, chief information security officer, Tycos International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Golden Harbor Consulting
Kris Lowery, vice president of IT risk, office of the CIO, IBM
Tim Mathew, chief information security officer and vice president of security and compliance markets, Splunk, former director, information protection, KPMG
Stephen Northcutt, president, SANS Technology Institute
Randi Sanovich, former general director, information security, General Motors
* Howard Schmidt, partner, Ridge Schmidt Security; former cyber security coordinator, White House
Ariel Silverstone, chief security officer, GNQ; former chief information security officer, Expedia
Justin Somain, former chief information security officer, Yahoo
Craig Spiezio, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
W. Hard Tipton, executive director, (ISC)2; former CIO, U.S. Department of the Interior
Amit Yoran, chief executive officer, NotiFiness; former director, U.S. Department of Homeland Security’s National Cyber Security Division

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

THIS MONTH
SC CONGRESS eSymposium

JUNE 4
eSymposium: IO Management
End-user authentication and access is a key component to keeping sensitive data secure. Not only do such practices and solutions aid to reduce insider threats, but they also help to better safeguard cloud-based applications, critical databases and more.

JUNE 25
eConference: Auditing and compliance
Maintaining compliance with government and industry requirements should go beyond just a tick in the box. Indeed, efforts associated with auditing should be a direct reflection and in support of a corporate IT security program.

NEXT MONTH
JULY 11
eSymposium: Supply chain vulnerabilities
News about supply chain vulnerabilities hit hard late last year when the Penta gon accused some China-based companies of actively embedding backdoors and other malware in the products they sell to companies and government agencies in the United States. We examine these vulnerabilities and offer preventative steps you can implement.

FOR MORE INFO
For details on SC Congress 24/7 events, please contact Anthony Curry at anthony.curry@haymarketmedia.com. For sponsorship opportunities, contact Mike Alesie at mike.alesie@haymarketmedia.com. Or visit www.scmagazine.com/sc-congress-247.

WHO’S WHO AT SC MAGAZINE

EDITORIAL
VP, EDITORIAL: Ilana Armstrong
ilana.armstrong@haymarketmedia.com
EXECUTIVE EDITOR: Dan Kaylan
dan.kaylan@haymarketmedia.com
MANAGING EDITOR: Greg Masters
greg.masters@haymarketmedia.com
DIGITAL CONTENT COORDINATOR: Marcos Colón
marcos.colon@haymarketmedia.com
REPORTER: Danielle Walker
danielle.walker@haymarketmedia.com
TECHNOLOGY EDITOR: Peter Stephenson
peter.stephenson@haymarketmedia.com
SC LAB MANAGER: Mike Stephenson
mike.stephenson@haymarketmedia.com
DIRECTOR OF SC LAB OPERATIONS: John Altman
john.altman@haymarketmedia.com
SC LAB EDITORIAL ASSISTANT: Judy Traub
judy.traub@haymarketmedia.com
PROGRAM DIRECTOR, SC CONGRESS: Eric Green arn, green@haymarketmedia.com
REGULAR CONTRIBUTORS:
Stephen Lavoie,
Dob Rausch,
Kenan Erper Hoffman
DESIGN AND PRODUCTION
ART DIRECTOR: Michael Zinng
michael.zinng@haymarketmedia.com
PRODUCTION MANAGER: Kirasi Rahaman
kirasi.rahaman@haymarketmedia.com
SC EVENTS:
EVENTS DIRECTOR: Natasha Mulia
natasha.mulia@haymarketmedia.com
EVENTS MANAGER: Anthony Curry
anthony.curry@haymarketmedia.com
ASSOCIATE EVENTS MANAGER: Maggie Keller
maggie.keller@haymarketmedia.com
SUBSCRIPTION INQUIRIES:
CUSTOMER SERVICE: (800) 558-2703
EMAIL: haymarket@subbywest.com
WEB: www.scmagazines.com/subscribe

SC MAGAZINE EDITORIAL ADVISORY BOARD 2013

U.S. SALES
VP, SALES: David Stoffman
(646) 638-6028 david.stoffman@haymarketmedia.com
REGIONAL SALES DIRECTOR: Mike Sheehan
(646) 638-6006 mike.sheehan@haymarketmedia.com
WEST COAST SALES DIRECTOR: Matthew Allington (425) 340-6402
matthew.allington@haymarketmedia.com

EVENT SALES DIRECTOR: Mike Alesie (646) 638-6029
mike.alesie@haymarketmedia.com
ACCOUNT MANAGER: Dennis Kocher
(646) 638-6039 dennis.kocher@haymarketmedia.com
ACCOUNT MANAGER: Samantha Amoroso
samantha.amoroso@haymarketmedia.com
SALES/EDITORIAL ASSISTANT: Ivo Howar
(646) 638-6024 ivo.howar@haymarketmedia.com
ACCOUNT EXECUTIVE, LICENSING AND REPRINTS:
Elton Wong (646) 638-6302
elton.wong@iyaymarketmedia.com

SC MAGAZINE LISTS RENTAL:
elton.wong@haymarketmedia.com

ACCOUNT EXECUTIVE, LICENSING AND REPRINTS:
SalES/Editorial ASSiSTANT:
(646) 638-6104  roo.howar@haymarketmedia.com

ELITE MARKETING:
ACCOUNT EXECUTIVE:
Brandon Lark
(908) 541-4300
brandon.lark@haymarketmedia.com

EMERITUS:
HOWARD SCHMIDT

SYLVIA BURGESS

CIRCULATION
VP, AUDIENCE DEVELOPMENT & OPERATIONS:
John Crowe
john.crowe@haymarketmedia.com

AUDIENCE DEVELOPMENT DIRECTOR:
Sherry Dornen (646) 638-6003
sherry.dornen@haymarketmedia.com
ASSISTANT CIRCULATION MANAGER:
Laura Weinblatt (646) 638-6100
laura.weinblatt@haymarketmedia.com

CUSTOMER DATA MANAGER:
Joshua Blair (646) 638-6049
joshua.blair@haymarketmedia.com

MANAGEMENT"
CEO, HAYMARKET MEDIA: Leo Maniscalco
EXECUTIVE VP: Tony Kruel
Belarus top producer of zombie IP addresses

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

KETCHIKAN, ALASKA – Eighteen students are alleged to have participated in a phishing ruse in which they tricked a teacher into divulging an administrative password. This enabled them to access their classmates’ computers and spy on them using a freeware program that was used by teachers to monitor students.

LEAVENWORTH, WASH. – Hackers raided the online bank account belonging to Cascade Medical Center to siphon $1.03 million and deposit it into 96 accounts under their control. So far only $133,000 of the fraudulent Automated Clearing House, or ACH, transfers has been recovered.

LOS ANGELES – Two Northern California email hackers were sentenced for attempting to use naked photos they stole to extort money from World Poker Tour players. Tyler Schriet, 23, received three years and Keith Hudson, 39, earned a two-year sentence. A third defendant pleaded guilty and will be sentenced later this year.

JACKSONVILLE, FLA. – A vendor for Winn-Dixie agreed to pay $428,500 to settle a proposed class-action lawsuit filed by an employee of the supermarket chain following a data breach. The defendant, employee purchasing company Purchasing Power, said it denied the lawsuit’s claims, but settled to avoid litigation.

GERMANY – The Ministry of the Interior proposed new IT security regulations aimed at critical infrastructure operators and telecom companies. The legislation would force these entities to meet minimum security standards and report major incidents to the Federal Office for Information Security.

SPAIN – A Dutch man accused of launching massive DDoS attacks was arrested here and transferred to his home country. Identified by reports as Sven Kamphuis, 35, he is accused of attacking Spamhaus, presumably because the anti-spam organization blacklisted his web hosting firm.

ALGERIA – The suspected co-creator of the SpyEye trojan, which is used to steal online banking credentials, was extradited to the United States to face a 23-count indictment. If convicted, Hamza Bendelladj, an Algerian national who was arrested in Thailand earlier this year, could face more than 30 years in prison.

INDIA – Government websites were hacked more than 1,000 times over the past three years, according to the minister of state for home affairs. The number of incidents has steadily risen during that period. Officials are hopeful that a new requirement that sites must be hosted by secure infrastructure providers will help.
The personal information of 50 million LivingSocial members was put in jeopardy following a breach of the popular online couponing site.

### Malware Vertical encounter rate

<table>
<thead>
<tr>
<th>Position</th>
<th>Industry</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Education</td>
<td>165%</td>
</tr>
<tr>
<td>2</td>
<td>Retail &amp; wholesale</td>
<td>100%</td>
</tr>
<tr>
<td>3</td>
<td>IT &amp; telecommunications</td>
<td>80%</td>
</tr>
<tr>
<td>4</td>
<td>Food &amp; beverage</td>
<td>75%</td>
</tr>
<tr>
<td>5</td>
<td>Health care</td>
<td>65%</td>
</tr>
<tr>
<td>6</td>
<td>Banking &amp; finance</td>
<td>45%</td>
</tr>
<tr>
<td>7</td>
<td>Government</td>
<td>40%</td>
</tr>
</tbody>
</table>

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

### Index of cyber security

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

### Spam rate

**Volume by month for each region**

- **Asia Pacific**: 4.6B
- **Europe**: 2.1B
- **Africa & Middle East**: 1.6B
- **North America**: 991M
- **South America**: 849M
- **United States**: 9.03%
- **Japan**: 3.81%
- **Colombia**: 3.19%
- **Spain**: 1.69%
- **United Kingdom**: 1.60%

### Internet dangers

**Top 10 threats**

<table>
<thead>
<tr>
<th>Name</th>
<th>Movement</th>
<th>Date first observed</th>
<th>Type</th>
<th>Last month</th>
<th>Months on list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lamechi.B</td>
<td>↑</td>
<td>01/01/12</td>
<td>Downloader</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Hotbar</td>
<td>↑</td>
<td>09/3/10</td>
<td>Adware</td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>Loring</td>
<td>↑</td>
<td>02/01/11</td>
<td>Downloader</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OnLineGames.AH</td>
<td>↓</td>
<td>12/6/10</td>
<td>PasswordStealer</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Zbot</td>
<td>↓</td>
<td>09/2/10</td>
<td>PasswordStealer</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Fesber.F</td>
<td>↑</td>
<td>02/04/11</td>
<td>Worm</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td>Vobus</td>
<td>↓</td>
<td>01/01/11</td>
<td>Worm</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Fesber.A</td>
<td>↑</td>
<td>02/04/11</td>
<td>Worm</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>Ramnit.A</td>
<td>↑</td>
<td>09/10/10</td>
<td>Bot</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>Soften.L</td>
<td>↑</td>
<td>01/08/11</td>
<td>Worm</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Zombie IPs Global distribution

The biggest increases in month-over-month zombie activity occurred in India, Iran and Peru, while the largest decreases occurred in Russia and Vietnam.

### Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Zeus trojan
3. Butterfly botnet
4. Pushdo trojan
5. Dapalo trojan

There were 12,412,915 attacks in the United States last month, primarily originating from Columbus, Ohio; Los Angeles; Overland Park, Kansas; New York; and Cleveland. There were 21,012,779 foreign attacks last month, primarily originating from Tokyo; Bucharest, Romania; Mumbai, India; Taipei, Taiwan; and Sao Paulo, Brazil.

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

1. ZeroAccess trojan
2. Pushdo trojan
3. Butterfly botnet
4. ZeuS trojan
5. Rustock trojan

### Index queries

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

### Received spam Top five regions

- **United States**: 9.03%
- **Japan**: 3.81%
- **Colombia**: 3.19%
- **Spain**: 1.69%
- **United Kingdom**: 1.60%

Spam rate indicates the accumulated emails tagged as unsolicited.

### Top breaches in April

**Data loss**

- **LivingSocial Washington, D.C.**
  - As many as 50 million members of the deal website may have had their personal information and encrypted passwords exposed after a cyber attack.
  - 50,000,000

- **Kirkwood Community College Cedar Rapids, Iowa.**
  - Hackers accessed the school’s website and applicant database system. Anyone who applied to a Kirkwood campus may have had their personal data exposed.
  - 125,000

- **Scribd San Francisco**
  - Owing to a hack, users of the digital library site had their encrypted passwords stolen. Those who were affected received instructions for resetting them.
  - 100,000

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

607,781,515 (as of May 13)

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

Canadian Privacy Commissioner Jennifer Stoddart called for fundamental reforms to Canada’s privacy law that would make companies more accountable for their actions.

The updated law also would give the commissioner stronger enforcement powers, including statutory damages. In addition, she would be able to order organizations to take mitigating measures.

A new border protection program must follow privacy laws.

Border. Check?

The United States has tracked thousands of foreigners passing into Canada. A pilot project under its Entry/Exit Initiative tracked non-U.S. or Canadian citizens traveling north across the border. "Opportunities exist to identify document anomalies or fraud," a statement from the Canadian government said.

The two governments are now exploring the privacy implications for an expanded second phase.

“The may as well admit defeat on the first review, get rid of Bill C12, described as inadequate, and start again with new hearings,” he said.

You might get hacked, but you will get audited.”

— Jeremiah Grossman, founder and CTO of WhiteHat Security, on how compliance still remains a leading driver for organizations

Investing in secure software doesn’t seem to help make users much safer. Meanwhile, it often detracts from the functional- ity and usability of software. While nobody would argue that we completely ignore software security, economics and the basic need for practicality call for a more pragmatic approach.

THE SC MAGAZINE POLL

Do you support the Cyber Intelligence Sharing and Protection Act (CISPA)?

Yes 16.33%
No 83.67%

Source: reports

I consider the economics of the end-user to be the most widely exploited, and then the impact that exploit can have on tar- geted organizations can be cata- strophic. All widely deployed software products should be hardened against attack as part of the original design. This includes steps such as threat modeling, spec reviews, code reviews and hands-on pen testing.

Unfortunately, even though the industry is not yet mature enough to decipher what actu- ally works well, people have stepped in with regulation prematurely – and it’s been a bad thing for almost everyone involved. Look at PCI – it hasn’t stopped credit card breaches. It’s not helping the end-user much, and it’s keeping vendors from spending time and money on measures that could have a much more positive impact as we learn more about how to build robust systems. Rather than wasting resources on compliance with ineffec- tive standards, software developers should be doing things that actually help secure software.

Debate

Software developers are not incentivized to improve security.

FOR

Software developers are not incentivized to improve security. Investing in secure software isn’t worth the time or effort because of the cost of compliance with regulations. Compliance often detracts from the functional- ity and usability of software.

AGAINST

Compliance is key to software security. Without it, software developers are not incentivized to improve security. It’s not helping the end-user much, and it’s keeping vendors from spending time and money on measures that could have a much more positive impact.

THE STATS

92% of Democrats in the House voted in April for passage of CISPA

117.6k number of signatures on petition to White House to stop CISPA (as of press time)

Source: reports

Java exploit

What is it?

A remote code execution vulnerability (tracked as CVE-2013-2423) affecting Java versions 7 Update 17 and prior, which allows a complete sandbox bypass via browsers.

How does it work?

The root cause of the vulnerability is a type- confusion issue in Java’s reflection, which allows calling internal methods to disable the security manager. This issue can be leveraged by simply convincing a user to visit a web page that contains malicious Java content.

Should I be worried?

Yes, an exploit for this vul- nerability is now bundled in various exploit kits that allow arbitrary code execu- tion in a reliable manner. Users should show caution when visiting untrusted websites if their systems are not patched.

How can I prevent it?

Oracle has since issued version 7 Update 21, which fixes the vulnerability. Any system using an older version should update to this generation. This update fixes 42 security issues, including the one discussed above.

THE MONTH

THREAT OF THE MONTH

Java exploit

Java exploit

Java exploit
A recent wave of a vicious prank known as “swatting,” in which mischief-makers call 9-1-1 and use special equipment to make it appear as if their phone number is coming from the home of the person they are targeting, is generating nationwide attention. The hoax, which is not new but has seen significant upticks in incidents of late, is a modern-day telephony network, and is created by criminals who call 9-1-1 as “swatting,” in which the posting or circulating spam. “It all comes back to trick.”

He explained that all modern-day telephone networks — whether it’s a private branch exchange (PBX) or a voice over internet protocol (VoIP) connection — are susceptible. “The identification of the caller is trusted by the recipient and is created by the sender,” Winnie said. “As long as we’re talking about a digital connection to the phone system, you can send anything you want. As swatting becomes more prevalent, state lawmakers have introduced legislation that would stiffen penalties for offenders. But while new laws may offer a deterrent, there’s little technical that can be done to prevent the pranks.”

The hoax, which is not new but has seen significant upticks in incidents of late, is a modern-day telephony network, and is created by criminals who call 9-1-1 as “swatting,” in which the posting or circulating spam. “It all comes back to trick.”

He explained that all modern-day telephone networks — whether it’s a private branch exchange (PBX) or a voice over internet protocol (VoIP) connection — are susceptible. “The identification of the caller is trusted by the recipient and is created by the sender,” Winnie said. “As long as we’re talking about a digital connection to the phone system, you can send anything you want. As swatting becomes more prevalent, state lawmakers have introduced legislation that would stiffen penalties for offenders. But while new laws may offer a deterrent, there’s little technical that can be done to prevent the pranks.”

Steve Milner, a South Jordan, Utah-based enterprise security management firm, has acquired a product line from VMware, a Palo Alto, Calif.-based vendor. With the purchase, LANDesk takes on VMware’s “Pro- tect,” which will now be called the “Shavlik Protect” portfolio. The acquisition expands LANDesk’s user-oriented IT management market presence.

Nick Hetrick network team lead, WellsSpan Health

How do you describe your job to average people? As a member of WellsSpan security ops, I take the lead on vulnerability and protection management. I proactively mitigate techni cal risk for existing systems and new implementations. This role is also responsible for daily operations and support of WellsSpan’s security controls. I also manage the implementation of new security controls that protect the enterprise.

Why did you get into IT security? I was looking for a way to expand my skillset. Previously, I held senior network engineer- and network manager-related positions at other organizations. I wanted to capitalize on this skillset to grow professionally. IT security is always something that caught my eye. I just had to gather enough courage to step outside my comfort zone. I’m happy I made the leap and would recommend others do the same.

What was one of your biggest challenges? From a security standpoint, ensuring secure remote access for a large and complex organization is a challenge. AAA [authentication, authorization and accounting] are the driving factors for any remote access solution, but this is easier said than done and requires many infrastructure pieces to be implemented, including business processes.

What keeps you up at night? Ensuring our systems and their data remains safe. Malware and network-based attacks become more sophisticated each day. This also holds true for phishing attacks. As a result, we are always looking for new products or ways to optimize existing protections to keep the bad guys out.

Of what are you most proud? I’m proud of the work that has been accomplished, in a very short time, to stand up a new centralized security department and shape the direction of how the enterprise protects its systems.
A case study in curbing phishing

Denise Wood
CISO, FedEx

FedEx strives to be a leader in all aspects of customer satisfaction. We realize our customers play an integral role in protecting themselves and helping secure cyber space, and we want to do all we can to help them.

The challenge of securing an organization’s reputation and doing business in cyber space has never been more difficult, with the exploitation of e-commerce and the pervasiveness of hackers and scammers exploiting those channels. FedEx has responded to this challenge by introducing two customer-focused initiatives: the FedEx Customer Protection Center and the Email Security Program.

In 2009, we launched the FedEx Customer Protection Center on FedEx.com to help educate our customers and reduce potential brand damage caused by online scams. Our Customer Protection Center has become the authoritative source for the communication of security and fraud-related information to our customers. The FedEx Customer Protection Center provides online safety tips, real-life examples of actual phishing scams, and a dedicated email to which customers can report potential scams. Since the center’s inception, more than 270,000 reports have been submitted via the site and the abuse@fedex.com address. We reflect the results of these reports to our customers to raise their awareness of active scams and phishing campaigns. Transportation and logistics services have also become the target of enormous global phishing campaigns, and the prevalence of these ruses using express shipment keywords drove us to create our Email Security Program. This initiative, launched last year, implements technologies to aggressively suppress the staggering amount of malicious email sent falsely using the FedEx name, while allowing legitimate, FedEx-generated emails to continue to reach their intended audience.

With 40 years of IT innovation, obtaining an inventory of all sources of digital communications with our customers was a huge undertaking. Once that was done, our Email Security Program was designed to leverage industry proven standards to ensure all legitimate messages have good security hygiene and that messages that fail authentication and policy enforcement are discarded.

The Customer Protection Center and the Email Security Program are just two ways that FedEx secures its brand in cyber space so that we do not lose the ability to communicate digitally with our customers. These initiatives are a small part of the holistic solution comprised of our best assets—millions of customers, cutting-edge technology and the pride of the FedEx brand in cyber space.

30 seconds on...

Building trust
FedEx’s commitment to customers is called “Purple Promise,” says Wood. It includes protecting customers by providing a trusted e-commerce experience.

Latest defenses
Though she wouldn’t disclose specific solutions, Wood says she and her team are confident in the tools the company has deployed to fight spam, malware and emerging threats.

Always vigilant
Wood says she and her team expect to greatly improve their response time to identify and shut down malicious sites as the programs that have been implemented are refined.

An educated consumer
Informing millions of customers to be more “online savvy” improves their own security and expands the army of informed users to better protect cyber space, says Wood.

From the CSO’s desk

Back to basics

Security programs have been and will continue to be built around fundamental security principles: access control, least privileges; defense in depth; configuration and change management; standards and compliance, etc. Tools and processes supporting these abound, and companies have spent an extraordinary amount of money implementing them.

Unfortunately, we continually fail to push them to their ultimate capabilities. Instead, we install, walk away and lose interest. As security practitioners, it is our professional duty to build solid foundations in the security basics, heding the tide of hype which fools us and our leaders into diverting our attention to the shiny coin. These foundations have to include full lifecycle enablement, continuous monitoring for improvement, and metrics guiding decision-making and maturation.

Until we succeed in managing the basics, we’ll fail in addressing the advanced.

Storage is risky on mobile

The biggest risk of mobile computing continues to be unauthorized physical access to the device as a result of loss or theft, but threats of viruses to mobile devices continue to grow. The vulnerabilities of these smartphones and their unprotected applications allow easy access into the enterprise’s systems and data environment.

Mobile device/information management (MDM/MIM) solutions are one type of technology that can be implemented. They generally have some method of device registration, monitoring and remote wipe in case of loss or theft. More advanced versions of these management suites include the ability to create separate, encrypted data partitions to store and access corporate data. Another advanced option within MDM/MIM solutions include data leakage prevention (DLP) functionality. DLP software provides some protection for end-users and applications copying and distributing proprietary and confidential information.

Still, these security solutions—which primarily address the physical and logical perimeters of IT systems and applications—are insufficient because devices are configured to bypass them to allow communications to critical enterprise resources and access to internal applications and data.

In addition to device-based solutions, a forward-thinking company should factor in data security. To mitigate the risk of data loss, theft and corruption on mobile devices, it is important to minimize, if not eliminate, all assets from being stored on the device. Development of web-based applications that can be accessed and viewed via mobile browsers allows companies to concentrate on higher levels and availability of server-based authentication and access security solutions. Maintaining data at the servers—rather than pushing it to the devices—decreases the possibility of data loss and centralizes the security administration, resources and tools within hardened data centers.

“…”

Maintaining data at the servers decreases the possibility of data loss...”
Tech-savvy Generation Y workers can be an advantage in the enterprise, says James Beeson, CISO at GE Capital Americas. Marcos Colón reports.

Last year, when James Beeson’s son was at Texas Tech University, studying to become an engineer, he came across a calculus problem that had him stumped. So, the 20-year-old did the only obvious thing a shrewd college kid would do: He asked his family and friends for help – without exerting too much effort.

So rather than going through the manually intensive process of reaching out to each person one by one, he took a high-resolution picture of his laptop screen, and sent the photo in a group text message to everyone.

Beeson was impressed by his son’s ingenuity and efficiency. But the CISO and IT risk leader at GE Capital Americas since 1997, a commercial financing and leasing provider, also knew it underscored how a younger generation of users thinks and operates, the type of mindset that could introduce security risks to employers.

“I think they’re so used to sharing and so used to having a much more open environment, that they’re used to going wherever they need to get things done, without necessarily thinking about the ramifications of the data they may be creating,” Beeson says.

With nearly 15,000 endpoints, many of them bring-your-own-devices (BYOD), deployed in GE Capital Americas, Beeson deals with many employees who resemble his son in terms of IT practices. Whichever way you like to refer to them – digital natives, millennials, Generation Y – there has been a steady influx of young, tech-savvy individuals entering the workforce. And because text messaging and web surfing is all they’ve ever known, their inclination to adhere to an organization’s security policies and guidelines may not be as firm as their predecessors.

“I don’t see [the way they act] as a problem,” Beeson says. “I see it as a great way to solve problems collaboratively and quickly. What I do see, though, is that we’re not ready for it from an information security and data protection perspective.”

But thanks to his children, Beeson has been out in front of this new challenge, implementing forward-thinking security awareness training, acceptable-use policies and technology controls to help manage younger workers’ tendencies and their toys. “I’ve watched the way they have been brought up and have used technology and I’ve seen the shift,” Beeson says of his children. “I’ve also seen it at work with the younger generation that comes into the workforce.”
Consumerization
devices from potential threats. And most worrisome of all, according to the findings, these respondents may be fully aware that they’re breaking the rules, but they do it anyway.

Riskgy business
A majority of the risks associated with digital natives emanates from their use of social media. Chenxi Wang, the former vice president and principal analyst at Forrester Research, says. Seeing as they’ve grown up socializing online even more than in person, the lines are blurred when it comes to these platforms.

“It’s not in their DNA to think twice about posting something (work-related) on a public forum,” Wang says. “They’re not brought up to consider that there is certain information that should not be posted on places like Facebook and Twitter because they’ve always lived and breathed these platforms.”

Based on a Check Point study, the source of attacks causing most concern for this new breed of worker is social and P2P file-sharing networks, while email or phishing attacks remain problematic for the “baby boomer” generation.

It’s time for firms to make some adjustments to accommodate the advantages digital natives bring. Before anything else, says Steve Durbin, global vice president of the Information Security Forum, a nonprofit organization that works with enterprises around the world to address security and risk management issues.

He says companies should focus on creating an environment that empowers, rather than limits, the abilities of Gen Ys. “It’s about enabling (them) to, dare I say it, have fun doing [their] job,” Durbin says.

But, there are risks that must be addressed. Wang points out that younger workers are tech-savvy on their smartphones. And, with mobile malware increasing, a BYOD-friendly environment could be ripe for security incidents.

When joining an organization that supports BYOD, an employee’s device will likely start touching sensitive data, something that they’ve never experienced before, says Domingo Guerra, president and CEO of Appthority, a San Francisco-based mobile application security firm.

“At home, everything they own, even if it’s quite personal, they didn’t consider to be sensitive data,” Guerra says. “They’ve shared their relationship status on Facebook. When they get to work, it’s a clash of culture because you can’t share everything you do at work with the world.”

However, Gen Y isn’t the only place to point a finger for its excessive use of mobile devices, says Zach Lanier, senior research consultant at Accurant, a Denver-based firm that helps align IT security and business objectives.

This phenomenon also extends to the so-called consumerization of IT. These are not just corporate email devices anymore,” Lanier says. “They’re gaming and social media devices. The phone is not the main feature anymore.

Because the targeted environment could be ripe for security incidents. “If you look solely at the choices that they make before picking which apps they have to install random applications on their phones without thinking about what the permission prompts mean, and what communication channels that might offer a malicious actor, then I might say maybe they’re not so security savvy,” Lanier says.

However, he adds that the answer doesn’t lie in creating closed environments or placing endless limitations in terms of an organization’s BYOD strategy. Instead, Lanier says there should be a requirement for digital natives to have to opt in to the personal devices they use for an enterprise’s BYOD environment.

“If you agree to bring your cool, shiny, new device and hook it up to our network, the compromise is that you have to accept that we will exhibit some control over that,” Lanier says.

Productivity versus security
Appthority’s Guerra adds that a locked-down environment is not the way to go, seeing as it won’t jibe with younger employees and could limit their productivity. Instead, he views their ability to use collaborative tools, both on desktops and mobile devices, as a major benefit for organizations.

“The young generation is great at working in teams and collaborating online,” Guerra says. “You are able to keep people happier if they have the tools they feel will make them productive. Gen Y is not dumb. They just don’t know what a risk is and why it’s a risk. If you give them the tools and information, they’ll most likely be more compliant.”

While there are challenges that come with employing a nascent workforce, there’s no denying the benefits they offer enterprises.

According to the previously mentioned Check Point survey on Gen Y versus baby boomers, only 31 percent of Gen Y respondents ages 18 to 25 believe that security is more important than productivity. While this may seem like an unattainable statistic for security professionals, the relatively low level of productivity digital natives offer organizations far outweighs the risks.

“Very few people are concerned about IT security,” Guerra says. “They’re timely, but not time managed,” he says. “They don’t care about working in an environment that’s nine to five. They share knowledge constantly.”

But, to enable this brand of worker to reach maximum productivity, it must be given the proper tools. A study conducted by Johnson Controls Global Workplace Innovation, which surveyed 2,800 digital natives, revealed that 77 percent of respondents believe advanced technologies in their workplace are “important” to “very important.”

Durbin says that a majority of Gen Y employees think IT departments are slow to pick up on the latest trends and developments in technology.

“It’s all about speed, [the] latest technology and the tools as a means to get the job done,” Durbin says. “I think if you look at that perspective and compare that with the kind of environments that we see in most large enterprises, you can begin to understand some of the pinch points that are going to exist as Gen Ys become more prevalent in the workplace.”

Turn back the clock
According to Beeson, the perceived IT needs of younger staff can coexist with the data security and privacy requirements that companies face, but it comes down to understanding the behaviors and needs of millennials. To do so, he recommends that security practitioners find their own “digital mentors,” much like his own children are to him.

“Coach them and let them coach you,” he says. “What you find is that understanding makes a big difference in how you can actually leverage and use the devices and technology to your advantage the way that they use them.”

While Beeson says there’s certainly a gap that needs to be bridged in the enterprise between millennials and boomers, he says education may be the answer. Security professionals need to start thinking more about the access needs of their colleagues, without having a close-minded approach to security.

“Try and educate the ‘digital immigrants’ on how the digital natives are at work and play, and try to educate the digital natives on why there are risks,” he says.

There’s no way around dodging the wave of talent that’s flooding into the workplace. Beeson says, and IT must start thinking about ways to embrace it.

“If we want to go higher and bring on the best and brightest into our companies, we’ve got to understand this and figure out ways to use it,” he says.

—James Beeson, CISO, GE Capital Americas
The private sector has been very reluctant to share information...

– Avner Levin, Ryerson University

Robert Eastman, vice president of global solutions for Lockheed Martin, adds that the increase in sophistication and complexity of attacks demands increased awareness. “We have to extend the knowledge and understanding of what’s going on beyond senior leadership in corporations and government to employees and average citizens.”

Breaking this barrier is an essential component of generating awareness of cyber crime, says Avner Levin, law and business chair at Ryerson University’s Ted Rogers School of Business Management. “The private sector has been reluctant to share information about cyber crime, data breaches and other security-related matters, and the availability of such data through this survey is welcome.”

Taylor refers to it as a shared responsibility and says that society as a whole needs to look at the results together and determine what constitutes acceptable cyber behavior and what will not be tolerated. “Only then can you put the policy, regulatory and education pieces together,” he says.

Michael Brown, BlackBerry’s vice president of security product management and research, says his company hopes that the report will help raise awareness, particularly among small and midsize businesses, about the vulnerabilities associated with mobile devices. If smartphones and tablets are not secured, he says, the enterprise network is vulnerable. “Companies need to start thinking that mobile devices are smaller versions of laptops in the sense of what you can access and interact with when you’re on a device.”

The report makes three main recommendations: Organizations should plug the gaps in their cyber crime preparedness, including more trained personnel; better strategies and mitigation procedures; business needs to go beyond mainstream media to build awareness of cyber threats; and Canada’s national law enforcement agencies – Public Safety Canada and the Royal Canadian Mounted Police – should take a larger role in communicating about cyber crime.

For its part, Public Safety Canada agrees, saying the federal government welcomes the research because it will help keep Canadians and businesses safe. “This study aligns with the government of Canada’s commitment under the Cyber Security Strategy to cooperate with the private sector to strengthen Canada’s cyber resiliency,” a spokesperson says in an email.

Taylor agrees. “The survey can be a weapon to fight back against these attacks,” he says. “What we found makes a compelling case that the threat is real and immediate.”

Levin says the ongoing endorsement of large sector leaders will be essential in keeping information flowing, something that researchers have been craving. He says financial services companies previously declined to share data regarding cyber attacks with Ryerson University. “I hope the day will come when corporations will be willing to cooperate with academic research projects as well,” he says.

Taylor agrees that working together to find ways to protect enterprises is critical. “For my part, I will be speaking with businesses, governments, individuals and communities to get the collaboration started as soon as we can,” he says.
Awareness training

Security company Mandiant recently outed the sophisticated threat group that security experts had been tracking for years. It was unrelated to the Chinese government, blaming them for the theft of hundreds of terabytes of information from more than 140 organizations over a period of years. Many of those so-called advanced persistent threats (APTs) are based on software that has quietly found a home within unsuspecting enterprises. Fundamentally, such APTs represent a threat to an enterprise that it cannot anticipate.

According to security professionals, APTs are a technical quandary. However, training corporate insiders to be more resistant to security threats is also a continuing challenge for organizations of all sizes. Security training is a critical component of an enterprise’s security management strategy.

Training: Bad actors

Ever since the David Nosal case, dating back to 2004 – when a high-level staffer at an executive search firm left to start a competing company, and, with the help of other former colleagues, walked off with the company’s proprietary information – companies have been on high alert for security threats that lurk within current and former employees. Security training is a critical component of an enterprise’s security management strategy.

Insiders have more access to vital assets than an outside try to break in, says Sam Erdheim, senior security strategist at AlgoSec, a Boston-based company focused on network security policy management. Education is important, he says, because it can greatly reduce risks related to social engineering, an age-old tactic employed to manipulate people into divulging proprietary information. Erdheim recalls a recent incident when his aunt received an email that purported to be from him. “However, she was able to recognize that something was wrong and actually contacted me to tell me my account had been hacked,” he says.

Beyond social engineering, there are other serious risks involving employees, such as the loss of storage and mobile devices. “Employees who aren’t alert to the danger might find a lost memory device. Companies have been on high alert for security threats that lurk within current and former employees. Sam Erdheim, senior security strategist at AlgoSec, says insiders need to be trained about attacks that emanate from the outside, but also be regularly reminded about internal security policies and the consequences of violating them.

In addition, he says, database or firewall administrators who “touch” much more sensitive information than others, should receive greater focus from an educational and enforcement standpoint. “Change management, for example, is not handled well at many organizations, which could increase potential vulnerabilities,” he says. That’s because the people who have the power to make changes to a process may take shortcuts, but these changes may have security consequences that need to be highlighted in training, he says. “Poor process and lack of visibility into what is going on can have a big impact, especially for highly trusted people with system access,” he adds.

According to security pros, organizations are and should be concerned about the way APTs and less sophisticated threats are and should be concerned about the way APTs and less sophisticated threats are handled. Good training can succeed on its own. “Training should help them to succeed,” he says. “If you test them with phishing attacks, make it an opportunity to learn more, not a chance to criticize them.”

Further, Abrams says companies shouldn’t consider developing their own training methods met their specific needs. “Sometimes, outsiders can provide additional expertise or personnel to help, but often companies can succeed on their own.”

And, be patient, he adds. “Cars have been around for 100 years, so society has finally made safety almost second nature. It will take time for IT users to get to that same level.”
“Good morning

Winners”

Entries are now open for SC Awards 2014

Make sure you review our new and revised categories:

Best Advanced Persistent Threat (APT) Protection *NEW
Best Risk/Policy Management Solution *NEW
Best UTM Security Solution *REVISED

Nominations close Sept. 6, 2013
download your entry kit today.

Visit awards.scmagazine.com to
download your entry kit today.
Nominations close Sept. 6, 2013

How we test and score the products

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

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

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor. All reviews are set for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

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

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

What the recognition means

Best Buy goes to products the SC Lab rates as outstanding.
Lab Approved is awarded to extraordinary standouts that fit into the SC Labs environment, and which will be used subsequently in our test bench for the coming year.

So, you’ve got your policy in place. Then, based on your policy, you have tweaked your network to comply. You run the vulnerability assessments and pen tests and you’re pretty sure you’ve got the information security engine purring like a contented kitten. You’re off to other things, such as the daily fires with which you constantly deal. Sometime when you weren’t looking there was a new regulatory requirement, two new firewalls and a new corporate website for the marketing team. Now what? Is it time to run a whole new risk assessment? Not necessarily.

This month’s products – and there are a slew of them – watch policy, make sure that you know what needs to be changed and what doesn’t, and how your organization’s risk picture has changed. These tools have been maturing from large, unwieldy software beasts to compact, easy-to-use tools with a lot of power in smaller packages. That is not to say that they are miniaturized, trivialized or otherwise designed to cut corners. In reality, they do the same as, or more than, their predecessors. They just do it better with more manageable user interfaces and more powerful policy engines.

Strangely, we have come from one or two credible players in this arena to nearly two dozen. That is not the way we usually see a market evolve. In fact, with this product group we have broken all past records for the number of products in a single issue. Will the usual convergence happen eventually? Maybe, but this bumper crop of products sends a message that policy engines are maturing from large, unwieldy software beasts to compact, easy-to-use tools with a lot of power in smaller packages.

I conducted a seminar for small businesses recently and I made the point that compliance does not equal security. An alarming number of major breaches have taken place in enterprises that were, for example, PCI compliant. So the issue is not being able to tick off the boxes on a compliance audit. The issue is securing the enterprise as the bad actors become better at their trade and gain support from groups with money and an axe to grind. This month’s group of solutions can help you put that checkmark in the compliance column while staying – and knowing that you are staying – secure.

—Peter Stephenson, technology editor
Risk & policy management

This month we look at risk and policy management tools, and we have a lot of them for your consideration.

Enterprise risk management is a continuous process. It begins with setting objectives and identifying risks. Once the risks are identified, they should be assessed to understand how to treat them. Risks can either be controlled or eliminated. In either case, there needs to be some way to communicate the risk picture and continue monitoring. That continued monitoring may illuminate additional risk objectives – and new strategy needs to be set starting the cycle over again. Risk management tools provide a platform on which to perform this risk management cycle.

Policy management, on the other hand, is not quite as clearly defined. In some cases, policy management refers to the supervision of an organization’s security policies derived from risk management, regulatory requirements and other types of input. In other cases, it refers to how policy is applied, managed and updated to devices. It is not uncommon to see these types of applications in the same product. However, policy management, like risk management, is a continuous process. And, no surprise, the two – policy and risk management – are tied together because policy is intended to address risk.

Typically, conventional wisdom tells us that the first task in creating an enterprise architecture is to perform a risk assessment. Once the risk assessment is complete, one needs to create policies to address the risks. So, if one has a need for a secure enclave, such as an online banking system, the admin will address the risks inherent in such a system, create policies that address the risks and then design an architecture that addresses those risks.

Now that an architecture is in place, one can begin to populate it with tools. However, at this point, the admin will find that the tools need to be configured to implement and enforce the policy also must be configured with its own policies – although these really are settings that enforce or implement policy – and these need to be kept current. Current with what? Well, the policy, of course. Risk drives the policies, so as risks change policies – both in the abstract (the organization’s written security policy) and in the concrete (configuration policies), policies need to change. For a big enterprise, all of that can be daunting.

That is where our tools enter the picture. It has long been my position that both these two types of tools are necessary to manage an enterprise’s security properly. The big problem – and one that user organizations and vendors alike have been struggling with for years – is how do you make this work for all but the largest organizations.

I am aware of an organization that needs what these tools offer. Some years back, they purchased a pricey but well-thought-of tool and went through training, configuration, transferring policy, etc. Part way through the process they decided they did not have the resources to get the job done right, and they shelved the initiative. The tools we reviewed this month can go a long way toward keeping that sort of thing from happening in the future.

So, the bottom line: If yours is a medium to large enterprise, managing policies, risks and various attendant configurations is a real issue. Most likely, if you haven’t implemented an automated approach, you are struggling to keep everything configured, policies aligned with requirements and risks measured and managed as new ones come over the horizon.

Automated risk and policy management is a major step if one wants to make the most of human resources, instead of marshaling these workers to manual tasks that never resolve.

Are these tools pricey? Some may be, but this is like any other security product. Look closely at what is needed to accomplish and either make it fit your pocketbook or start lobbying for a bigger one. In the long run, though, the savings through automating these tasks will be significant enough to justify their purchase.

Michael Liposits and Mike Stephenson contributed to this month’s Group Test.
Agiliance RiskVision v6.5 SP1

The Agiliance RiskVision platform manages enterprise risk by making it visible, actionable and measurable across business units, IT operations and security management in near real time. The tool comes as a single platform with multiple modules that can be activated via licensing. Manager modules are available for compliance, enterprise risk, vendor risk, threat and vulnerability, and policy and incident.

Agiliance provides a holistic view of security and compliance in one integrated enterprise platform that enables companies to move from a reactive, threat-driven approach to a proactive, risk-aware posture. The platform brings together threat and vulnerability data, security configuration data and compliance and risk assessment data. RiskVision correlates this data against its “business-criticality aware” asset database, as well as its multi-regulatory compliance framework of 50-plus standards and policies, providing organizations with an aggregated view of their risk and compliance posture.

The solution is delivered either as on-premise software running on available hardware or as an on-demand, cloud-based platform. It requires Microsoft Windows Server 2003 or 2008, and either MySQL 5.5 or Oracle Database 11g R2 for server side deployment, and a simple web browser and Adobe Flash v10 or higher for the client.

RiskVision has a strong, out-of-the-box policy module that is built off of COBIT, ISO and NIST frameworks. There is a lot of pre-populated content for policy, assessment, controls and reporting. It supports continuous import/export of data using prebuilt templates from MS Word, Excel and XML. Users can automate assessments against these standards or internal controls. The workflow tool makes it easy to develop and manage the assessments. This tool also has a feature that allows one to validate a user response to ensure they actually read what was sent. The offering comes with a fully integrated ticketing solution and can also be integrated to the common ticket platforms on the market.

New features in this version include mobile device and user detail support. RiskVision will collect and correlate mobile data from mobile device management (MDM) vendors. It can then rate access versus risk related to an application using a device (BYOD). RiskVision will collect and correlate mobile data from mobile device management (MDM) vendors. It can then rate access versus risk related to an application using a device (BYOD). RiskVision will collect and correlate mobile data from mobile device management (MDM) vendors. It can then rate access versus risk related to an application using a device (BYOD).

AlgoSec Security Management Suite v6.4

The AlgoSec Security Management Suite is comprised of three parts: the FireWall Analyzer, FireFlow and BusinessFlow. The FireWall Analyzer allows administrators to fully automate auditing and management of FireWall rules and policies. FireFlow provides a change workflow platform to manage FireWall policy changes, including automated changes to Check Point devices via the ActiveChange feature. Finally, BusinessFlow brings together firewall and security policy with application needs. Without putting systems at unnecessary risk, administrators and application managers can use BusinessFlow to easily and accurately ensure that a proper policy that grants required application rules is deployed throughout the environment.

We found installation of this appliance to be quite straightforward and easy. The initial installation is done by connecting to the appliance through a console or SSH connection to configure the IP and network settings. Once we had the network settings in, we were able to manage and configure the appliance through the web-based management GUI. We found this interface to be fairly simple to navigate with an intuitive layout. We also found the integration of the various functions to be well-organized throughout the interface. As for adding and managing devices, we found this product to be easy to configure and were up and running in minutes. This product comes pretty well loaded out of the box. On top of device support for almost any firewall and router, the AlgoSec Security Management Suite comes preloaded with several ready to go workflows for adding, removing and re-certifying rules and removing or changing objects. Also included are pre-defined reports for regulatory compliance auditing. Some of the templates include PCI, SOX, ISO 27001, NERC CIP, Basel II and J SOX. Aside from compliance auditing, this product also helps streamline policy risk assessment through deep analysis of the existing rules throughout the environment, as well as finds unused rules and objects and shadowed, duplicate and expired rules to eliminate clutter and unnecessary risk to the network. On the application side, this product offers full automation for translating application connectivity requirements to firewall and router rules. This ensures each application gets properly crafted rules with no unopened open or wrong ports.

Documentation included with this product consists of several PDF user guides and manuals. We found all guides to be well-organized and easy to follow with many step-by-step instructions, configuration examples and screen shots. AlgoSec offers three different tiers of technical support to customers as part of a support and maintenance program. Customers can purchase support at nine-hours-a-day/five-days-a-week, 16/5 and 24/7 levels. Each of these levels includes phone, email and web-based assistance.

With pricing starting at around $10,000 for the appliance, software and licensing, we find this product to be a very good value for the money. The AlgoSec Security Management Suite offers a lot of features and functionality at a competitive price.
Allgress Insight and Risk Manager v4.1

Allgress Business Risk Intelligence helps companies quickly and automatically aggregate data from security and compliance assessments and technical inputs, and turn this into meaningful, actionable, risk-specific intelligence that can be aligned with the goals of the business. With Allgress, one can identify risk areas that are underexplored, and reorder security priorities to better align with the current business environment. Allgress helps admins assess risk or compliance within their organization by determining how closely it adheres to a particular standard.

The solution is sold as on-premise software running on the Microsoft platform, Windows Server 2008 R2 (x64) and SQL Server 2008R2 (x64). We were told that typical implementations take about two weeks. There is also a hosted, cloud-based model. Licensing is either perpetual or subscription based on the model deployed. Pricing is based on the size of the organization and the number of modules purchased.

Allgress is a risk platform that includes modules supporting assessments, vulnerability analysis, policy management, mitigation and incident management. It has a well laid-out user interface with tabs across the top for each function. Users are usually no more that three clicks away from any of the information desired. The tool is preconfigured with a number of popular standards, and uses the Unified Compliance Framework (UCF) content library. The library's functionality is easy to use, but its important to note, the library is hosted in the cloud, not locally within the on-premise solution. Assets come in from the user's vulnerability data and are manually entered or imported.

The visualization capabilities are impressive. From the risk heat maps to the slick, wheel-based vulnerability graphs, data is presented in a usable and meaningful way. Trending techniques and business modeling offer a clear balance between past, present and pending threats to the business. One also has a beneficial “what if” analysis tool to model changes or mitigations prior to investing or deploying.

Allgress is a flexible platform that can grow with the organization's maturity level in managing risk, compliance and security. It can provide an efficient balance of timely, understandable results at a justifiable pricepoint without the added complexity of an overabundance of functions. This could be a pro and con depending on one's needs. There are more sophisticated tools on the market with more bells and whistles. The value of Allgress is to help both IT staff and non-technical-oriented leadership understand their vulnerability risk posture by employing a language they can understand. This is intended to prioritize IT resource investments to meet business objectives.

Standard eight-hours-a-day/five-days-a-week support is included with either the hosted or purchased licenses. Extended 24/7 support is available at 30 per cent of the list price.

Allgress delivers a solution that can be deployed quickly so as to immediately deliver value through visualisation for all technical and business groups. – ML

Aruvio GRC v2.2

The Aruvio GRC Suite is a complete set of governance, risk, and compliance (GRC) applications, including controls, compliance, vendor risk, enterprise risk, incident management, and policy and training. The solutions are geared toward mid-sized organizations, as they are designed to be simple to deploy and priced to be attractive for smaller user counts.

The product is available as a cloud-based SaaS offering only, and is built on top of Salesforce.com technology. As a fully hosted offering, the system is typically deployed in under one week. Since it’s offered as software-as-a-service (SaaS), a web browser can be used to access the product. Therefore, it is accessible via any device running a web browser, including mobile devices, such as iPads and iPhones.

Aruvio is an audit-driven solution with modules available to test compliance, preliminary risk and risk assessment. There is a tool to quickly develop audits and workflows. All web-based, it uses email notification to users as a workflow engine for all audit and alerting functions. Role-based authentication controls display who has access to what features. Aruvio integrates regulatory compliance documents and consolidates inputs. Users can upload company-specific policy, standard documents or use the pre-loaded common control framework that comes from integrating to the Unified Compliance Framework (UCF). The seamless integration between frameworks and internal standards helps avoid redundant control testing with “test once, report many.”

Assets and vulnerabilities can be imported from various configuration management databases (CMDB) and vulnerability scanners using an easy-to-use data loader interface. Once loaded, users can perform risk assessment of identified vulnerabilities and threats by assets. There is an asset wizard to create assets as well. From what we saw, asset creation looked to be manual. This can be a pro and con: The positive being it is easy to roll up assets to “systems,” and the negative being there will be some setup time.

There is a policy module as well. One creates policies outside of the tool and upload them as PDF files. Further, there is a useful feature that allows one to create the training on the policy and track that adherence, as well as a read-and-accept audit-tracking feature. Users can deploy the data from the policy tool to map policies to controls, and then measure and report on compliance under one’s risk assessment. Also, there is a vendor risk module that allows admins to set up white-labeled and branded portals to deliver and track vendor assessments for inclusion in one’s risk reporting. It appeared to be more of a manual process to get all the data in, but that said, there are data imports that are easy to use.

Reporting and dashboard capabilities are well done. Users have numerous reports and views out of the box and one can customize any of these as desired. The dashboards are easy to use and it is simple and quick to get to the detailed data. One can look at a risk profile as a whole or quickly click to a view of risk by any regulatory type – i.e., quickly see a risk profile for just PCI DSS.

Support is included in the yearly subscription fee and includes 24/7 phone and email access. There is not a web-based support option. – ML
Citicus ONE vR.35

Citicus ONE is an integrated system for organizations to automate their IT governance, risk and compliance management processes. The tool uses an asset-based risk assessment approach. Citicus ONE can be used as an efficient, constructive and continuous method of measuring and managing information risk and other areas of operational risk—across an enterprise. It can be used to conduct tens, hundreds or thousands of risk evaluations, and keep them up to date efficiently.

The tool is available as both installable software and as an in-the-cloud, hosted service. The on-premise solution is supported on MS Windows Server 2003 or above, MS SQL Server 2005 or 2008, and requires .NET 3.5. For user management, the on-premise solution is fully integrated with Active Directory. Assessments deliver evaluation results that create individual “issues” or “action plans” for follow-up or remediation activities. Assets can be imported via a simple object access protocol (SOAP)-based web service from configuration management database (CMDB) tools or other data sources. Citicus ONE will help link issues with action items to establish the required control improvements to remediate or manage risk. Interdependencies between assets can be recorded so that risk dependencies can be tracked. There is a workflow/remediation capability under its “issues” section to assist with this effort.

The user interface (UI) makes it easy to configure the control assessment framework using one’s own local security policies and regulations, or one can use the built-in control libraries covering areas such as ISO 27001, PCI DSS, Information Security Forum’s Standard of Good Practice (ISF SoGP), NIST, vendor assessment/third-party, party physical security and SCADA requirements. The process is completely UI driven with no coding necessary. A simple pull-down menu drives the entire process. Remediation planning is supported through recording risk and compliance “issues” and the specific action required to resolve these. Actions can then be assigned to individuals, budgeted and tracked to completion. The completion of remediation activity automatically updates compliance and risk ratings. As well, incident-reporting templates are available and can be customized to one’s needs. Using remediation and incident management tools, one can quickly automate the linking of actions to specific controls. Users can generate a risk scorecard by asset.

Reporting is a strength of this product. It is role-based, so it’s easy to deliver an executive dashboard or a more detail-based homescreen for an analyst. Reports are largely graphical and interactive. The visualization capabilities of the product are well done.

New features in v3.5 include an automated workflow capability for assessment and remediation functions. Also new are analytics to provide a prediction of likelihood of incidents. The prediction capability does not deliver a risk number, but rather a ranking based on the status of various controls.

The documentation is integrated with the software and is clearly laid out. Standard 10-hours-a-day/five-days-a-week phone, email and web support is included in the first-year price and is 18 percent thereafter. There are no other levels of support available beyond standard. – ML

FireMon Security Manager with Risk Analyzer and Policy Planner

The FireMon Security Manager with Risk Analyzer and Policy Planner modules offers comprehensive network security management, including firewall and router risk analysis, policy compliance auditing, change management and risk analysis. This product features tools that allow administrators and security professionals to analyze the entire network infrastructure through visualization. This provides an easy and intuitive way to see where possible risks and weak points may be found in the network so that they can be assessed quickly before they become a bigger problem. This solution also offers fully integrated change management and rule cleanup capabilities, as well as remediation recommendations and ongoing change monitoring.

We found the initial setup and configuration of this appliance to be quite simple. We had the appliance up and running within minutes of turning it on. The first step of the installation is to connect a monitor and keyboard to the appliance and power it on. Once we powered on the appliance for the first time, we were greeted with a short setup wizard. This wizard allowed us to configure all the initial settings of the appliance, including IP and network settings. Once we completed the setup wizard, we were able to access the appliance through the Security Manager GUI client application for all configuration and management.

Once in the management interface we noticed the true power of this product. To start, the interface is elegantly designed and quite intuitive to navigate. We found it easy to add devices and begin the process of analysis. We also found this product to include a multitude of automation and visual analysis capabilities. Overall, we found this product to be quite comprehensive in features and functionality for complete policy management.

Documentation provided with this product includes quick-start, getting-started, administrator’s, and user’s guides. The getting-started and quick-start guides provide the necessary steps to get the appliance up and running in the network, as well as some basic configuration steps. The administrator’s guide provides more installation and configuration detail, as well as detailed descriptions of the product features and functions. We find all these guides to complement each other nicely and to be well-organized and easy to follow with clear instructions, detail and screen shots.

FireMon offers silver and gold support levels to customers as part of an ongoing support and maintenance program. Each option includes various levels of phone- and email-based technical aid, as well as access to an online portal. Customers accessing this portal can find many resources, including product updates and upgrade downloads and a knowledge base.

As a price of $25,000 for the hardware, software and licensing, this product may seem a bit pricey for some organizations, but we find this price tag is reasonable overall. This product includes a lot of functionality for the price. With the FireMon Security Manager with Risk Analyzer and Policy Planner in place, organizations can not only find and remediate risk points, but easily manage ongoing security policy and policy change. – MS
LockPath Keylight v3.0

The LockPath Keylight platform is a family of applications that includes management of compliance, threats, risks, vendors, incidents and business continuity. The platform is centrally managed and has a single sign-on system with configurable permissions that allow multiple users to manage different aspects of the system.

The tool is delivered either as a cloud-based SaaS offering or as an on-premise solution. The SaaS model simply requires a modern browser and internet access. The on-premise offering is built on the Microsoft platform, using .Net and C# with SQL as the backend database. We were told that a typical deployment can be installed and configured for use in 30 days.

Keylight’s Risk Manager provides a comprehensive set of tools to identify, assess and prioritize the most relevant risks for an organization. Risks are captured from multiple sources, including user entry, compliance, policy and risk assessments, and integration to network and security devices. Keylight has a substantial list of built-in connectors for plugging into network and security products. The Threat Manager provides vulnerability remediation, and it also has the ability to integrate with several vulnerability scanners, including products from Qualys, Nessus and Rapid7.

Once risks are captured, Keylight includes a configurable workflow engine that can move risks between individuals and groups. This is configured through a menu-driven wizard and requires no custom code. The same workflow tool is integrated through the entire product suite. The Dynamic Content Framework allows users to customize all the risk elements and to even create custom risk types. Users also have the ability to cross-relate objects from all applications, such as policy to a risk, or a risk to a business continuity plan.

The offering has a questionnaire-driven compliance module. These templates are easy to create and customize right down to custom scoring with the ability to flag questions and route them through additional workflows, such as a mandated review process, etc. Keylight also includes a full policy management suite, which offers the ability to import or build policies, move policies through a configurable workflow process, and relate policies to regulations within a content library. Another module, Incident Management, is also fully integrated and uses the same email-driven workflow described above. We were not provided with a lot of detail on the Business Continuity Manager, but wanted to mention that it offers the ability to generate, test and report on business continuity planning (BCP) readiness. There is also a Vendor Management module for extending assessments to vendor partners.

The reporting capabilities of Keylight are strong. All the reports are created through a simple, drag-and-drop interface. Everything is available to report on: risk objects, policy exceptions, drilling of a risk to a policy exception, etc. The heap map view is one of the better visuals we saw in our Group Test review process this month.

Support is included in the license price, but there is only one option: eight-hours-a-day/five-days-a-week. Users can contact assistance via phone, web or email. Documentation is built in as online help, which is well done. – ML

Lumension Risk Manager v4.4

Lumension Risk Manager (LRM) is a compliance and risk management solution that provides a framework for streamlining compliance management and assessing business risk. It provides visibility into compliance and risk through four capabilities: risk profiling, controls framework, assessment and risk/compliance reporting.

The solution is delivered as on-premise software running on one’s hardware. It is a Java-based web application running on a Microsoft Windows Server that can be viewed on any MS Windows-compliant device. LRM deploys on Windows 2005-2008 and SQL Server 2005 through 2008 R2.

The product is designed as a compliance and business risk assessment tool, combining compliance and risk management into a single process. It is geared to providing end-to-end visibility of all control activities needed to ensure protection of information. It harmonizes common controls from more than 450 regulatory standards into a single set of controls, thus easing the burden and duplication inherent in manual compliance management practices.

To assist in managing the raw amount of data associated with each of these, LRM analyzes the data and puts it into a category of meaningful, neutral or less meaningful. Each of these can be assigned a custom risk value that rolls up into the final risk calculation.

Lumension provides both standard and premium support options as part of its subscription cost of the software. Standard options include 8 a.m. to 5 p.m. phone-based technical aid, along with email assistance with one-day response.

Support is included for a fee and includes 24/5 live phone support. – ML
ManageEngine DeviceExpert v5.9

DeviceExpert from ManageEngine provides a comprehensive approach to network configuration and change and compliance management. This product features the tools needed to analyze and monitor changes to the many devices in the environment, prevent unauthorized changes, define policy and validate that systems are meeting policy and compliance requirements. DeviceExpert includes support for almost any switch, router or firewall, which ensures that all devices in the environment can be analyzed from one easy-to-use console.

We found this solution to be an easy install overall. It comes as a simple executable installation package that can be installed on Microsoft Windows or Linux machines. We installed it on Windows Server 2008 and had no trouble getting it installed and up and running quickly. After a short installation wizard, the product was installed – along with all the necessary components needed – and we were able to navigate to the web-based management interface. Overall, we found the interface to be easy to navigate and to have a clean layout. We also found it easy to add devices and manage policy directly in the interface. For the initial configuration of the product, devices can be added in bulk using the device discovery feature, which makes deployment quick and easy.

We find this product to be quite comprehensive in the way of features and functionality. The first thing we noticed when we started using this product is its well-organized dashboard. The “home” tab of the management interface features a dashboard that shows a well-detailed, bird’s-eye view of the latest configurations, changes, policy violations and compliance overviews, among other charts and graphs. This dashboard provides a good starting place to bring the environment into compliance and manage risk. Aside from the dashboard, we also found it easy to view inventory and run compliance reports. This product also features a fair amount of configurable automation of tasks, such as deploying changes across multiple devices in the network using configuration templates.

Documentation provided with this product includes a single help manual. We find this short help manual to be adequate in detail and to include clear, step-by-step configuration instructions, but there are no screen shots or configuration examples to help clarify configuration steps. This guide provides a good overview of the product configuration, but we would like to see more detail.

ManageEngine offers 24/7 phone and email support to all customers during the 30-day evaluation of the product. After evaluation, customers can purchase additional support through an annual package. Also available to customers is a large online aid area, which includes access to many resources, such as a knowledge base, user forums, videos, tutorials and product documentation.

With a price starting at $795 for a 10-device license and going up to $14,995 for up to 2,000 devices, we find this product to be an excellent value for the money. While DeviceExpert does require extra hardware cost, we find that its low price point for less devices makes it cost-effective for smaller organizations looking for solid network device policy management and compliance without the high cost of other options. – MS

McAfee Total Protection for Compliance v7.x

McAfee Total Protection (ToPS) for Compliance reduces remediation time from months to days by providing unique, countermeasure-aware, impact/risk assessment capabilities. The tool correlates endpoint and network countermeasures with new vulnerabilities and provides a third dimension to the vulnerability impact assessment by adding the status of the current countermeasure to vulnerability severity and asset criticality. It enables organizations to conduct (agent-less, agent-based or hybrid) compliance audits, configuration assessment, vulnerability assessment, asset management and countermeasure-aware risk assessment for a range of technologies.

It runs on a Microsoft platform and requires MS Server 2003-2008 and SQL Server 2005-2008. A spokesperson at the company claimed deployment of the software was within a few hours. Certainly, users can be up and running within a few days depending on the level of customization, workflow complexity and integration with non-McAfee products.

The solution addresses risk at the IT risk level using the OVAL (open vulnerability and assessment language) standard for risk assessment. ToPS proactively correlates threats with state system information – including vulnerability data, patch level, configuration information, application data and countermeasure information – to find critical assets at risk so as to optimize remediation/patch efforts.

The agentless option allows users to gather valuable information from systems with zero footprint on those devices. The agent-based, agentless or hybrid collectors can co-exist in the same environment so one has numerous deployment options. New to this release is the ability to assess desktops, such as Adobe and Java-based threats. ToPS has also added the ability to conduct file integrity checks to recognize changes made, to report and track changes, and to specify entitlement to certain files. Other additions to this release that caught our attention include the ability to now track risk associated with BYOD devices and endpoints. ToPS has also added the ability to conduct file integrity checks to recognize changes made, to report and track changes, and to specify entitlement to certain files. Other additions to this release that caught our attention include the ability to now track risk associated with BYOD devices and endpoints.

McAfee, an Intel company

Vendor: McAfee, an Intel company
Price: Ranges from $16.38 to $105.54 per node based on the number of nodes
Contact: mcafee.com

Features: Reporting/disk-free, agentless capabilities, mobile-device support
Weaknesses: Still a stronger solution in a pure McAfee environment, but getting better. Still, with all the modules it can be pricey for a larger deployment
Verdict: Strong IT risk management tool with some innovative capabilities.

GROUP TEST | Risk & policy management

GROUP TEST | Risk & policy management

CONTACT DETAILS
Vendor: ManageEngine
Price: Starting at $795
Contact: manageengine.com
Features: Ease of use ★★★★★, Performance ★★★★½, Documentation ★★★, Support ★★★★½, Value for money ★★★★★
OVERALL RATING: ★★★★★

Strengths: Low cost and easy to deploy.
Weaknesses: Documentation could be more detailed.
Verdict: Excellent price point, even with the extra hardware needed; but, weak in documentation for smaller organizations without a lot of technical resources.

CONTACT DETAILS
Vendor: McAfee, an Intel company
Price: Ranges from $16.38 to $105.54 per node based on the number of nodes
Contact: mcafee.com
Features: Ease of use ★★★★★, Performance ★★★★★, Documentation ★★★★★, Support ★★★★★, Value for money ★★★★★
OVERALL RATING: ★★★★★

Strengths: Reporting/disk-free, agentless capabilities, mobile-device support.
Weaknesses: Still a stronger solution in a pure McAfee environment, but getting better. Still, with all the modules it can be pricey for a larger deployment.
Verdict: Strong IT risk management tool with some innovative capabilities.
Modulo Risk Manager v8.1

Modulo Risk Manager is a single, fully integrated platform for organizations to automate and unify their IT governance, risk and compliance (GRC) processes. Based on an intuitive and flexible workflow, the tool enables organizations to identify, analyze, evaluate and treat risks across the enterprise. By mapping IT and non-IT assets to business processes, Modulo adds business relevance to operational data for risk-based analytics and decision making.

It is offered as both a hosted SaaS solution or as an on-premise software deployment. The on-premise offering has two licensing models: perpetual (the user buys it) or subscription (user’s hardware, license rented). The on-premise solution requires MS Server 2008 R2 64-bit, .NET Framework 3.5 and MS SQL Server R2 Standard Edition 64-bit. The web server has similar Windows requirements, and further needs.Net 4.0 and a valid SSL digital certificate.

The offering manages risk, policy and compliance with multiple regulations, internal policies and standards. The MetaFramework is aligned with ISO 31000 and delivers a substantial knowledge base to reference. The solution includes the five core domain modules: management of risk, compliance, policy, workflow and knowledge.

The solution has vast support for integrating data from many directory, network, security, vulnerability and asset management systems. Enhanced in this version is an innovative, open way to automate the collection of information from third-party devices through its open source GRC collectors, dubbed modSIC, for Modular Open Distributed SCP (security content automation protocol) Infrastructure Collector. modSIC provides a common platform for developing a service to collect and analyze technology assets based on the open SCAP standard. Data can be collected based on a custom model or by using public knowledge bases through OVAL (open vulnerability and assessment language).

There are several new features to the product in v8.1, the most notable of which is an automated workflow component. The tool moves tasks through the entire risk process. There are also options for incident management with a strong tree mapping style report. The vendor risk and business continuity management (BCM) functions are new. This module provides an efficient integration capability to easily link one’s risk to the business continuity plan for the organization, including operational, financial and regulatory. With a new social integration capability, one can also collect social data and measure image impact.

Reporting and visual representation of the information is strong. Tools, such as tree maps and geo mapping, have been enhanced. Plus, there are effective “what if” tools available. New to this version too is a Big Data management feature, and the delivery of more predictive analytics. However, the real strength of this tool is the correlation and visualization of the massive amount of collected data into a manageable and usable format.

Eight-hours-a-day/five-days-a-week standard support is included for the first year. There are premium support options available for a 20 percent fee for both the SaaS and software versions. These are available either by phone, email or web. – MI

NetIQ Secure Configuration Manager v5.9

Secure Configuration Manager from NetIQ provides a feature-rich platform for monitoring and ensuring policy compliance throughout the entire network environment. This product can provide management and monitoring of many systems throughout the network, including Microsoft Windows systems, Linux, Unix, VMware ESX, databases, web servers running internet information services (IIS), and network-attached storage. The tool can help administrators easily detect and remediate systems that are out of configuration compliance based on risk and security, which ensures that critical systems stay safe and within requirements.

Installation and deployment is quite a process, as we found last year. Not much has changed in getting all the components of this product set up and running. The initial installation is comprised of getting a Windows Server 2008 R2 installation running with Microsoft SQL Server 2008 R2 and IIS. After the server is ready and loaded with a couple other prerequisites, the installation of Secure Configuration Manger can begin. We did find that once the server is properly prepared, the overall installation of the product is quite straightforward and is well automated.

After installation was complete, we were able to easily access the management console and begin configuring the product. Overall, we had an easy time of configuring the various features and functions, and – as in years past – we were still quite impressed with the layout and organization of the many dashboards, visual charts and graphs that help to easily find and remediate problem areas or systems out of compliance. This product comes fully loaded with many compliance-based reporting templates ready to go out of the box. We like the added functionality of being able to find and report on user privileges to certain systems to ensure that all entitlements are up to date and correctly provisioned.

Documentation provided with this product includes a few guides in PDF format. Among the guides are an installation guide that details the installation and initial configuration steps in a clear and well-organized format. We find all documentation to provide a good amount of detail and step-by-step instructions, but would have liked to see more visuals, especially for more advanced configuration tasks.

NetIQ provides basic support at no cost with the purchase. Customers can purchase additional assistance through a support and maintenance program. Additional support available includes essential and premium levels at 12/7 and 24/7, respectively. Support options included phone- and email-based technical aid, as well as access to an online area which includes many resources, such as a knowledge base and product documentation downloads.

Secure Configuration Manager is priced based on a per-server software license model. Pricing starts at $1,200 per server. We find this product to be an excellent value for the money overall. While it does require a little bit more work on the front end to get everything up and running, we find that the features and capabilities of this solution are well worth the effort. – MS
New Net Technologies
Change Tracker Enterprise

Change Tracker Enterprise from New Net Technologies offers full change and policy compliance management and monitoring. With this product, administrators can easily audit and monitor changes throughout the entire IT infrastructure, including Microsoft Windows systems, Linux, Unix, network devices and firewalls. Administrators can also establish a baseline known good state, and Change Tracker will help pinpoint systems out of compliance and recommend the necessary remediation.

We found installation of this product to be simple, but not as straightforward as running an executable. There are quite a few steps that need to be done to the server before actually installing the product to then prepare the server and server services. This product is installed on a Microsoft Windows system, which can be either Windows 7 or Server 2008 running IIS version 7, and with the .NET Framework installed along with SQL Server 2008. Once we had all the software prerequisites installed, we had to go through a few steps to configure the services, such as IIS. After those few simple steps were completed, we were able to install the product itself, which actually went quite quickly as we were guided by a short setup wizard. Once the product is installed, all further configuration and management is done via a well-organized and intuitive management console.

This product offers a lot in the way of features and functionality. Change Tracker Enterprise can be used on its own or integrated into Log Tracker Enterprise for added SIEM capability. By itself, Change Tracker Enterprise can be used to help administrators and security professionals with vulnerability and hardening of systems, file integrity monitoring, and change and configuration management. All these functions are well integrated into a monitoring and reporting engine that can help maintain compliance across the environment.

Documentation provided with this product includes a full administrator’s guide in PDF format. This is available in the program folder after installation is complete. We find this guide to be nicely organized and easy to follow with many step-by-step instructions, screen shots and configuration examples. Other than the administrator’s guide, we were only provided a short review.s guide for installation purposes. While this short guide did help us start and get the product installed, we would have liked to see a full installation guide with a bit more detail.

New Net Technologies offers limited assistance at no cost to clients. Customers needing more robust support can purchase a plan as part of an ongoing maintenance cost. There are several support levels available to customers. Customers can also access a large aid area online that includes a knowledge base and many other resources.

At a price of $2,200 out the door for software and licensing, we find this product to be an excellent value for the money. New Net Technologies Change Tracker Enterprise offers many change and policy management features at a reasonable price for almost any size organization. – MS

GROUP TEST | Risk & policy management

Promisec Endpoint Manager

Promisec Endpoint Manager is a full-scale policy and endpoint management platform that allows administrators to inspect, monitor and enforce configuration and compliance policy across the entire IT environment from one easy-to-manage console. With this product, administrators can define a policy for Microsoft Windows, Linux, Unix, Mac and Android devices on the network, and ensure that compliance to the security policy is adhered to.

We found this product to be a simple install as it did not take us long at all to get it up and running. The first thing we had to do was install the Endpoint Manager server on a Windows Server machine. The installation of the server management console was quick, guided by a short setup wizard that was easy to follow. After the server software was installed, we were able to access the intuitive management console to begin configuring the product and our policy. Our overall experience with the management console was good, and we felt comfortable navigating around and configuring policy right after our first login.

One of the main features of this product that we found to be most important was the granularity of the configurable settings for the policies. From a single console, we were able to define various hardware and software policies and assign them to various areas of the environment – all based on a simple network scan and discovery. Once we found the systems in the network, we were able to easily apply a policy and scan the system for compliance to the policy. If the system did not meet our policy, we were given remediation options to bring the system into compliance. As an added benefit, we were able to get a full inventory of our systems – both at the hardware and software level – which helps to manage systems and licensing requirements.

Documentation provided with this product includes an installation guide, as well as a full user guide. The installation guide provides an excellent amount of detail and installation steps to get the product up and running with an initial configuration, as well as some brief feature introductions. The user guide goes more in-depth and provides much more detail on advanced configuration of features and policies. We found all documentation to include many clear step-by-step instructions, configuration examples and screen shots.

Promisec does offer no-cost, eight-hours-a day/five days a week phone and email-based technical support to all customers. Unfortunately, that is the extent of the assistance offered – there is no 24/7 option available. Also missing from the Promisec support portfolio is an online aid area. We find online support to be invaluable when technical support is not available and an administrator is trying to solve a problem. We hope to see more options available from Promisec in the future.

Promisec Endpoint Manager starts at $14 per endpoint up to 1,000 endpoints, based on a yearly subscription. We find this product to be an average value for money based on overall cost of ownership. While this product does provide a lot of features and functionality, it can be quite costly on an ongoing basis overall. – MS
RedSeal 6 Platform v6.6

RedSeal 6 Platform is a risk-based IT security management platform that enables organizations to identify, prioritize and respond to critical points of weakness in complex enterprise security control infrastructure. RedSeal accomplishes this through modeling enterprise network assets (i.e., routers, hosts, applications, etc.) and the security control/remediation infrastructure (firewalls, etc.) that protect those assets. The tool uses risk analytics to examine the model to identify high concentrations of risk and non-compliance. These analytics provide risk managers with the information needed to drive planning and prioritized action that systematically reduces exposure to cyber attack.

The product is delivered as either software running on a general purpose server or as a pre-loaded appliance. The appliance OS is Linux-based. RedSeal software runs on a Microsoft platform and requires Windows Server 2003-2008. RedSeal uses a Postgres database for its backend data store.

The tool is designed to continuously identify and prioritize key points of weakness in one's enterprise security controls. RedSeal models configurations from data collected from network devices – such as firewall, UTM devices, routers, load balancer and wireless controllers. It can also model data from vulnerability information pulled from several leading scanner vendors, and can pull security data from supported SIEM vendors. RedSeal can collect device configuration data from the leading configuration management databases (CMDBs). Through the collection of this data, one can automatically create needed asset pools. More importantly, users instantly can build a detailed network map with a visual of how things are attached in the enterprise, and what is reachable based on configured policies. This high-level overview of connectivity and reachability is a key strength for this product.

Admins can model attack simulations and determine how threats might propagate through the environment, and can model changes to see what new vulnerabilities or threats are exposed. There is a new, winning feature in this release that uses analytics and creates groupings to easily show graphically where users may have gaps in network controls or unknown access based on policies. RedSeal does not supply a regulatory or standards policy library, but that information is mapped in the backend so that users can create risk maps and reports for compliance against such standards as PCI and NIST.

Another new component is the change management workflow. This addresses risk assessment, what-if analysis, security oversight and continuous monitoring. There is additional support for BYOD risk from collecting information on mobile devices.

The reporting and visualization capabilities are powerful while remaining easy to use. Admins have high-level executive dashboards delivering key decision-making information to leverage investments based on risk. The analyst capabilities are superb and include recommendations for best practice configuration and remediation.

Support is fee based and includes options for 24/7, four-hour or one-hour response. Support is available via phone, email and web-based options. Fees for support start at 20 percent of appliance or license fees. – ML

RSA Archer GRC Platform 5.3 SP1

RSA Archer’s Risk Manager is part of an enterprise GRC product portfolio sold and licensed as modules: audit, policy, risk, compliance, enterprise, incident, vendor, threat and business continuity management.

It is composed of three logical tiers—interface, application and database—that are deployed on two physical tiers. The platform itself is deployed on two physical tiers that can be hosted on one physical server or deployed across multiple servers. This includes the web tier and the database tier. In a single host configuration, the platform requires an OS with Windows 2003 Server with SP1 or later, Windows Server 2008 or Windows Server 2008 R2 Standard, Enterprise, or Datacenter editions. SQL Server 2005 SP3 or later, SQL Server 2008, or SQL Server 2008 R2 X64 editions of SQL Server are recommended. The product is scalable for large, enterprise-class deployments.

The risk module can be used standalone, but, in reality, users will want to deploy it in conjunction with the enterprise management (asset tool), incident management and threat management modules for a complete view of risk. We reviewed the policy, risk and threat management modules.

The policy module comes out of the box with a wealth of content supporting popular regulatory and standards, as well as content for best practice controls. Assessment questions are either based on industry-defined compliance questionnaires, such as fraud (Red Flags), standard information gathering (SIGIC), PCI DSS, or tailored to specific authoritative sources, such as COBIT. These questions can streamline the process for defining appropriate compliance content, and they are easily tied back to one’s internal standards. New in this version is the ability to add cost measurements to individual controls, so that users can now map individual control costs to the risk exposure. RSA Archer Risk Management Module enables users to proactively risks to reputation, finances, operations and IT infrastructure as part of a governance, risk management and compliance program. Archer takes both a qualitative and quantitative approach to risk.

The risk module is assessment driven. Assets can be imported from integrations with supported vulnerability, configuration management database (CMDB) or data leakage prevention (DLP) vendors, or from third-party sources via an API-like data feed manager. The Threat Management Module is updated in this release and has a built-in threat methodology to deliver threat assessments built on ISO and NIST. Vulnerability data comes in from industry sources and correlates to assessment data to deliver remediation recommendations.

The report-building interface is solid and provides users with configurable dashboards. The product employs a common data module across all its modules, so reporting, workflow and alerting for all functions work the same. We were shown one screen that had a clean, roll-up view of every module summary, i.e., compliance, incident management, vendor risk, risk, threat and status overviews. Basic support is included with the product purchase and provides eight-hour-a-day/five-days-a-week access. Enhanced assistance is available for a 25 percent fee based on the license price and provides 24/7 access and priority response. – ML
Rsam GRC v8

Rsam GRC v8 is a platform for risk management and security risk intelligence enabling organizations to perform risk assessments, manage compliance, threats and vulnerabilities, policies, remediation activities, issues, incidents and more. Rsam differentiates itself from traditional GRC platforms by focusing more on proactive enterprise risk management (ERM).

The tool is offered either as an in-the-cloud SaaS offering or as a customer on-premise software. It runs on Windows Server 2003/2008 with SQL database backend, IIS and .NET Framework. One can deploy the product on virtual machines, shared environments, clustered environments or standalone servers.

The modules that are part of the suite include: risk, compliance, remediation, threats/vulnerabilities, audit, incident management, policy and vendor risk. These components are all rolled into the risk analytics engine. Modules are licensed separately. There is a brand new user interface in this version – clean and easy to follow – with tabs across the top for the various modules and navigation panes below.

Rsam provides a fully automated policy management lifecycle. In Rsam, policy structures support unlimited hierarchical levels and policies can be authored directly in Rsam or imported from Word, Excel, databases or web API calls. As well, policies can be linked to Rsam’s robust content library, encompassing 10,000-plus, road-tested controls, which are carefully cross-mapped across compliance/industry standards, such as ISO 27002, FFIEC, GLBA, NIST, COBIT, HIPAA, PCI and SOX. Form-driven menus drive users through the assessment creation process and one has an automated workflow to move, measure and manage the assessment through the process. The data gathering and bulk management of the information is impressive.

The risk analytics module creates dynamic rules that maximize management of policies, risks and findings. Customers can define their own custom risk-driven rule sets. The output of the assessments, threat and vulnerability imports generates “findings.”

Getting data into Rsam has been enhanced in this release. The tool’s universal connector is data-source agnostic and allows customers to integrate data from other existing tools without waiting for Rsam to establish a formal relationship with that third-party product. The universal connector integrates with just about any other tool, either via direct API calls, database queries, file exchanges or simple SMTP messaging.

Also, there are numerous out-of-the-box risk management reports, plus a tool for creating custom dashboards. The new dashboards are solid. Also new are capabilities for universal and metrics search that allow for the scheduling of a function to be run and posted to a dashboard.

The built-in documentation and help function is done well. Training, a knowledge base and help guides have all been updated. Rsam annual support and maintenance comes in at 20 percent of software license fees. Technical support is provided via phone, email and WebEx. Support hours are 8 a.m. to 8 p.m. EST. Assistance includes updates/upgrades to Rsam software and content templates. – MI.

Skybox Security View Enterprise Suite v6.5

Skybox Security View Enterprise Suite v6.5 is a complete portfolio of proactive security risk management solutions that automatically finds and prioritizes risks and drives remediation. The offering delivers proactive security risk management solutions to prevent cyber attacks and data breaches and maintain IT compliance. The suite enables continuous monitoring of security controls, vulnerabilities and risks, and includes predictive analytics to proactively assess the risk of attacks, and deliver intelligent, actionable security recommendations to make existing defenses more effective.

The solution is delivered as on-premise software or as an appliance. It is usually deployed in a three-tier architecture with one or more data collectors, a centralized server and a management interface. It is typically deployed as an enterprise software solution, a preconfigured hardened appliance or run as a VM on either Windows or Linux operating systems.

The product is designed to bring the human element back into security and risk, which is a good thing. Skybox delineates the network security controls by mapping the network, gathering configuration information and looking for compliance in those configurations. To provide complete visibility of the security infrastructure, the tool builds a virtual model of the network by importing configuration logs and relevant data from firewalls, routers, intrusion prevention system (IPS), vulnerability scanner and patch management systems. Skybox Security integrates directly with more than 70 network devices, management systems and threat information services. Additional device integration is provided through the platform’s open API. This integration also supports the vulnerability discovery function. Skybox also houses roughly 37,000 vulnerabilities in its threat dictionary.

There is an integrated change management capability that ties directly into the ticketing system workflow. One has the ability to run “what if” analysis against policy or configuration changes, and can see a reachability report resulting from the proposed changes. There is some programming that goes into building out the ticketing system templates to support the feature. In addition, a scan-less vulnerability detection feature gives users an option to gather data without agents. The “attack simulation toll” is a clever feature, allowing the analyst to do a real-time risk analysis with a visual representation of the possible attack points and progression of the threat.

Reporting is done well with template and custom report capabilities. The network mapping tools are effective as a visual and allow for drilldown into specific devices and rules that tie to risks. There is an “attack explorer” option that allows users to research from where a threat/attack could come and then test and map out paths to see where it might reach. This tool provides the information needed to remediate potential threats before they actually occur.

There are two levels of support available: eight-hours-a-day/five-days-a-week and 24/7. The pricing is $18 and 28 percent of net license and hardware price. Both choices include phone, email and website options. – MI.

**GROUP TEST | Risk & policy management**

**Vendor** Rsam

**Price** $20,000 annual subscription or $50,000 perpetual license.

**Contact** rsam.com

<table>
<thead>
<tr>
<th>Features</th>
<th>★★★★☆</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Performance</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Documentation</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Support</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Value for money</td>
<td>★★★★☆</td>
</tr>
</tbody>
</table>

**Strengths**
- Strong assessment and workflow tool set
- Strong data import abilities
- Universal risk taxonomy

**Weaknesses** None noted.

**Verdict** Enterprise risk management (ERM) approach is solid, and consolidates, prioritizes and visualizes risk in an ongoing model.

**GROUP TEST | Risk & policy management**

**Vendor** Skybox Security View Enterprise Suite v6.5

**Price** Starts at $15,000

**Contact** skyboxsecurity.com

<table>
<thead>
<tr>
<th>Features</th>
<th>★★★★☆</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Performance</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Documentation</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Support</td>
<td>★★★★☆</td>
</tr>
<tr>
<td>Value for money</td>
<td>★★★★☆</td>
</tr>
</tbody>
</table>

**Overall Rating** ★★★★★☆

**Strengths**
- Substantial attack explorer tool
- Great analyst tool set
- Risk dashboard

**Weaknesses**
- A bit light on compliance content.

**Verdict** This solution will actually give analysts the resources and, more importantly, the time to focus on finding and mitigating risk.
**SolarWinds Patch Manager and Firewall Security Manager**

Patch Manager and Firewall Security Manager from SolarWinds are two products that can be used together by administrators and security professionals to achieve a full picture of system patch policy and firewall policy auditing. Patch Manager features a large catalogue of third-party software that is updated consistently to work in tandem with solutions such as Microsoft Windows Update Services. Firewall Security Manager provides the ability to analyze and audit firewall security policy, and ensure that firewalls are compliant with organization policy, as well as secure.

We found both of these products to be easy to install and configure. Installation files for both had to be downloaded from the SolarWinds Customer Portal. Once we had all the necessary files downloaded, we were able to start the installation. To install Firewall Security Manager, we had to run the setup executable on our Windows Server. After a short installation wizard, we had the product installed and were able to launch the client application to begin managing our firewalls. Patch Manager was a similar install.

Overall, we found both products to be quite easy to use and manage. We also found them to have an abundance of on-board features, as well as extendable features through integration with other products or applications. For example, Firewall Configuration Manager can integrate directly into Network Configuration Manager from SolarWinds to extend configuration management capabilities to include more auditing and compliance reporting, as well as change management and automation. Patch Manager also can integrate directly into Microsoft System Center Configuration Manager to streamline updates and patch management across the entire Microsoft infrastructure. While the integration of these products into others is great, they also stand on their own quite well and do not require other products to be good tools.

Documentation includes installation and administrator guides in PDF format. We find all the documentation to be well organized and easy to follow with many step-by-step instructions for installation, configuration and integration. However, we did find the documentation to lack clear screenshots and visuals, which could have better illustrated more complicated configuration steps.

SolarWinds offers customers a solid combination of no-cost and fee-based support options. All customers receive the first year of technical support as part of the purchase price of the product. After the first year, customers can choose to purchase additional technical support through an annual agreement for a fee. Customers also have access – at no cost – to a large online community, as well as documentation downloads and other resources.

With prices starting at around $3,000 for Patch Manager and $1,300 for Firewall Security, we find these products a good value for money overall. However, for some environments the value can go way up if some of the tools that can integrate with these products are already available. We find the true value in both of these products is how well they can integrate and add a large amount of functionality to other products. – MS

**Symantec Control Compliance Suite v11**

Symantec Control Compliance Suite (CCS) automates key IT risk and compliance management tasks. It is an integrated solution comprising several different modules, including security, risk, policy, assessment and vendor risk management. Users can deploy a combination of these modules to meet business objectives. The CCS risk approach includes a definition of a business asset that one wants to manage, understand the IT risk for this asset, prioritize remediation based on IT risk, and then monitor risk reduction.

CCS Risk Manager is a new module that allows users to create a view of IT risk as it relates to a business asset – whether that is a business process, group or function. This piece provides the ability to define a virtual business asset that one can manage from an IT risk perspective. By grouping together all of the IT asset categories associated with one’s virtual business asset, the user can manage the composite risk associated with it. Risk can then be determined from assessment-driven results and vulnerability information.

The Policy Manager helps one plan for internal and external audits using more than 150 customizable policy templates, all mapped to centralized controls. Policy lifecycle management and policy-attestation tracking are all built into the module. The Assessment Manager delivers out-of-the-box content for multiple regulations, frameworks and best practices. Its content is based on an OWAL (open vulnerability and assessment language) model. Symantec also delivers content based on its own content team. Vulnerability Manager delivers end-to-end vulnerability assessment of web functions, databases, servers and other network devices. Additionally, CCS natively gathers security configuration data from server, database and application platforms. Data can also be consumed from external asset systems, including Active Directory, Altiris and other configuration management databases (CMDB). Third-party assessment data is ingested through External Data Integration and Connectors using comma-separated values (CSV), open database connectivity (ODBC), or web service connectivity. Advanced risk scoring allows users to differentiate between real and potential threats, ensuring the most critical and exploitable vulnerabilities are given priority when it comes to remediation efforts.

Dynamic dashboarding and reporting are updated in this release – and are well done. Risk and compliance scores roll up neatly, and the ability to move right from reporting into remediation workflows, controls review and risk scoring detail helps every level of user. The data framework and extensive controls library provide a normalized view of one’s data, and the analytics capabilities deliver valuable information to the reports and dashboards. One can move right from graphical views directly into the pivot-based detail, making it simple to research or interrogate the information.

No base support is included with the product. There are basic and essential assistance options available for purchase at 23 and 28 percent of the manufacturer’s suggested retail price. Support options are accessible via phone, email or web. – MI
Tripwire Enterprise and DataMart

Tripwire Enterprise and DataMart are two products that compose a suite for maintaining configuration states of servers, network devices and databases, as well as robust reporting services, to allow for deeper analysis of security and configuration policy. Tripwire Enterprise is a tool for full-service system configuration management that allows administrators to put a policy in place and have systems continuously checked against that policy to ensure compliance. DataMart is a way for administrators to collect information from various sources throughout the environment, including output from configuration and vulnerability management systems, and turn the data into a way of testing security policy changes through the use of dashboards and rich reports.

We found these products can be easily installed on the same server, and initial installation and setup does not take long at all. Both products include Windows and Linux installers for greater deployment flexibility. For our installation we chose to install both on a Windows server. The installation process is similar in both products, and is done by running an executable installer, which launches a brief setup wizard. At the completion of the setup wizard, all the components are installed and all further management is done via a web-based management interface. We found the interfaces to be well-organized with intuitive layouts.

We found Tripwire Enterprise to be more like three products in one, rather than just a simple system configuration management tool. It is built on three solid functions that include configuration management, file integrity monitoring and remediation. These three tools work together to provide a robust feature set. The Policy Manager function allows administrators to define policy and assess their configurations against any of more than 250 policies, standards, regulations and guidelines. Then, File Integrity Manager continually checks systems for unauthorized or unnecessary changes. Finally, Remediation Manager automates remediation and maintains compliance throughout the enterprise. Documentation includes both installation and administrator guides in PDF format. We find all documents to contain an excellent amount of detail and to be well-organized. Also included are many screen shots and configuration examples which help illustrate how to configure and use many of the features. Tripwire offers all customers basic, no-cost phone and email support with purchase. Customers requiring more options can purchase additional aid. The cost for premium support is based on the number of licenses purchased. All customers also have no-cost access to an online area that includes many resources, such as a knowledge base and user forum.

At a price starting at $18,000 for both Enterprise and DataMart, this product can be quite pricey for some environments. In this pricing model, however, DataMart takes up the bulk of the cost, so if data modeling is not a part of the overall strategy for an environment, the cost drops significantly. That said, DataMart does offer a lot of excellent capabilities for better security policy and overall security posture. We find this product to be a good value for the money for both medium and large organizations. – MS

Tufin Security Suite R-13-1

Tufin Security Suite is back again this year and, just as in years past, it has some great new features onboard. The Tufin Security Suite is comprised of the company’s two previous products, SecureTrack and SecureChange, and its newest offering, SecureApp. These all work together to streamline firewall, router and network infrastructure policy so that all rules are in order and compliant to the organization’s needs – without being redundant or limiting. This product is available as both a physical or virtual appliance and can integrate directly into any network environment due to the large breadth of supported products.

While this tool is quite powerful, it also requires quite a bit of configuration to do its job at the highest level. The initial setup of the appliance is done by simply connecting it to the network and accessing the web-based management console to launch the initial setup wizard. At the completion of the wizard, the appliance has all the network and initial configuration settings necessary to be up and running in the network. All further configuration and management is done via the web-based management console. This single console houses the various pieces of the suite, and it is easy jumping between the applications. We found the console to be easy and intuitive to navigate and to have an organized layout.

The high point of this product is the way that all the various parts of the suite are quite powerful by themselves, as well as together. The first component really is SecureTrack, which allows for full auditing and management of firewalls and routers throughout the entire network infrastructure. Using SecureTrack, administrators can easily find and eliminate non-compliant, broken or duplicate rules quickly and easily. SecureChange takes the audit one step further by provide change management and change workflows, as well as provisioning change throughout the enterprise as needed. The latest edition, SecureApp goes one step beyond that to automate application access and provisioning. This allows app designers and administrators to be able to ensure that an application gets the required access to the network it needs without sacrificing security.

Documentation includes a quick-start guide, as well as user guides for each of the three applications. The quick-start focuses on getting the appliance up and running in the network and the user guides provide all the necessary configuration information for the product features and functions. We found the documentation to be well-organized and to include clear instructions and screen shots. Tufin offers no-cost support to customers during business hours. Customers requiring 24/7 support can purchase premium assistance at an additional recurring cost. Customers can also access an online portal, which includes many resources, such as a knowledge base and product documentation downloads.

At a price of $45,000 for up to 10 managed applications, this product comes with quite the price tag. However, we rate it a solid value for the money based on its many advanced features and how well these are integrated. The Tufin Security Suite offers a robust feature set that can help streamline network infrastructure policy, along with allowing for new applications to be easily added without any worry that security is being compromised. – MS
Recently, SC Magazine published an article about a company called Path, which settled Federal Trade Commission charges that it violated the Children’s Online Privacy Protection Act. The FTC accused Path of collecting personal data from children without parental consent. Path agreed to pay a civil penalty of $800,000 as part of the settlement.

Although many app developers like Path have a privacy problem because their practices don’t match their policies, other app developers have a more fundamental problem – they have no privacy policy in place at all. Companies without a privacy policy are at risk for a lawsuit or government enforcement action. This is not a theoretical issue. Last December, California Attorney General Kamala Harris sued Delta Airlines in San Francisco Superior Court for allegedly failing to have a privacy policy for its mobile app, called Fly Delta. Her complaint claims Delta violated California’s Online Privacy Protection Act (OPPA), which requires commercial websites or online services that obtain personally identifiable information about state residents to post their privacy policies.

If your business is headquartered outside of California, you may be asking yourself why Harris’ suit based on a California law matters to you. The suit matters because her office (or class-action plaintiffs) can sue an app developer for allegedly violating OPPA as an unfair trade practice, even if they are out of state. Delta Airlines is a Delaware corporation with its headquarters in Atlanta. Harris sued in San Francisco, contending that Delta regularly did business in California and also violated the law there. By offering an app to Golden State residents without a privacy policy, Delta arguably injured the state’s residents and made it subject to suit in its courts.

If you sell mobile apps and you don’t have a privacy policy, now is the time to write and post one in a conspicuous place. Users should have a chance to review the policy before using the app. Also, your business should support the policy with more detailed practices and procedures. For instance, your business should conduct a periodic review of your privacy policy to make sure it continues to match your information practices. Companies like Path get into trouble when they don’t update their policies to match new marketing programs or app features that collect more or new kinds of personal data.

The California law also requires that the policy cover certain topics. An app’s privacy policy must identify: the categories of information collected by the app; the categories of businesses or individuals with whom the app provider may share the information; any means for the consumer to review and request changes to the information; the process to notify consumers of changes to the policy; and the effective date of the policy.

In short, app developers should create, maintain and update their privacy policies, and make sure their policies match the information practices.

Stephen Wu is a partner with the Silicon Valley law firm Cooke Kobrick & Wu LLP.

...app developers should create, maintain and update their privacy policies, and make sure their policies match their information practices.”
Security in Knowledge
Mastering data. Securing the world.

Join your peers and industry experts at the infosec event of the year!

Mr. Arthur Coviello, Jr.
Executive Chairman, RSA, Security Division of EMC, Executive Vice President, EMC

Dr. Madan M. Oberoi
Director, Cyber Innovation & Outreach, INTERPOL Global Complex for Innovation

Mr. Frank Abagnale
Famous fraud expert and subject of the best-selling book and hit movie “Catch Me If You Can”

www.rsaconference.com/asiapacific2013