State secrets leaked by a whistleblower, DDoS attacks on banks, BYOD and cloud...the evolution of security technology only accelerated this year.
Dell™ SonicWALL™ next-gen firewalls provide a deeper level of network security without slowing down performance.

Not all next-generation firewalls are the same. To start, Dell SonicWALL next-generation firewalls scan every byte of every packet while maintaining the high performance and low latency that busy networks require. Additionally, Dell SonicWALL network security goes deeper than other firewalls by providing high-performance SSL decryption and inspection, an intrusion prevention system that features sophisticated anti-evasion technology, and network-based malware protection that leverages the power of the cloud. Now your organization can block sophisticated new threats that emerge on a daily basis.

Go deeper at: www.sonicwall.com/deepernetsec

look beyond the obvious.
Editorial

In search of some cheer

Like no other year before, 2013 illustrated just how essential cyber security is to global business endurance, economic durability and personal rights to privacy.

The fractured story of the NSA/Snowden drama seems unceasing and the various revelations that still are coming to the fore only continue to reinforce just how important information security controls are to just about everything we do these days. Whatever your political leanings, Edward Snowden’s questionable acquisition and then sharing of confidential documents drives home the need for robust internal security mechanisms to faithfully address the many insider risks that plague all organizations. Then there’s the result of the still forthcoming leaks, which illustrate just how vulnerable technologies like encryption are and just how essential personal freedoms and privacy are to most of us.

Too, as topics continue to splinter off from Snowden’s initial decision to expose the NSA’s secret snooping, we continue to contemplate many other ethical, security and privacy questions that plague the actions taken in the name of critical infrastructure protection and national security. Any multi-tiered, peopled construct, be it a government agency or a corporation, requires checks and balances. In this instance, even if these existed, they were overrun by individuals who were given too much power or autonomy to make devastating unilateral decisions. After all, one cannot argue the distrust felt by many American citizens and U.S. allies for our government.

Beyond this story, of course, more issues have plagued security and privacy officers. Advanced persistent threats are proving the truthfulness of their moniker, causing plenty of problems for both commercial and government institutions. As well, challenges with BYOD, cloud services and other technologies on which we rely are proving just as chronic. Industry and government compliance mandates, too, are undying and seeming to only push more organizations to embrace security, although, thankfully, it seems that nowadays these no longer are the lone driver.

Meanwhile, as our political leaders squall like little children over issues that should be solved through intellectual discourse and compromise (yes, I expect way too much), antiquated laws like the Computer Fraud and Abuse Act still linger, causing plenty of legal conundrums and still other questions of ethics and fairness to arise.

All of these concerns and the disquiet surrounding them will greet us all with the new year. Indeed, they may become even more acute as more and more IT security incidents bleed into and impact our physical worlds. In saying goodbye to the last 12 months, we must be prepared for what’s to come in 2014. Some quiet before the next storm should do us all some good, helping us to be at the ready. Until then, let’s all look forward to a prosperous and as-blissful-as-we-can-get new year.

Illena Armstrong is VP, editorial of SC Magazine.
Professional face on a regular basis.

Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

For sponsorship opportunities, please contact Anthony Curry at anthony.curry@haymarketmedia.com. Or visit maggie.keller@haymarketmedia.com. For details on SC Congress 24/7 events, please contact Anthony Curry at anthony.curry@haymarketmedia.com.

WHO’S WHO AT SC MAGAZINE

For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketc.com. Or visit scmagazine.com/events/seventh/209/

WHAT IS SC CONGRESS 24/7?

SC Magazine has created a free virtual environment that is open year-round.

Dec. 3 eSymposium in Canada

We’ll take a sweeping survey of what is being discussed in Canadian security circles and what companies can do to maximize their protection of corporate assets and customer information.

Dec. 12 eSymposium: Hacktivism

These vigilante-style, politically motivated attacks are meant to embarass executives by publicizing their secret dealings. What can authorities do to go after these behind these illegal activities, and how can corporations better protect themselves? We’ll take a deep dive.

ON DEMAND eSymposium: APTs

Often patient and much more technically advanced than the average criminal, cyber thieves enlisting APTs infiltrate networks and surreptitiously steal critical data bit by bit, day by day, month by month. If a company reacts too hastily after discovering them, the bad guys can quickly modify the coding on which their attacks are based and become well-hidden once again. Some companies are getting a handle on these attackers and their methods. We look to them to help us better equip other security teams to address these threats.

FOR MORE INFO

For details on SC Congress 24/7 events, please contact Anthony Curry at anthony.curry@haymarketc.com.

Collect mobile device evidence in the lab, field, or anywhere in between.

Celebrate’s UFED Series is now the only mobile forensics solution available in three distinct options: PC software, dedicated single-purpose hardware, or a preconfigured rugged PC kit.

Find out why Celebreite sets the standard for mobile forensics with industry-leading extraction, decoding and analytics for the broadest range of mobile devices.

Visit www.ufedseries.com for more details.
Iran top producer of zombie IP addresses

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

TRENDS

300 million mailboxes worldwide

TOP 3 COUNTRIES

Iran (EMEA), Peru (South America), United States (North America), India (Asia-Pacific)

LARGEST CHANGES

+10,000

Roughly 18,000 patients of Toronto Western Hospital’s Donald K. Johnson Eye Centre may have had personal information compromised after a chief doctor lost three unencrypted USB sticks. The data on the portable drives included names, addresses, phone numbers, health card numbers and procedure codes.

QUEBEC – A 12-year-old boy pleaded guilty to three charges of hacking and downing three Canadian government websites and causing about $50,000 in damages. The fifth grader traded the information he gathered with members of hacktivist collective Anonymous in exchange for video games.

POLAND – Hackers claiming to be affiliated with hacktivist collective Anonymous obtained information they said was stolen from Poland’s Ministry of Economy. The group said it had a problem with ministry trade missions. The leaked information posted on the internet includes passport photos, correspondence between officials and credentials for government websites.

RUSSIA – A website belonging to the Council of Russian Muftis was attacked and defaced by hackers. The site was manipulated to show a picture of a pig with a copy of the Quran in its mouth and also contained a message that the website must be taken down because it had been sullied.

SOUTH KOREA – South Korea is warning people about the dangers of downloading uncertified video games. Officials said that if games were developed in North Korea, the product might contain malware that could be used in an attack. South Korean law enforcement said the malware may collect and transmit location data and that infected computers could be used to launch DDoS attacks.

SOUTH AFRICA – The national Department of Health website was hacked and defaced, prompting involvement from law enforcement and the National Intelligence Agency. Initial media investigations suggested the attack may have been carried out by “Moroccan Agent Secret,” a hacker group reported to have been involved in the breach of more than 200 South African websites in December 2012.

LOS ANGELES – A team of security experts, working with assistance from the FBI and Secret Service, have come together to form the Cyber Intrusion Command Center. The organization will be responsible for responding to threats against the city’s computer networks, as well as attacks aimed at critical infrastructure, such as airports.

NEVADA – Three news sites belonging to the Greenspun Media Group were targeted by a hacker in a distributed denial-of-service attack that downed the websites for several hours on Oct. 15. Officials said that lasvegassun.com, lasvegasweekly.com and vegasinc.com were down from 6:20 a.m. to 10 a.m. The group has taken measures to prevent future disruptions.

JAPAN – Japanese officials said the nation is in need of at least 80,000 additional information security engineers to deal with increasing cyber warfare activity. The country is promoting programs to produce high-level computer hackers, including a five-day security camp in Chiba, where high school and university students can learn from experts.

SOUTH KOREA – South Korea is warning people about the dangers of downloading uncertified video games. Officials said that if games were developed in North Korea, the product might contain malware that could be used in an attack. South Korean law enforcement said the malware may collect and transmit location data and that infected computers could be used to launch DDoS attacks.

LOCATIONS

High-level activities

Medium-level activities

Low-level activities

DataBank
The Zero Access trojan was most used by attackers in the United States and elsewhere.

Malware Vertical encounter rate

<table>
<thead>
<tr>
<th>Position</th>
<th>Industry</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Food &amp; beverage</td>
<td>138%</td>
</tr>
<tr>
<td>2</td>
<td>IT &amp; telecommunications</td>
<td>121%</td>
</tr>
<tr>
<td>3</td>
<td>Retail &amp; Wholesale</td>
<td>121%</td>
</tr>
<tr>
<td>4</td>
<td>Education</td>
<td>100%</td>
</tr>
<tr>
<td>5</td>
<td>Health care</td>
<td>67%</td>
</tr>
<tr>
<td>6</td>
<td>Banking &amp; finance</td>
<td>46%</td>
</tr>
<tr>
<td>7</td>
<td>Government</td>
<td>38%</td>
</tr>
</tbody>
</table>

The chart above reflects the encounter rate in October 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.

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

Malware

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
<th>Source: Cisco</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>Hackers accessed Adobe customer information and source code for popular products, customer encrypted passwords, customer ID, and customer credit and debit card information were exposed.</td>
<td>2.9 million</td>
<td></td>
</tr>
<tr>
<td>AHCMA</td>
<td>The October 12 office theft of two laptops resulted in the exposure of patient information from a number of facilities.</td>
<td>729,000</td>
<td></td>
</tr>
<tr>
<td>University of Arizona</td>
<td>A July breach of the university’s College of Law website allowed intruders to access class rosters and applicant lists.</td>
<td>9,080</td>
<td></td>
</tr>
</tbody>
</table>

Top breaches in October Data loss

The biggest increases in month-over-month zombie activity occurred in Iran, China, Belarus, Russia, and China, while the largest decrease occurred in India.

Internet dangers Top 10 threats

<table>
<thead>
<tr>
<th>Name</th>
<th>Movement</th>
<th>Date first observed</th>
<th>Type</th>
<th>Last week</th>
<th>Weeks on list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gammaru A</td>
<td>▲</td>
<td>02/13/13</td>
<td>Worm</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Gammaru A</td>
<td>▲</td>
<td>07/16/13</td>
<td>Worm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gammaru A</td>
<td>▲</td>
<td>06/18/13</td>
<td>Worm</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>Gammaru A</td>
<td>▲</td>
<td>07/09/13</td>
<td>Worm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gammaru U</td>
<td>▲</td>
<td>06/21/13</td>
<td>Worm</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Gammaru U</td>
<td>▲</td>
<td>06/22/13</td>
<td>Worm</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Gammaru A</td>
<td>▲</td>
<td>07/23/13</td>
<td>Worm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Saltie AM</td>
<td>▲</td>
<td>09/26/10</td>
<td>Virus</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>Gammaru V</td>
<td>▲</td>
<td>06/21/13</td>
<td>Worm</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>Hotbar</td>
<td>▲</td>
<td>09/23/10</td>
<td>Adware</td>
<td>14</td>
<td>19</td>
</tr>
</tbody>
</table>

Spam rate Volume by month for each region

<table>
<thead>
<tr>
<th>Region</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific</td>
<td>5.4B</td>
</tr>
<tr>
<td>Africa &amp; Middle East</td>
<td>2.6B</td>
</tr>
<tr>
<td>North America</td>
<td>1.1B</td>
</tr>
<tr>
<td>South America</td>
<td>748.9M</td>
</tr>
</tbody>
</table>

Received spam Top five regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>19.13%</td>
</tr>
<tr>
<td>Colombia</td>
<td>6.3%</td>
</tr>
<tr>
<td>Italy</td>
<td>5.36%</td>
</tr>
<tr>
<td>Egypt</td>
<td>5.01%</td>
</tr>
<tr>
<td>France</td>
<td>4.84%</td>
</tr>
</tbody>
</table>

Zombie IPs Global distribution

The chart above reflects the customer’s perception of the risk of web malware in October. 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 Perceived risk

<table>
<thead>
<tr>
<th>Index value</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1.5</td>
<td>2.0</td>
</tr>
<tr>
<td>2.0</td>
<td>3.0</td>
</tr>
<tr>
<td>2.5</td>
<td>4.0</td>
</tr>
<tr>
<td>3.0</td>
<td>5.0</td>
</tr>
</tbody>
</table>

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

Source: ICS, www.cybersecurityindex.com

The chart above reflects the customer’s perception of the risk of web malware encountered in October. It can be used to assess the risk level per threat category and industry vertical.
NEWS BRIEFS

A U.K. man was indicted for his involvement in the alleged hack of U.S. Army and other government-run databases. According to federal prosecutors, Lauri Love, 28, along with unnamed co-conspirators, allegedly exploited vulnerabilities in Adobe ColdFusion and carried out SQL injection attacks to access the databases over the past year. Arrested in late October in his home in England, Love was charged in federal courts in New Jersey and Virginia for computer crimes. Using the ColdFusion and SQL injection attack methods, the group is accused of stealing data from a long list of U.S. Army systems and other agencies and organizations.

The National Institute of Standards and Technology (NIST) introduced a preliminary cybersecurity framework to help organizations to describe their current security posture, describe for risk management improve-...
A seat earned at the Round Table

O

ver the years, the role of the CISO has evolved, but as the threat landscape intensifies—targeting both large and small enterprises—this position is rapidly garnering a strategic voice at many organizations.

Once regarded strictly as a technical position that focused on fighting the cyber fires created by malware or other advanced threats, at many organizations CISOs now sit at the table alongside the C-level executive.

According to the “2013 IBM Chief Information Security Officer Assessment,” which featured in-depth interviews with 41 professionals who hold senior security positions at their organizations, a majority of participants shared the same primary business concern as their CEO: Loss of brand reputation. The impact can be felt through negative public perception or a hit to stock prices.

What these findings indicate are many security leaders are tasked with recognizing risk factors associated with business decisions in order to communicate the impact that incidents may have on brand reputation.

While it might be a tall order to see beyond the technical details of the position, failings result in earning credibility and trust from upstream management. The changing face of the threat landscape places a focus on thwarting attacks, but according to a recent study by Forrester Research, CISOs should really be focusing on leadership, strategic thinking, business knowledge and, most importantly, risk management.

Jay Leek, CISO at the Blackstone Group, an investment management firm headquartered in New York, believes that the role of the CISO is evolving into more of a chief information risk officer function.

“I do think that it’s starting to happen right now, but it’s in the beginning of its phase where it’s no longer being looked at as a technical role, but more as a vital business function,” Leek said.

Others agree. The position has changed in that it’s more of a business enabler, said Shukri Khader, CISO of Avon Products, an international manufacturer based in New York. He said that due to repeated breach incidents, as well as demanding and evolving regulations and privacy laws, a close partnership between the CISO and the business is “paramount” in order for them to lead the risk management discussion.

“The CISO is becoming more visible, with growing authority, accountability and increasing business impact across the organization,” Khader said. — Marcus Colón

59%

of security execs polled cited identifying and assessing risks as a top priority

Source: IBM

JOBS MARKET
Me and my job

Alexandra Catalin Costoiu
chief security researcher, BitDefender

How do you describe your job to average people?

Initially I used to describe my job as “I am paid to stay all day and watch porn websites,” but then, people started asking me to recommend the most interesting sites. Now I just tell them I’m a security researcher, which sounds geek-ish enough to stop any further questions. But for those more resilient, I would have to say that I portray myself as “the gatekeeper” against internet threats.

What do you think needs more attention from the industry?

Parental control and security techniques that focus on protecting our newest and at the same time more at-risk users: children and teenagers. One should keep in mind that the internet is a grey area where a lot of danger co-exists with useful information, and distinguishing right from wrong can prove quite challenging to the category of users to which I am referring. So, it is our duty to prevent these types of situations and keep the new generation at bay from IT menaces.

What security threats are overblown?

One cannot be too careful about security threats, so better be safe than sorry. Nevertheless, each situation should be treated accordingly and we need to try and come up with the appropriate solution.

What annoys you?

People not paying attention and not actually listening to what we, as security advisers, are saying. For example, at the university where I teach, most of the computers are still infected with Conficker.

Of what are you most proud?

I would have to say the fact that I was directly involved in designing and developing anti-spam and anti-phishing technologies and actually see that my work has paid off for our customers.

What would you use a magic IT security wand for?

I would have to say: world (IT) peace! I wouldn’t mind being unemployed someday.

Skills in demand

There is no one singular solution to mitigate the growing vulnerabilities of our digital universe, but in every sector the demand for computer forensic examiners (aka “CFE”) is on the rise, and they are poised to serve some of the broadest needs of our digital universe.

What it takes

In-depth understanding of forensic data collection, chain of custody, and rules of evidence, along with strong documentation and working knowledge of personal computers, servers and networked systems are all critical.

Compensation

Entry-level roles start around $70K. Mid-level positions can pay up to $325K.

Source: Adam Weissman, director of legal technology, Mullen Group

Update

2 MINUTES ON...

Randal Asay has joined Catbird, a San Francisco, Calif.-based virtualization and cloud security provider, as CEO. Asay, the former director of infrastructure engineering at Walmart, will be central to the growth of Catbird’s first software-defined solution, called dCatbird. Asay was responsible for securing data and operations for the global company, where he built a secure ecommerce platform or virtual infrastructure that supported billions of dollars in business.

Paul Paget has joined Pwnee Express, a Boston-based penetration testing and network vulnerability assessment firm, as CEO. He will drive the company’s growth strategy and focus on building its position in the remote security intelligence market. Prior, he served as CEO of Savant Protection, an infrastructure and industrial control system security firm, where he remains on the board. Paget brings more than 30 years of experience in leadership positions at technology companies.

Sue Friedberg, Buchanan Ingersoll & Rooney, has joined Savant Protection as general counsel, and also leads Buchanan in its own data security compliance efforts.

Allan Manville has joined Livingstone, a global software asset management (SAM) service provider, as the head of enterprise sales for EMEA. In the role, Manville will be responsible for the company’s sales across the region, where he will focus on the firm’s managed service offering. Prior, Manville managed Adobe’s license and compliance team throughout northern Europe.

Buchanan Ingersoll & Rooney have on board Paul Paget, an experienced leader in the cybersecurity industry.

Buchanan Ingersoll & Rooney has added Buchanan Ingersoll & Rooney to its cybersecurity team.

Phong Tran has joined Mithril Capital Management, a Californian firm focused on building its position in the Mac and iOS ecosystem.

Mithril Capital Management has added Paul Paget, an experienced leader in the cybersecurity industry.

Sue Friedberg has joined Buchanan Ingersoll & Rooney, a Pittsburgh-based law firm, with expanded cybersecurity compliance efforts.

Alexandra Catalin Costoiu has joined BitDefender as chief security researcher, a position where she will focus on protecting the company’s newest and at-risk users: children and teenagers.

BitDefender has added Alexandra Catalin Costoiu as chief security researcher.
The changing face of data protection

Denise Wood
CSO, FedEx

I nformation security personnel are challenged with protecting company reputation and enterprise and customer data from a constant and expanding barrage of cyber criminals. Security departments are generally a small band of employees charged with safeguarding huge employee populations and endpoint devices. Increasingly, these teams are being pressed to be leaner and more efficient in addressing this evolving landscape.

The ability to quickly adapt skills and processes is critical. That’s primarily because endpoints today can include not only computers but also other mobile devices.

One of the quickest ways to keep up? A barrage of cyber criminals.

Three solutions are key:

»First is governance. Infor-mation security personnel must know the most important policies and the essential technical standards given their role and use of assets and information.

»Secondly, awareness. Why have a team of 100 people protecting your organization when you can have a team of thousands? By educating employees, partners and even customers, you can expand your army of stewards exponentially.

Put awareness and education of the latest cyber threats and protection methods at the top of your information security list. This will encourage proper cyber hygiene and reduce opportunities for employees to fall prey to threats specifically designed to take advantage of their naivity.

»Third, expanded partners. Your information security operation has a variety of supplemental partners that can help: Solution providers have professional service agreements that can augment your program; third-party vendors are growing their expertise in areas such as monitoring and logging, penetration testing and secure coding; and private and public information-sharing initiatives are beginning to evolve.

Embrace the changing face of information security as a body of influence and begin your journey with governance, awareness and expanded partners. Information security is everyone’s business in the end, so start including everyone in the process.

As the network shifts

W hile 20 percent of the connections to a network are unknown, despite the investment of millions of dollars in security technology, it is critical to identify all connections within an enterprise. This 80-20 rule requires a premier discovery solution, one that will define a network perimeter and validate that unknown connections do not exist.

Performing this audit starts with “fact-based” compli-ance reporting that provides continuous monitoring and shows that protective measures are in place involving sensitive corporate and individual data. This process automates audit reporting on a network’s infrastructure, allowing companies to configure their IT policy guidelines to meet specific conditions and threats.

For example: The exponential increase in the use of connected devices, distributed management environments and changing circumstances – all of these events underscore the necessity of leaving nothing to chance. In other words, 20 percent of a network cannot be left unguarded. There must be continuous monitoring of security controls and comprehensive cybersecurity situational awareness. These are the very building blocks of a proactive brand of network security. Without these tools, security analysts rely on locally focused specialty products, which do not encompass that critical 20 percent, leaving complex systems vulnerable to attack or serious compromise.

And, while a variety of monitoring products exist, continuous monitoring involves a “fact-based” approach, which results in a pro-active solution that is tightly coupled to a network’s infrastructure.

For example, an information security in a box solution can do after access is granted. Huge mistake.

Actively monitor all access points to ensure that you are honoring the strict rules you put in place.

You must turn your approach to securing your network shifts over again, expecting a different result. We have our physical security and give them to the infosec personnel.

...the perimeter changes at the speed of business...

Higher purpose

One of the quickest ways to improve your security posture is to demand a higher level of security from your vendors and providers, says FedEx CSO Denise Wood.

Best practices

This can be done via service levels agreements, security assessments before vendor selection or onboarding, and interim audits throughout the lifecycle of the relationship.

Getting buy-in from all

Security teams have limits. Devices, threats and opportuni-ties are too numerous to be handled by the standard set of tools and a mindset of “information security in a box.”

Expanded endpoints

That’s because devices touching the network now include laptops, printers, smartphones, POS terminals, bar code read-ers and an infinite amount of other mobile devices.

Combatting insider threats

E veryone agrees that combating cyber threats is a business priority. Unfortunately, many enterprises focus their efforts in the wrong areas.

Bad actors want your sensitive data, and their methods get more sophisticated by the day. They are targeting your privileged users via phishing and social engineering, and they’re staying one step ahead.

You must assume your perimeter has been compromised.

You must make your infrastructure blind to privileged users’ top objective. Most enterprises control data, layers security outward from there and place checkpoints along the way. The ability to “watch the watcher” is imperative. It used to be “trust but verify.” Now it’s “plan and verify.” Decide who should be able to see what data under which circumstances, and verify that it’s happening. You may not have a rogue insider in your organization, but getting privileged user credentials is bad actors’ top objective. Most enterprises control who gets access, but don’t control what they can do after access is granted. Huge mistake.

You must make your infrastructure blind to the data. It is high time to split the responsibil-it y of systems management and data access management. Smart enterprises take data access decisions away from privileged users and give them to the infosec personnel.

Insanity is doing the same thing over and over again, expecting a different result. We must stop the insanity by focusing on the data and controlling privileged user access.

Opinion

30 seconds on...

Michael Markulec
CTO, Lumeta

Sol Cates
CSO, Vormetric

...the perimeter changes at the speed of business...
The National Security Agency is instituting some major changes after one of its trusted insiders, namely Edward Snowden, reportedly requested passwords of co-workers to gain access to systems for which he was not authorized. His ruse: Act the role of systems administrator needing the keys to do his job. Already inside, his co-workers believed him to be on the up-and-up. After all, despite his only being present a few weeks, they assumed he’d already gone through rigorous screening and could be trusted. Wrong.

Along with increased focus on insider threats and subsequent privacy concerns that the seeming never-ending NSA/Snowden saga has prompted, other major trends in 2013 abound. The continued rise of bring-your-own-device (BYOD), hacktivism, advanced persistent threats, cyber espionage, mobile malware and more are plaguing CSOs everywhere. Our year-end special Reboot reviews some of the newsworthy happenings related to these issues and gains some insight from thought leaders on what lies ahead.

Also in this annual special edition, we recognize once again leading industry minds whose undertakings this year contributed to the space in a palpable way. These industry veterans stand out for their skills, managerial prowess, insight and advocacy. And, finally, in our Product Section, you’ll find our picks for this year’s Industry Innovators.

As this year-end issue demonstrates, the vibrancy of this industry is as bright as ever and the challenges only more acute. However, stellar professionals on all fronts are at the ready.
Introduction of Aaron’s Law: After the January suicide of activist and developer Aaron Swartz, who was being prosecuted at the time for alleged Computer Fraud and Abuse Act (CFAA) violations, lawmakers introduced legislation to reform the federal anti-hacking law. Nicknamed “Aaron’s Law,” the legal measure would limit unnecessarily aggressive punishment for computer crimes.

Law passed to curb China espionage threat: In March, a new U.S. law was passed requiring federal agencies to review Chinese IT equipment before purchasing the goods. The legislation was signed by President Obama to prevent unauthorized access to federal networks.

After the Introduction of Aaron’s Law: Computer Fraud and Abuse Act (CFAA), the legal measure named “Aaron’s Law,” the legal measure reform the federal anti-hacking law. Nicknamed “Aaron’s Law,” the legal measure would limit unnecessarily aggressive punishment for computer crimes.

Regulators close firm after costly attack: Huntington Beach, Calif.-based Efficient Services Escrow Group was shut down in March by state regulators after it failed to recover lost funds following a $3.5 million cyber heist. Attackers infected Efficient’s networks with a remote access trojan, which resulted in three fraudulent wire transfers, where money was sent to dubious accounts in Russia and China.

Google “Street View” ruling: Experts are concerned that Google could use the technology to identify individuals. The academics did not say how they would limit unnecessarily aggressive punishment for computer crimes.

“at this point, we only know what we know,” says Miller. “We could make some generalizations about the vulnerabilities of CANs and firmware, but we can only take it so far without getting our hands on a wide range of cars in different categories. The expense of doing that kind of research is prohibitive, and so far no one has stepped up to give us access to other cars.”

Valasek says that it would be great if a fleet of Porsches, BMWs and other luxury cars arrived for them to test. “I would be happy with a fleet of Ford Fiestas,” adds Miller.

CHRIS MITCHELL

Age: 60

Occupation: Professor of Computer Science

College: Royal Holloway, University of London


Unless you boast a photographic memory or very good record keeping, it’s a Herculean task to remember all of your passwords without some assistance. This even goes for a respected computer scientist like Chris Mitchell, who is a professor at Royal Holloway, University of London.

“We all have many, many logins, and we can’t possibly remember good strong passwords for all these applications,” Mitchell says. “So, we either use the same password for everything, or write them all down — or both. And that’s me included. It’s not possible to remember 50 strong passwords.”

This year, Mitchell, with postgraduate researcher Haitham Al-Sinani, set out to address the weakness in the conventional password-based model. Their creation, called Uni-IDM (universal identity management), is a software-based tool that helps users manage the authentication process. Installed on a desk top, smartphone or tablet, Uni-IDM opens up a window any time a user attempts to log into a website and seeks to verify any site to which a user is sending an identity.

“This same window will show up every time you log into a site — you’d recognize it as your software intervening on your behalf — and this software will kind of take charge of the process that would normally involve browser redirects,” he says.

Mitchell introduced a working prototype in August and the commercial division of Royal Holloway is in discussions with several major technology companies over licensing it. Uni-IDM builds on what’s been tried already — for example, it picks up some of the elements of Microsoft’s failed CardSpace. It doesn’t invent new methods of authentication, but instead provides users a way of managing all of the authentication tactics already out there, such as Facebook’s OAuth or Google’s OpenID or regular passwords.

Mitchell offers a clarifying metaphor: “It’s the Swiss pocket knife of the identity management world, with little gadgets for every identity management system.”

There is a populism to his undertaking. He sees authentication not as a technological problem but a business one. Sophisticated technology already exists, but save for financial institutions and the occasional employer, authentication tokens are not offered to users. Workers are instead left to their own devices with dozens of passwords to remember.

Mitchell is well suited to work on this issue. In 1990, he arrived at Royal Holloway to work on HP Labs and helped create its Information Security Group. The college launched an M.Sc. in information security in 1992, which Mitchell believes was the first of its kind in the world. He began focusing on identity management systems and authentication 10 years ago. Uni-IDM came out of a newfound belief that computer scientists should find a way of delivering authentication protocols to end users in a single interface.

Naturally, the team at Royal Holloway is also developing a Uni-IDM for mobile devices. “And mobile users are a key market,” he says. “We also need to think about opening the Uni-IDM to other devices.”
Reboot 2013

TOP 8 BREACHES

LivingSocial: More than 50 million customers of deal-of-the-day website LivingSocial were notified in April of a cyber attack that resulted in data being compromised. Hashed and salted passwords were obtained, but financial information was not accessed.

Evernote: Note-taking services provider Evernote alerted its nearly 50 million members in May that a cyber attack may have granted intruders access to information including hashed and salted passwords. The company said that no financial information was accessed.

Adobe: The number of Adobe customers impacted in a breach disclosed early in October skyrocketed to about 38 million after officials with the computer software company initially reported that 2.3 million were affected.

Huawei: More than 50 million users of the Honeywell home automation platform were also affected by a hacking attack that reportedly compromised accounts.

State Administrative Office of the Courts: In July, an administrative office and insurance information – after thieves broke into an administration office and stole two laptops.

Washington State: The Washington State Administrative Office of the Courts announced in May that it suffered a data breach. Court records and financial information are secure, but 160,000 Social Security numbers and one million driver’s license numbers may have been accessed.

Monterey County, Calif.: Nearly 150,000 residents who received social assistance payments through CalFresh, MediCal, CalWorks and Foster Care between 2002 and 2009 may have had data compromised after attackers hacked into a computer that was out of use since 2009.

Drupals org: Vulnerabilities in third-party software used by open source content management platform Drupal.org allowed attackers access to information on nearly one million accounts. The data included hashed passwords, but not financial information.

AHMC Hospitals: More than 700,000 patients of California-based AHMC Hospitals had personal information compromised – including Social Security numbers and insurance information – after thieves broke into an administration office and stole two laptops.

TOP 8 BREACHES

LivingSocial: More than 50 million customers of deal-of-the-day website LivingSocial were notified in April of a cyber attack that resulted in data being compromised. Hashed and salted passwords were obtained, but financial information was not accessed.

Evernote: Note-taking services provider Evernote alerted its nearly 50 million members in May that a cyber attack may have granted intruders access to information including hashed and salted passwords. The company said that no financial information was accessed.

Adobe: The number of Adobe customers impacted in a breach disclosed early in October skyrocketed to about 38 million after officials with the computer software company initially reported that 2.3 million were affected.

State Administrative Office of the Courts: In July, an administrative office and insurance information – after thieves broke into an administration office and stole two laptops.

Washington State: The Washington State Administrative Office of the Courts announced in May that it suffered a data breach. Court records and financial information are secure, but 160,000 Social Security numbers and one million driver’s license numbers may have been accessed.

Monterey County, Calif.: Nearly 150,000 residents who received social assistance payments through CalFresh, MediCal, CalWorks and Foster Care between 2002 and 2009 may have had data compromised after attackers hacked into a computer that was out of use since 2009.

Drupals org: Vulnerabilities in third-party software used by open source content management platform Drupal.org allowed attackers access to information on nearly one million accounts. The data included hashed passwords, but not financial information.

AHMC Hospitals: More than 700,000 patients of California-based AHMC Hospitals had personal information compromised – including Social Security numbers and insurance information – after thieves broke into an administration office and stole two laptops.

TOP 8 BREACHES

LivingSocial: More than 50 million customers of deal-of-the-day website LivingSocial were notified in April of a cyber attack that resulted in data being compromised. Hashed and salted passwords were obtained, but financial information was not accessed.

Evernote: Note-taking services provider Evernote alerted its nearly 50 million members in May that a cyber attack may have granted intruders access to information including hashed and salted passwords. The company said that no financial information was accessed.

Adobe: The number of Adobe customers impacted in a breach disclosed early in October skyrocketed to about 38 million after officials with the computer software company initially reported that 2.3 million were affected.

State Administrative Office of the Courts: In July, an administrative office and insurance information – after thieves broke into an administration office and stole two laptops.

Washington State: The Washington State Administrative Office of the Courts announced in May that it suffered a data breach. Court records and financial information are secure, but 160,000 Social Security numbers and one million driver’s license numbers may have been accessed.

Monterey County, Calif.: Nearly 150,000 residents who received social assistance payments through CalFresh, MediCal, CalWorks and Foster Care between 2002 and 2009 may have had data compromised after attackers hacked into a computer that was out of use since 2009.

Drupals org: Vulnerabilities in third-party software used by open source content management platform Drupal.org allowed attackers access to information on nearly one million accounts. The data included hashed passwords, but not financial information.

AHMC Hospitals: More than 700,000 patients of California-based AHMC Hospitals had personal information compromised – including Social Security numbers and insurance information – after thieves broke into an administration office and stole two laptops.

TOP 8 BREACHES

LivingSocial: More than 50 million customers of deal-of-the-day website LivingSocial were notified in April of a cyber attack that resulted in data being compromised. Hashed and salted passwords were obtained, but financial information was not accessed.

Evernote: Note-taking services provider Evernote alerted its nearly 50 million members in May that a cyber attack may have granted intruders access to information including hashed and salted passwords. The company said that no financial information was accessed.

Adobe: The number of Adobe customers impacted in a breach disclosed early in October skyrocketed to about 38 million after officials with the computer software company initially reported that 2.3 million were affected.

State Administrative Office of the Courts: In July, an administrative office and insurance information – after thieves broke into an administration office and stole two laptops.

Washington State: The Washington State Administrative Office of the Courts announced in May that it suffered a data breach. Court records and financial information are secure, but 160,000 Social Security numbers and one million driver’s license numbers may have been accessed.

Monterey County, Calif.: Nearly 150,000 residents who received social assistance payments through CalFresh, MediCal, CalWorks and Foster Care between 2002 and 2009 may have had data compromised after attackers hacked into a computer that was out of use since 2009.

Drupals org: Vulnerabilities in third-party software used by open source content management platform Drupal.org allowed attackers access to information on nearly one million accounts. The data included hashed passwords, but not financial information.

AHMC Hospitals: More than 700,000 patients of California-based AHMC Hospitals had personal information compromised – including Social Security numbers and insurance information – after thieves broke into an administration office and stole two laptops.
Reboot 2013

TOP 8 THREATS

Sazaara: A data-hijacking trojan that targets U.S. users as part of an international campaign that includes Austria, Switzerland, and Belgium. Sazaara primarily spread via phishing emails. The malware lies dormant on victims’ machines until June 2015, when it begins communicating with its command-and-control server.

Obad: Considered by researchers to be the most sophisticated trojan that targets Android smartphones, this virus exploits two previously unknown vulnerabilities in the mobile platform to send text messages to premium-rate numbers and download additional malware.

Gezi: The security industry hasn’t seen the end of this banking trojan, even though some of its operators have been apprehended. The most recent version has infected thousands of machines in the U.S. and targets the master boot record of IE users to ultimately steal financial information.

Hand of Thief: Linux users were targeted by this financial data-stealing trojan, which was being sold on Russian underground forums. While the first version included standard malicious functionalities, sellers intended to add a suite of web injections that increased its price tag.

Cutwail botnet: Considered the world’s largest spam botnet, Cutwail seems to have no end. This year it resurfaced when a cyber gang opted to distribute their botnet, Cutwail seems to have no end. This year it

Phyllis Schneck received an early introduction to the world of technology which now shapes her day-to-day duties and challenges. Recently appointed the head cyber security official for the Department of Homeland Security (DHS), Schneck believes that her father played a huge role in laying the groundwork for her distinguished career. “My father taught me about computers since the time of age three,” Schneck says. The former CTO for the global public sector division at McAfee adds that although women are “still outnumbered” in the industry, her main focus has been in mentoring young girls who can help close the gender gap. “I think cyber security is a great place for young girls to learn technology,” Schneck says. Among her many achievements, she counts “being a good aunt” and her niece as her biggest triumphs.

In her expansive security career, however, Schneck takes a page from her time at McAfee, where she was most proud of her work in helming the development of its global intelligence system, which was launched in 2005. Befitting of her current role, one of her duties at McAfee was guiding the company’s cultivation of products and services for industrial control system security. Schneck takes a level headed approach to how the DHS should address potential attacks against critical infrastructure. For her, it’s essential to view the responsibility as one supported by a sprawling ecosystem, where the public and private sector have developed a sense of trust and collaboration. “We don’t believe in fear,” Schneck says. “We believe in science and understanding. It’s almost like crowdsourcing, where we can put a lot of different types of perspectives and information together.”

She hopes to neutralize some of the information about security distributed to the masses that concentrates on the fear factor, like “hackers and grids going out,” she says. Instead, she believes it’s more impactful to determine how the agency can improve the country’s resilience against attacks. “We want to make sure our infrastructure can bounce back,” Schneck says. Prior to joining DHS, Schneck took on numerous roles to enhance the country’s readiness. For one, she has served as vice chair of the National Institute of Standards and Technology (NIST) Information Security and Privacy Advisory Board, NIST, a federal agency that was founded in 1901 is considered one of the country’s oldest physical science laboratories. Presently, the agency has taken an integral role in supporting President Obama’s “Improving Critical Infrastructure Cybersecurity” executive order, which was issued in February.

In October, NIST introduced a preliminary cyber security framework as guidance for companies working to prevent attacks that could interrupt essential services or processes within the country, like electricity, water management, gas and oil production or work within the financial services sector. Schneck’s work in bringing the public and private sector together was also carried out through her role as working group chair for the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity, which advises President Obama. Her efforts in support of private sector and government collaboration to stave off critical infrastructure threats and cyber crime further evolved in her eight years as chair of the National Board of Directors of the FBI’s InfraGard program. As founding president of InfraGard Atlanta, Schneck grew the program from 2,000 to more than 30,000 members nationwide. She gained expert knowledge in the private sector as the vice president of corporate strategy at SecureWorks, and founder and CEO of Avalon Communications, which has since been acquired by SecureWorks. She is also a presence on campus. Her work in academia spans from early efforts at her alma mater Georgia Tech, where she co-founded the school’s information security center, to Johns Hopkins University, where she maintains a seat on the department of computer science’s advisory board. She was also named the Loyola University Maryland David D. Lattanzio Center 2012 Executive of the Year.

Having now stepped into a relatively new position at DHS, which was created in 2011, she succeeds Mark Weatherford, the former deputy under secretary for cybersecurity, who held the title for about a year-and-a-half before resigning. Bruce McConnell took over the role as the department’s replacement prior to Schneck’s appointment.

Suzanne Spaulding, deputy undersecretary for DHS’s National Protection and Programs Directorate, says that since her arrival, Schneck has “hit the ground running.” Spaulding reports to Spaulding, who took on her role about two years ago.

Spaulding says an integral part of Schneck’s role has been keeping lines of communication open between the public and private sector – a task fitting the former McAfee CTO.

In her short time at DHS, Schneck has served as a mouthpiece in Washington, and in other parts of the country, so that critical infrastructure operators feel comfortable working with the government. “I have engaged by the administration in an executive order and NIST’s cybersecurity framework. “Her background prepares her beautifully for this role,” Spaulding says. “We really are about supporting critical infrastructure owners and operators, since about 85 percent of our critical infrastructure is owned by the private sector.”

Schneck is well aware of how the “private sector thinks,” Spaulding explained, which “gives her credibility.”

Going forward, Schneck’s says her central goal will be to strengthen the synergy between the corporate world and the government, creating a renewed understanding of, and ability to prevent and respond to, evolving threats against the nation.

For her, helping DHS strike the right balance between citizen privacy and security is key to successfully fulfilling her role. “My top priority will be building trust between DHS and the private sector,” Schneck says. – Danielle Walter

Phyllis Schneck
Age: 42
Occupation: deputy undersecretary for cyber security for the National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security
College: Georgia Tech, Ph.D. computer science

PHYLIS SCHNECK

Image by Joseph M. Eddins Jr./Getty
A though she spent several years as a criminal defense attorney, defending “all kinds” of interesting characters, Jennifer Stisa Granick, the director of civil liberties at the Stanford Center for Internet and Society (CIS), says her current role is the most exciting she has ever had.

It all started when she began defending people accused of computer crimes, “because it seemed interesting.” At that point – in the 1990s – computer law was in its embryonic form. “My mother didn’t have any idea what I did,” says Granick, and there was a widely-held belief that the internet was “unregulatable.”

Much has changed. “My mother now owns an iPad. I hope she has figured out that the internet can be regulated, both for better and for worse,” she says. Most critically, the internet age has increasingly put civil liberties – privacy, in particular – at center stage.

Granick, who is currently working on a book about the NSA, earned a law degree and cut her teeth on the evolving state of cyber law as the civil liberties director at the Electronic Frontier Foundation, and in a previous stint at Stanford, where she was executive director of CIS and taught cyber law, computer crime law, internet intermediary liability and internet law and policy. In 2007, O’Reilly Media released Security POWertools, which she co-authored. She also briefly defended internet activist Aaron Swartz after his arrest for downloading articles from JSTOR, while also challenging the scope of the law under which he was prosecuted.

“So much internet policy is about where society draws the line between competing values,” she says. On one hand, the technology is revolutionary in its ability to give people power to be creative and disrupt conventional ways of doing things. “How much of that is helpful and how much is dangerous could be asked regarding topics as diverse as copyright, free speech and surveillance,” she says. However, it was the revelations about government surveillance made public by Edward Snowden that have brought urgency and clarity to her work. “I have followed this area extensively and anyone who knows anything about these issues was very surprised by what has come out,” says Granick. “We knew from other whistleblowers that there were some shocking things happening. But Snowden provided the context, sense of scale and, above all, the documents, so government could no longer deny these activities,” she says.

“Many of us had some idea that government was collecting phone calls, but we didn’t have any idea it was on every single American for the last seven years, and that is truly shocking,” she adds. Likewise, says Granick, it was widely understood that government could collect emails and chats with people overseas, but the scale, as revealed by Snowden, was dumbfounding. “We knew it was a possibility. We had no idea of the extent,” she says.

Among Granick’s responses to the Snowden revelations was an opinion piece “The Criminal NSA,” which she co-authored with Professor Christopher Snowgaman and published in the New York Times earlier in the year. The article focused on what she believes is the flimsy legal basis on which the NSA spying programs, including Prism, and the collection of phone metadata are conducted.

“In terms of drawing those lines between competing interests, society needs to be able to evolve, but there are a lot of things very wrong with the way things are currently,” she says. In particular, Granick questions the assumptions that underlie government surveillance. “There is no mathematical equation where you increase surveillance and thereby increase an iP value. What we have found is that NSA has collaborated with business to put backdoors in products. These backdoors make all of us less secure and create opportunities for thieves to steal information,” she says. Furthermore, she says when there is an imbalance of information between the government and the people, it makes people less safe and less secure.

“I think government needs to be a positive force, but it has become a negative force,” she adds.

“We, as a society have built an infrastructure for mass surveillance and we are at a tipping point. It is time for our society to say whether this is the world we want to live in and if not, we need to dismantle that infrastructure,” she says. Granick says her book on the NSA is aimed at the general public and will explain in accurate and simple terms what the NSA is doing with phone calls, emails and other personal data. “Why we should care and what we can do about it.” Although no publisher has yet been determined, Granick says, “I’m looking for the book to come out before the November midterm elections.”

And, Granick says she is an optimist. “I think that this country was born on the idea of individual freedom and liberty and that when people understand that what the NSA is doing is revolutionary and it affects innocent people all over the world, I believe they will reject that.”

— Alan Earls

Barnaby Jack, the director of embedded device security for services firm iDefense, passed away a week before last summer’s Black Hat gathering, where he was scheduled to present on vulnerabilities in pacemakers. The topic made headlines in October when it was revealed that doctors replacing former Vice President Dick Cheney’s heart defibrillator in 2007 modified it so couldn’t be hacked by terrorists out to kill him. In testimony from all over the globe, colleagues said Jack was an inspiration and asset to the security community for presenting his research in a way that was compelling and engaging for everyone. He was honored with a posthumous lifetime achievement award at the annual Penie Awards, held during Black Hat.

Although the NSA has vast reach and capabilities to collect and store huge quantities of data, there are vulnerabilities in its infrastructure that have been discovered by independent researchers. Among the most impactful was a research breakthrough by researcher Karsten Nohl, co-founder of Berlin-based Security Research Labs: Karsten Nohl, attorney, special counsel to the Electronic Frontier Foundation: Each year, a multitude of security research- ers find vulnerabilities in popular products and technological platforms, many times sharing their findings with the commu- nity via conferences like Black Hat and DefCon. While they may be pushing boundaries and producing amazing work, there are extremely sensitive legal situations they must navigate around.

Thankfully, there are attorneys like Marcia Hoffman ready to be their guide. Her work in advising researchers and representing them in court is standout this year.

Jeff Forristal, CTO, Bluebox Security: A major Android vulner- ability that could allow an attacker to hijack any legitimate app without modifying its digital signature was disclosed by Forristal in July. The CTO eventually went on to present on the “master key” flaw in detail at the Black Hat conference, where he revealed that other Android flaws existed which gave miscreants similar “master key” privileges.

IN MEMORIAM

Aaron Swartz, 26, took his own life. A co-founder of social news website Reddit, and a well-known online political activist and program- mer, as well as a founder and former director of the nonprofit Demand Progress, a political action group that advocates for civil rights and liberties, he faced 35 years behind bars after he was accused by federal prosecutors of using his access to MIT’s network to steal millions of academic papers so they could be distributed for free. Overzealous prosecution of prodigies working around obstacles that stymie innovation has given rise to moves to reform the three-decade-old Computer Fraud and Abuse Act (CFAA), which critics believe is outdated and has enabled unnecessarily aggressive prosecutions. “Aaron’s law,” introduced in the House by Rep. Zoe Lofgren (D-Calif.), would limit the ways in which people can be charged under existing legislation, though it is currently stalled.

Acclaimed computer scientist, writer and journalist, Dr. Richard Stallman, often called the father of the GNU and Linux operating systems, has been revealed to have a history of inappropriate behavior toward women. Ms. Digital, a prominent female computer science professional, said she experienced a sexual advance by Stallman at a conference. Stallman denies the allegations.

Over-zealous prosecution of prodigies working around obstacles that stymie innovation has given rise to moves to reform the three-decade-old Computer Fraud and Abuse Act (CFAA), which critics believe is outdated and has enabled unnecessarily aggressive prosecutions. "Aaron’s law," introduced in the House by Rep. Zoe Lofgren (D-Calif.). would limit the ways in which people can be charged under existing legislation, though it is currently stalled.
Privacy legislation

CONTINENTAL SHIFT

Once distinct from U.S. policies, Canada is lately closing the gap with its southern neighbor on personal privacy issues, reports James Hale.

In 1969, Canada’s Parliament passed the landmark Criminal Law Amendment Act, two years after Pierre Trudeau, the country’s brash, young justice minister, had stated that “there’s no place for the state in the bedrooms of the nation.” The act legalized gay rights with protection from harassing phone calls and misleading advertising. In that same year, US President Richard Nixon, with the end of Jennifer Stoddart’s 10-year, high-profile tenure as federal privacy commissioner. Rumors around Ottawa’s bureaucratic inner circles say Parsons believes the emerging issues facing the commissioner demand a younger person with a broad understanding of digital technologies, while David Fraser, an attorney with McInnes Cooper, would like to see government look beyond its own ranks. “It would be a better understanding of how to regulate with more subtlety.”

The introduction of Bill C-13 and the revelations about CSEC spying on behalf of the NSA come at a critical time, coinciding as they do with the child pornographers. “Beyond Toews’ divisive rhetoric, C-30 was controversial because it would have allowed authorities to demand access information about ISP or telco subscribers. Instead of “reasonable grounds to believe” that an offence has been committed, police will only require "reasonable grounds to suspect.” The difference is huge, say legal experts.

“Levin says, “why bundle it with spying issues? It’s playing politics, and it’s unfortunate because it forces people to stand against what could be a good law on its own.” Omnisbus bills create a distraction,” says Fraser. “By throwing everything but the kitchen sink into C-13, the government has overshadowed what is needed to combat cyber bullying.” He adds that omnibus bills also create an impression that the government is not being transparent. “It raises suspicions that might be worse than the reality.” In addition, by generating so much negative energy, these omnibus privacy bills have the potential for creating confusion regarding the safety of newer technologies, such as cloud computing. "I think these successive pieces of legislation, along with the CSEC/NSA revelations, will have a negative impact on Canada’s information and communications technology sector, and that probably wasn’t intended,” says Fraser.

For those who oppose them, omnibus bills also present large targets, as Toews discovered with C-30. The British Columbia Civil Liberties Association has been vocal about launching a legal challenge to C-13 should it be passed by Parliament and receive royal assent. Whether that group or other opponents succeed at overturning the legislation, Parsons says it is clear that Canada’s privacy climate is changing. “Our traditional privacy rights are like a fracturing glacier. We don’t know yet if this will be the seismic shift that breaks it, but the temperature is definitely going up.”

BIG SHOES TO FILL: Replacing Jennifer Stoddart

The introduction of Bill C-13 and the revelations about CSEC spying on behalf of the NSA come at a critical time, coinciding as they do with the end of Jennifer Stoddart’s 10-year, high-profile tenure as federal privacy commissioner. Her replacement faces a number of thorny challenges, including – beyond the ramifications of C-13 – Canada’s new anti-spam law, the long-delayed review of the Personal Information Protection and Electronic Documents Act, the implications of wearable computing devices, like Google Glass, and the growth of Big Data.

Some observers, like Citizen Lab’s Chris Parsons, thought Stoddart’s successor would be Chantal Bernier, her deputy for the past five years, but the government has only named Bernier interim commissioner. Rumors around Ottawa’s bureaucratic inner circles say that the government has interviewed as many as 15 candidates and is planning on extending the hiring process well into 2014.

The problem is that the concept of personal privacy is abstract to most people, says Christopher Parsons, a postdoctoral fellow at the Citizen Lab in the University of Toronto’s Munk School of Global Affairs and the principal of Block G Privacy and Security Consulting. “Canadians are becoming more aware because of the controversy surrounding C-13 and its predecessor, Bill C-30.”

Originally titled the Lawful Access Act when it was introduced two years ago, Bill C-30 grabbed media headlines when Vic Toews, then-justice minister, renamed it the Protecting Children from Online Crime Act — without a warrant, and would have required telecommunications providers to ensure that there was a back-door entrance to allow all communications to be intercepted.

The bill was officially withdrawn in February 2013 by Rob Nicholson, then-justice minister, who pledged that another online surveillance bill would not replace it. Introduced in a new session of Parliament in November 2013, “Bill C-13 is not as bad as or as comprehensive as C-30,” says Fraser, but its reception has been just as cold as the one that greeted the earlier legislation.

“Once you get past the two pages that actually address cyber bullying, it’s almost word for word like the second part of C-30,” says Parsons. “The only things missing were passed separately after C-30 was withdrawn.”

Parsons and other critics point to the provision that reintroduces the concept of lawful access, noting that it lowers the bar for law enforcement officials to obtain so-called production orders to access information about ISP or telco subscribers. Instead of “reasonable grounds to believe” that an offence has been committed, police will only require “reasonable grounds to suspect.”

“Levin says, “why bundle it with spying issues? It’s playing politics, and it’s unfortunate because it forces people to stand against what could be a good law on its own.” Omnisbus bills create a distraction,” says Fraser. “By throwing everything but the kitchen sink into C-13, the government has overshadowed what is needed to combat cyber bullying.”

The legislation contains no criminal or civil recourse for those whose information is turned over to law enforcement agencies. “ISPs are already disclosing private information on a daily basis,” says Parsons. “C-13 legalizes that practice, and consumers will have no possible response.”

Others tend to agree. “ISPs have started to view themselves as enforcers, and they shouldn’t,” says Avner Levin, chair of the law and business department at Ryerson University’s Ted Rogers School of Management in Toronto. “The result is that personal information is becoming de-sensitized.”

The introduction of Bill C-13 and the revelations about CSEC spying on behalf of the NSA come at a critical time, coinciding as they do with the child pornographers. “Beyond Toews’ divisive rhetoric, C-30 was controversial because it would have allowed authorities to demand access to subscriber information from both ISPs and telecommunications providers without a warrant, and would have required telecommunications providers
What threat vectors will be most prominent in 2014? Why?
Sanjay Beri, founder and CEO, ZapThink: One of the top threat vectors has always been and will continue to be insiders – typically, employees doing malicious things or people inadvertently causing harm because they don’t know how to use applications in the safest way. It also can include people outside the company who, because they have access to internal data, can propagate threats inside the corporate environment. In some of the latest breaches, attackers were getting access to passwords of people who had admin access to a data center.

Jason Bloomberg, president, NetSekope: Targeted social engineering attacks have and will be the most prominent threat to organizations and users alike. When traditional threat vectors are combined with a social engineering component, these threats evolve into sophisticated tactical attacks with greater success. We saw the evolution of phishing into spear phishing and we continue to see social engineering attack vectors as platforms to introduce new threat variations, including ransomware, such as Cryptolocker.

Enrique Salem, former CEO, Symantec: There’s a range of threat vectors that can be used, but the most sophisticated and widely used attacks are those that are highly targeted and handcrafted for a specific employee at a particular company. An attacker can go onto social media sites, like LinkedIn and Facebook, and build a whole profile for a target.

What security solutions/services will see increased adoption? Why?
SB: Traditional perimeter protection, such as firewalls and intrusion detection, is increasingly ineffective against most attacks these days. Newer technologies – like application-level protection, sandboxing and heuristic analysis that look at activities and threats at a deeper level than traditional networking gear – are a burgeoning space because they can stop attacks that AV and other traditional solutions can’t.

JB: Organizations will increasingly look for holistic security solutions. Point solutions that deal with particular threats never provide adequate security. And with the explosion of threat vectors, free and easy hacking tools, and increased vulnerabilities, organizations must take an approach to security that leverages enterprise architecture – holistically covering organization, process, information and technology.

JC: Businesses and enterprises will be spending their money on cloud-based security solutions in an effort to strengthen their security posture while enhancing their detection and response capabilities. The cloud is providing a flexible platform for new security vendors to offer their security solutions at a competitive price.

BF: You will see more uptake of zero-day defenses like whitelisting and detonation chambers. They are increasingly available and working their way into security requirements that dictate what is purchased. You will also see more endpoint protection to protect against insider threats. The Snowden scandal has made it clear that data loss prevention is a key priority, and so spending on these tools will rise.

AL: With the growth of cloud services, I think most CISOs have realized that they are here to stay. Rather than rail against their insecurities, some of us have begun looking for ways to use cloud services for security. In particular, my group has started to move away from the “stack” of security appliances we’re used to implementing at internet connection points in favor of leveraging cloud resources to perform those functions for users wherever they happen to be.

ES: There are a number of big trends happening today that will drive the adoption of new security solutions. Consumerization of IT, where the end-user has more control over the devices and applications they use in the workplace; a significant move to a smartphone- or tablet-centric computing environment; and adoption of cloud apps by businesses of every size, from the largest companies in the world down to the smallest.

What will see declining adoption rates? Why?
SB: Because they are less effective at stopping threats than newer technologies, solutions like firewalls, IPS, AV gateways and traditional networking gear will see a slowdown in adoption. I’m not saying people won’t still have them, but the reliance on them will be diminished. People are spending millions on that software, but they’re not catching the threats. This may force down pressure on those older solutions, as well.

JB: I don’t believe any category of security solution will decline in 2014. Some will accelerate more quickly than others, but even the laggards will show some growth.

JC: 2014 will see a decline in checklist-based security assessments and audits. They simply are not working. 2013 saw a record number of data breaches, affecting everything from government agencies to mid-sized businesses to enterprises. Consequently, these organizations are spending thousands of dollars (millions for larger data breaches) on the investigation and clean up of a security incident and consumer data breach notifications. This does not include money spent to remediate the security issue to prevent a recurrence.

BF: Traditional anti-virus tools using blacklisting will suffer in popularity. Companies will always need standard AV tools, but they will be increasingly supplemented by other tools that serve to defeat advanced attacks.

What to look for in 2013?
Sanjay Beri is the founder and CEO of NetSekope. He holds numerous patents and has led the design and development of software, firmware, and hardware in various industries.

Jason Bloomberg is president of ZapThink, a Dovel Technologies company. He is a global thought leader in the areas of cloud computing, enterprise architecture and service-oriented architecture.

Joshua Chin is a founder and managing partner with Net Force. His professional focus is directed at strategic and holistic cyber security solutions and digital investigations.

Brian Finch, a partner in Dickstein Shapiro’s Washington, D.C. office, is head of the firm’s global security practice. He is a recognized authority on global security matters.

Arthur Lessard is EVP/CISO for Universal Music Group, responsible for information security governance, external threat management and security operations. His team handles security incident response and develops technology architectures.

Enrique Salem has more than 25 years of executive leadership experience. Most recently, he served as CEO of Symantec. Prior to that, he served as CEO of Brightmail.
More data doesn’t necessarily mean better security...

—Arthur Lessard, CISO, Universal Music Group

AL: While APT-style threats are a problem, I don’t necessarily subscribe to the “APT appliance” mitigation method. I think that the tools that are out there these days, including Splunk, are capable of doing a lot of the correlation promised by APT vendors without the need for a new set of hardware.

ES: Ultimately anything that is PC- or Windows-centric is decreasing in adoption and use. There’s a move away from the common computing platform that has been entrenched in home and work environments for decades. Since hackers, thieves and spies will go where the users are, anything built around traditional endpoint software will see declining usage.

Which security lessons will organizations be forced to learn?

SB: The biggest lesson organizations will be forced to learn is that there are huge implications for lacking knowledge of threats to your organization. Enterprises spend millions trying to solve for problems they know about or think they have, but the biggest problem is what they don’t know.

JB: Achieving adequate security is only getting more difficult and expensive, while hacking is getting simpler and cheaper. The bad guys are winning this war.

JC: Organizations must learn that there is no “us versus IT auditors” or “us versus information security people.” There is only “us versus the bad guys.” Whether one is part of the internal information security of an organization or an external auditor/consultant, there is a constant battle between people who are legitimately trying to improve the security posture and readiness of an organization and the decision-makers of an organization.

BF: As the C-suite increasingly realizes the threat posed by cyber attacks, they will expect better results from security investments. And when the inevitable breach or successful attack occurs, the C-suite will be forced to confront the fact that they cannot defeat every attack and will have to occasionally suffer losses.

AL: Actually, I believe the most interesting one that has been learned in the last few years, and which is still being ingested in some corners of the organization, is that information security is a component of standard business risks rather than a separate “IT security” line item. Trying to deal strictly with IT security (e.g. AV, server patching) without integrating your security groups with the business lines leaves a huge gap that can hurt the bottom line.

ES: The most important lesson organizations have to learn is to figure out what is the most important data they need to protect. They need to ask, “Where is the critical information and the intellectual property?” And they have to be focused because they can’t properly have that kind of control over all devices, data and offices. That would be expensive and not effective. So they need to figure out what apps and services are most important to their business, what data is going into those systems and whether they have appropriate controls for that data, device or app.

What will be the most surprising security-related development?

SB: I think the most surprising development will be, and this is slowly being realized, that the solutions that get 80 to 90 percent of security spend are offering only 30 percent coverage as far as protection. So what companies thought was “keep your lights on” security or the “must-have” product... the vast majority of the budget may need to (go or be managed) more efficiently so they can make room for other more effective stuff. That will be a hard thing for people to get their heads around, but they will.

JB: I predict a “Cyber 9/11” – a single coordinated attack so unexpected and damaging that it changes the world of security, especially cyber security, forever. If not in 2014, then soon.

JC: The most surprising development will be that digital attacks will start having real-life physical consequences. The consequences have thus far largely been limited to the digital world, but we will see an increase of security incidents affecting the physical world. It will be interesting what 2014 brings, especially in the areas of custom-tailored malware or attacks that impact the lives of people.

BF: That old attacks using spear phishing continue to work quite well. One would think that with all the education about such attacks people would be on the lookout for them, but they will still work and cause significant losses.

AL: That Big Data won’t solve all of your problems without the same processes and personnel needed with “Little Data.” To be honest, this shouldn’t be a surprise, since we seem to learn this lesson – more data doesn’t necessarily mean better security – with every technology advance, but it’ll surprise people nonetheless.

ES: A big breakthrough will be the ability to use security solutions that will enable IT to embrace the megatrends – including consumerization, cloud and mobility – without taking on too much risk. Next year will be the tipping point for that because there will be tools in the marketplace that allow admins to be more forward-looking as opposed to reactive.

A more extended version of this Q&A is available on our website, SCMagazine.com.

Visit us today at www.scmagazine.com or at
LIFELINE FOR THE HELP DESK

Enabling students to reset their own passwords relieved IT staff — and network congestion — at a North Carolina college. Greg Masters reports.

Like most educational institutions, Cleveland Community College (CCC) has embraced technology to enhance learning in the classroom, register students and to track and provide grades and transcripts. However, while integrating technology to improve efficiency and engagement, the college — working from a variety of legacy installations — ended up with a number of different systems that required separate login credentials. During registration periods, the help desk would get several hundred student requests to reset passwords. And, though a team of five IT staff ensures that the system is operational and maintained, as well as provides assistance with special projects on campus, the staff dedicated to the help desk was only available Monday through Thursday until 9 p.m. and Friday until 2 p.m., so a huge backlog of frustrated users could build up over the weekend.

“It was important for us to address the problem, not only for customer satisfaction and an improved user experience, but to maximize our limited IT resources and reduce help desk calls for resetting student passwords,” says Kyle Harmon, computer network specialist for CCC. “We really wanted to eliminate the need for multiple login credentials, but at the same time ensure a high level of security for online access for both staff and students.”

The public college is situated in Shelby in Cleveland County, N.C., about 44 miles west of Charlotte, and employs more than 500 faculty and staff members offering continuing education to more than 4,000 students. It provides associate degrees, diploma and certificate programs, as well as other vocational and general courses.

CCC uses Office 365 for student email and Microsoft SharePoint as a portal for accessing all of the college’s systems,” says Harmon.  

The task of identifying a solution that would meet the technology needs of the 50-year-old college fell to Harmon and his colleague at CCC, Network Specialist Chad Linder. They set about looking for an affordable system that was quick and easy to deploy, would enable self-service password reset and thus significantly reduce help desk calls to the IT team.

After reviewing a number of possibilities they went with a tool from SecureAuth as their all-in-one solution. “We felt SecureAuth delivered the best self-servises options for our students and employees,” says Harmon. “We also required a custom user-registration process that would not have been possible without the use of SecureAuth.”

SecureAuth IdP is not so much a tool, but rather provides to an enterprise the tools to become its own identity provider (IdP), says Craig Lund, CEO at Irvine, Calif.-based SecureAuth.

“The solution can integrate with a company’s current infrastructure — including enterprise data stores, authentication protocols and access groups – accept any identity, authenticate internal and mobile users, and assert them into any network, web, cloud or mobile resource.”

He adds that an easy-to-use identity access management console is included, which enables admins to configure two-factor authentication and single sign-on preferences for individual users, groups, applications and devices. The deployment at CCC went smoothly. “We opted to deploy the new identity access management system in phases beginning with faculty and staff, then students,” CCC’s Harmon says.

“The SecureAuth developers worked closely with us to customize the user interface and authentication policies specific to our user needs. The design was completed in less than two weeks.”

The IT team at CCC is pleased with the implementation. “In less than three months, SecureAuth and our IT team here at CCC had deployed the new system for each stage of the phased rollout,” Harmon says.

And, CCC’s IT team saw immediate benefits with the single sign-on and usability features, as users can easily register themselves and no longer have to worry about remembering credentials for so many different systems, Harmon says.

The results have been positive. CCC has significantly reduced call requests to its help desk while offering users a better experience for accessing the college’s different portals, Harmon says.

As far as the technology assisting with compliance requirements, Harmon says that was not a requirement when the system was first installed. However, since the original implementation, the college has configured its SecureAuth servers to present web pages that are in compliance with PCI standards.

The entire college has benefited from the new system, he adds. The help desk has seen a reduction in calls while staff, faculty members and CCC’s thousands of students now have a better user experience with just one set of login credentials, he says.

And, the solution is ideal for those on the go. “Due to the rise of the BYOD business environments, SecureAuth’s mobile solution is more fitting than others on the market,” says Lund. “Enterprises are not required to own the devices, but can still exercise control over the access granted on the mobile devices. Two-factor user workflows can be designed based on risk factors, so external users can be required to authenticate stronger or more often, and single sign-on can be configured to enable access to all applications or only certain ones.”

SecureAuth IdP is managed from a single “solid state” solution, either cloud or enterprise-based. Lund says. Because a single server is conducting all of the authentication workflow, SSO and IdM, all upgrades occur at a single point. The tool typically has an upgrade every quarter with a major release once a year, and the server is upgraded directly from the SecureAuth admin console, he adds.

Security is critical in today’s age of identity theft, says Lund. “SecureAuth’s solution allows enterprises to enjoy a true hybrid experience where the user credentials are vaulted at the enterprise, but the resources are anywhere, including cloud and mobile. These are not easy requirements to meet with one solution, and we are happy to have helped Cleveland Community College succeed in this challenge by deploying SecureAuth IdP.”

The goal for CCC was to implement the system in phases and that has now been completed, says Harmon. Security has, and always will be, a top priority for the college, so it is of critical importance that all information is secure and free from the threat of hackers and viruses, Harmon says. “With more staff and students now using tablets and smartphones to access our applications, it is crucial that we have a security system that allows multiple users access from desktop and mobile devices. We believe deploying SecureAuth has met our requirements for this.”

“”

— Kyle Harmon, Cleveland Community College

Case study
Well, it’s that time of year again. Each year at this time we take a look into the future while everyone else is reliving the events of the past year. Perverse, I know, but in our field the future really is now. So in the spirit of keeping up with advancements in information security, we take the December issue to honor those select Innovators that will likely generate those advancements.

Taking just a moment to look back with a couple of observations is not out of the question of course, so, a couple of thoughts on the past year. First, I do not think I have yet seen a year where the bad guys made more advances in technology, techniques and general damaging activities. We saw the emergence of what I call a cyber smash and grab, where the crooks take weeks or more quietly penetrating a card clearing house or other card provider and then – in a 24-hour period – use the stolen information to clean out hundreds of ATMs netting millions in stolen cash.

We saw the re-emergence of real creativity in malware so that now a high percentage of all breaches involve malware. Some of the malware is quite interesting, even though much of it is reworked older bugs. Even the reworking seems to be creative and, in some cases, quite dangerous. This, after all, was the year when we learned without question or argument that computer malware can have physical consequences.

All of this criminal innovation, disruptive though it was, had one positive effect: It shaped our security sensibilities and consequently our industry. One of the Innovators I interviewed, told me that in this field you innovate or you go out of business. That person was from a large company, and large companies aren’t always known for being innovators. That may well be changing now, out of necessity if for no other reason.

Over the years I have watched innovation in our field ebb and flow. It appears to me that we are in a period of innovation and creativity that might eclipse anything we’ve seen since the earliest glory days of Silicon Valley. Convergence in technologies and companies is increasing rapidly and academics, more than ever, are engaging with industry to discover new solutions to difficult security problems.

Also, this year marked my 50th year in the information security world, which started as a Navy crypto tech. Over this last half century, I have watched patterns and attacks change and the technologies evolve to keep up. Always to keep up. I hope that this year, my 51st, is the year when we – along with the white hats – can say, “We did it. We pulled ahead. After many years of playing catch up, finally we pulled ahead.” Have a great holiday season. – Peter Stephenson, technology editor
Along with innovation comes uniqueness, says Peter Stephenson, technology editor.

We always enjoy the annual Innovators issue because it gives us a chance to see things that will define our industry in the future. Some products were born in the R&D labs within larger companies and eventually saw the light of day because what they accomplished was important to the company. Some were the reason that smaller companies were founded. Whatever the source, we are interested. Each year we seek out the most of the bunch and highlight them.

One interesting thing that happened this year as we were interviewing Innovators was that we were asked what our process is for selecting an Innovator. That was not remarkable for the question so much as for the number of times it was asked. So, it seems appropriate that we elucidate a bit here.

After deciding the product categories that proved critical to the industry during the past year and/or showed some growth and development worth covering, we create lists of potential candidates in each that are further narrowed or fattened. The decisions that get us to the representative lists for each category are based on product reviews we have conducted, conversations with industry contacts we’ve had over the last 12 months, and an overall knowledge of and experience working in the industry.

With that, we pretty much have some solid Innovators lined up. In the past, we have found it necessary to create a new category occasionally, just as we did when cloud security started to take off. We add it along with the appropriate companies that deemed the move necessary. My editors and I look at the lists and offer any further commentary, if appropriate. Once we have the final rundown, we make contact with each vendor to set up interviews, which I conduct.

That said, what else did we learn in general this year? First, big companies are back in the game. Competition is hot – and that is positively identified, the next subject is allowed to do.

If we add to these fundamental security issues the operational issues of deployment, for this year’s access control market to attempt to differentiate against products that are not really intended to do what they accomplish.

We can draw a few conclusions from this year’s discussions. First, innovation is alive and doing well. The industry has picked up a head of steam that will within the next few years show us things we never expected. “I didn’t see that coming” may well be the descriptive phrase going forward.

Additionally, there is a serious crop of new solutions to problems both old and new. And those solutions are more user friendly, better organized and better concentrated on solving the problem they claim to address than we have seen in many a day.

Finally, it is clear that the bad guys are getting more proficient at circumventing security controls. But, at the same time, there are companies getting more proficient at preventing that circumvention. Can we jump ahead of the cyber crooks in the coming year? We certainly hope so. Perhaps that sounds naïve to you as hard-boiled security professionals, but we have talked to 18 Innovators who have the drive, passion and vision to do exactly that. We guess we’ll just have to see what the year brings.

Along with innovation comes uniqueness,BehavioSec

A
ccess control is, arguably, the key aspect of information protection. We think of access control in several ways. For example, we consider access control as the way into the system. We may also apply it to applications. Overall, access control has some facets that make it effective. The first, of course, is A and identification and authentication. This tells the object who the subject is and offers proof of identity. Next is authorization. Once the subject is positively identified, the next question to answer is what the subject is allowed to do.

If we add to these fundamental security issues the operational issues of deployment, provisioning and management, we have the core requirements for today’s access control products. There are a lot of products that, one way or another, fulfill those requirements. What we were looking for this year were those niche players who have something really special that shows the kind of creativity needed to address current and future access management requirements, to our great surprise, snuggled in with those smaller players with a high ‘cool’ quotient, was one of our old favorites, a large company with a wide-ranging reputation in the security space. This year, we began to see those larger companies. Last year, we were surprised by the presence of one giant, but this year we have more than one large entity. It was good to see these guys – ForeScout – in the game this year. But they were not alone. A once small company, now gobbled by a giant, was in our access management mix as well. Last year, we had one of those too and they passed into the Hall of Fame. We are predicting big things for this year’s access control company taken into a larger player. All indications are that the acquisition is a very good thing for both parties. We like that too.

Overall, we see some major changes in access management and those changes are exemplified by this year’s crop of Innovators. New approaches to the fundamentals that make it harder for the bad guys without forgetting what access management is all about – that’s what this year’s access control Innovators are all about.

BehavioSec

We are not in the habit of quoting last year’s discussion of a particular Innovator. Each year is new and fresh, but this Innovator really broke the mold and we thought it would be interesting to compare our views last year with this year. In 2012, we said: BehavioSec has taken a core concept that has not been executed well and did not really have a reason for existence, through creative thinking and good market understanding, built upon the concept. That core concept, of course, was keystroke monitoring. This Innovator took a fresh look at how keystroke monitoring was being done, fed the undernourished concept a good dose of algorithms and the result was a boon to the market. We may nearly devoid of false positives and negatives, easy to deploy and easy on end-users. This year, they continued their focus on mobile devices and expanded on their concept of separating business and personal data on tablets, smartphones and the like. One new piece of innovation was extending the notion of passcode authentication on mobile devices – which can be dodgy – to gesture authentication.

AT A GLANCE

VENDOR: BehavioSec

FLAGSHIP PRODUCT: BehavioWeb-Mobile

COST: $0.16/user/year (a sliding scale depending on platform, this price is for one million users for web)

INNOVATION: Invented the concept of “behavioral abstraction” and “continuous authentication.”

GREATEST STRENGTH: Market vision and, of course, knock-out technology

... this year we have more than one large entity...
EyeLock

Last year when we looked at these guys, they knocked our socks off. The scenario was the security entrance to the gates at a busy international airport and their product could pick out and verify identities at a distance and in a motion. We could only imagine the positive impact on both security and efficiency in this use case.

EyeLock is a miniaturized iris-based scanner that sports remarkable speed and accuracy. Now, with the EyeSwipe Nano, such commercial applications as banks, pharmacies, office buildings, etc., can take advantage of biometric-grade access control at a reasonable price. The Nano can replace traditional card swipe access management, maintain better security and speed up the access process. For example, access to access-controlled high-security rooms at Norwich University all are protected by swipe card access. Many times, students and professors on the access list approach one of three down loaded doors with books, tools, computers, etc., and must put everything down just to get their cards and open the doors. How much better it would be simply to walk up to the door and have it open. More important, when a student loses their swipe card, there is a chance of compromise. With the Nano, no such risk would exist.

EyeLock products are industry compatible and are comfortable with third-party access control products. Replacing an existing card swipe system, for example, should pose no problem. The challenge: If you have an oddball system, though, there is an software development kit available that can help you through the rough spots. The combination of speed, accuracy and ease of use all go to make this a truly innovative solution to a whole slew of tough challenges. Adding the affordability of the product just increases its appeal. And along those lines, necessary software for such things as provisioning and iris matching come with the product and are not licensed per user. Price, support, forward thinking and a whole of a solution to tough challenges all go to make these guys one of our favorite Innovators.

At a glance

VENDOR: EyeLock

website: eyeLock.com

FLAGSHIP PRODUCT: EyeSwipe Nano

Cost: $2,495.

Innovation: In-motion and at-a-distance iris authentication technology.

Greatest Strength: These folks continue to innovate, now adding a miniature version of their product priced to fit well into consumer applications. They know their market and what it takes to dominate.

ForeScout

We love this company here in the SC Labs. Its products always are welcomed in our Group Test reviews because they work well, do what they’re advertised to do, and support is good. But it is also a fine innovator. This is the company’s second year in the Innovators section, and we asked the company what was new over the past year. Boy, did we get an earful, and that seems to have been typical of the pattern we saw of most of our returning Innovators.

The big new thing from ForeScout this year is API and its new program/ecosystem. The company has written integrations now and expects many other third-party vendors to join. It developed the notion of “bi-directional integration” that allows it to integrate other third-party products into its ecosystem quickly and easily. In fact, customers and partners can do the integrations themselves with ForeScout’s API. It launched the new capability in late October and a week later had 25 new partners signed up. This is a big deal. For example, when FireEye sees an APT-infected host, it tells CounterACT and CounterACT remedies or removes the host from the network. The idea of customers applying their own integrations is important because they can apply their own use cases. Usually, it is typical that if an organization has a use case outside the mainstream, special arrangements need to be made with the vendor – at an added cost. The usual outcome is that the customer settles for the closest thing that the tool provides already or that it can deploy as part of a policy. The end result may or may not be a good fit.

With bi-directional integration, the customer applies the API to the use case and creates an integration that fits the use case exactly.

Add to this a clear focus on bring-your-own-device (BYOD) and the idea of pervasive security throughout the enterprise and you have forward-looking thinking. ForeScout has traditionally been a NAC powerhouse. The experience and creativity that took it there has taken the company to the next level with the innovations of the past year.

At a glance

VENDOR: ForeScout

Technologies

website: foreScout.com

FLAGSHIP PRODUCT: ForeScout CounterACT

CounterACT Cost: Starts at $9,572.

Innovation: Bi-directional integration: Customers and partners can do the integrations easily.

Greatest Strength: Pervasive network security, forward thinking.

RSA Aveksa

RSA Aveksa is a new entry in our Innovators segment and the company is quite interesting. First, its offering is another example of the trend we are seeing of platforms rather than tools. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.

First, Aveksa believes that IAM should be a line of business rather than tool. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.

First, Aveksa believes that IAM should be a line of business rather than tool. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.

First, Aveksa believes that IAM should be a line of business rather than tool. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.

First, Aveksa believes that IAM should be a line of business rather than tool. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.

First, Aveksa believes that IAM should be a line of business rather than tool. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.

First, Aveksa believes that IAM should be a line of business rather than tool. The Aveksa platform is a well thought-out approach to identity and access management (IAM). There are lots of innovations here.
Cellebrite

Cellebrite is one of those companies that doesn’t really surprise us. It simply satisfies market needs, competes creatively and usually just a bit ahead of the curve. When your products are aimed at forensic testing, that stability is a good thing. It engenders confidence in the veracity of your product’s results, something absolutely crucial in the forensic field. However, that certainty is not intended to imply that Cellebrite is a slow-moving company. Far from it. “These folks’ commitment yields top-drawer results and that is what we have come to expect from this Innovator.”

Cellebrite provides some first-rate forensic tools for mobile devices. They understand that market well enough to do it with a variety of innovative products.

iScan Online

“It’s the people, stupid! That’s probably stretching the Clinton campaign slogan a bit, but in the case of iScan Online it really fits. The founder of iScan is none other than one of the founders of another fine innovator, Saint. And it’s no surprise that both companies are in the vulnerability assessment game. There is one huge difference between them, though. Saint is a professor and movie professional penetration/vulnerability testers, and a very fine one it is, too. iScan Online is a vulnerability assessment tool for the rest of us.

The innovator who put this together, one Bill Austin (from Dallas), introduced us to this service about a year ago. We’ve been watching it and it has grown. Austin certainly knows how to turn a good idea into gold. When he told us about the functionality of his service it has – web-based, self-service vulnerability scanning, complete visualization of endpoints, 60 seconds or less to run regardless of the number of endpoints, and scans inside of OST and PST email files to name just a few – all for the price of a Chicken McNugget, we were hooked, if a tiny bit skeptical. A deeper dive into how it works that does what it does convinced us that this really is a sterling example of forward-thinking innovation. iScan Online works by executing a small script to run a small binary that sits on the endpoint. The script can be set to run using Active Directory, for example. And the endpoint basically is scanning itself. That’s how iScan achieves such remarkably fast scan times. The endpoint does not do any analysis, though. That all is done from the cloud. The service produces first-rate HTML reports that are simplified so that managers can get the important information quickly and accurately, plus they are presented in terms of solutions, not problems. This patch reports directly to the actionable information class, rather than the obscure reporting that often is seen. PCI scans, PAN scans (to identify credit card info that is not secured), and vulnerability scans all are available. This is a potential killer app in the vulnerability management domain. One huge benefit we see is that it is accessible to small and medium-sized businesses based on its reasonable cost and its ease of use. That’s good news because those are exactly the businesses that usually are considered low-hanging fruit by the domain and it takes its input from the UFED, whether physical or logical. The project analyzes a function on the UFED Physical also is new and this is another one of those tools that we’re not sure how we did without before it appeared. Finally, training enhancements, xml outputs, coexistence with EnCase and FTK and improved passcode-bypassing rounded out a year when this Innovator looked at what its market needed and gave it to us. We like Cellebrite for its innovation, creativity and solid competence. As well, the company’s support is in what we consider the top tier, certainly up there with some of the finest large companies we know.

Damballa

We were looking at our notes for this Innovator and at the top of the page, we scribbled: Not your father’s AV. It was a true statement about Damballa, that would have to be it in a nutshell. The current thinking about malware infections passes like a father’s AV. If ever there was a big problem is not stopping the infection, containing and preventing damage. That is exactly what this Innovator does, and it does it in a clever way. While other anti-malware products use signatures, behavior analysis (of the malware) relies on root our suspected bugs, Damballa uses behavior of the network to tell where the infections are. This has led to Cellebrite for most of the infection, it’s containing it big problem is not stopping the infection, containing and preventing damage. That is what we consider the top tier, certainly up there with some of the finest large companies we know.

Damballa uses behavior of the network to tell where the infections are. This has led to Damballa data scientists can use for analysis. This is a technical, mathematically-intensive approach and it applies Big Data constructs in ways that it never yet have been applied in the malware world. These records come from sources on an ongoing basis. As the data scientists at Damballa come up with new behavioral models and used that as the exemplar for the organization. We picked a product that was, as well, particularly innovative in its own right. We did that bet that you will see more and more of this until it defines the industry. The real change is that increasingly the snap-in modules may be third-party products or tools. That is a big deal in our view. So, with all of that as backdrop, let’s take a look at some intriguing products and companies, not to mention platforms. This group might well be a harbinger of things to come in future years. At any rate, we are here in SC Labs certainly think so.

DATA PROTECTION

Data protection is, of course, a rather large group that covers a lot of territory, and encompasses a variety of tools and services. The idea of data protection is at the core of information security. After all, if it were not for the data, we wouldn’t need all of these elaborate protections. So, as we’ve said many times, since it’s all about the data why not go straight to the data and protect it directly? Easier to say, as is the case with most types of protection in our digital world, than it is to do.

There is more than one mode of data protection. One is ensuring that data is not exfiltrated from within the enterprise as the result of some sort of malware or a malicious (or careless) user. Another is avoiding the fraud that encourages carelessness in the part of employees. Yet another is a hybrid approach that ties many levels of protection together on a single coherent platform. We saw all of those this year. And we are treating one of the vendors somewhat differently than in previous years.

In previous years, we have looked at a flagship product...
Fixmo

Fixmo solves a very important problem: the need to separate personal data from organizational data on a mobile device. The idea behind bring-your-own-device (BYOD) is that an employer can use their smartphone or tablet for business, obviating the need for the employer to provide those tools to employees and for employees to have multiple devices to cover personal and business use. The good news is that this bit of a boon for both employee and employer. The bad news is that it potentially puts organizational data at risk. Fixmo solves that problem by separating the two types of data and containerizing the organizational data.

Most BYOD users grudgingly accept the consequences of using their own devices for organizational data. Some of those consequences include the potential destruction of personal data if the device needs to be wiped remotely due to loss, theft or password fumbles. However, if the data is separated, control over organizational data becomes easier and less onerous for the user. It is easier because organizational data is easier to locate if it is only where it is supposed to be, rather than spread around the device. The Fixmo EMP (Enterprise Mobility Platform) takes all of the different functionalities needed to secure the mobile device and manages that security and combines them into a single platform. For example, Sentinel checks to make sure that the device is in a secure state while SafeZone applies encryption and strong authentication.

PhishMe

If this Innovator was not such a good fit for this issue, it might be worth it to include it just for the name. We must admit the first time we saw this company we had to take a pretty deep look at it to make sure that it was serious. Trust us: It is very serious. The principals came to this company from the cream of the crop of incident response organizations. Over time, they realized that it was pretty useless — in fact it often did more harm than good — to conduct a once per year social engineering attack, write a report and move on. Employees pushed back hard, believing they had been entrapped, and little if any behavior was changed. What to do?

The solution to the problem was phone and phone often. And, keep the employees aware of the ongoing training and even include real phishing messages in the training that have targeted employees.

Once an employee succeeds to a phishing attempt, remedial training begins immediately in the form of more than 20 individual training modules. The training, according to this Innovator, is fun — but with an underlying seriousness that it was quite good. Phishing and, particularly, spear phishing are the primary social engineering vectors used by attackers.

To combat the various types of phishing attacks, PhishMe uses Click-only, Data entry, Attachment-based, and Double Barrel (a patent-pending technology that simulates conversational phishing techniques by sending two emails — one benign and one containing a malicious element — to train users on this tactic used by APT actors).

PhishMe also has a unique benchmarking capability that compares anonymized results data with similar info from other customers. This helps organizations understand where they stand relative to other organizations that are potential targets. Once a scenario, its results are compared to the results of the same scenario run against other PhishMe customers. If we were giving awards for the most creative and unusual way to solve a tough security challenge, this Innovator would certainly be right at the top of our list.

McAfee/Intel

This is a tough one to describe on the individual product level. The product box says that industry icon McAfee’s flagship product is Email Protection. Perhaps that is as good as any of this Innovator’s fine products that we might select, but if we were to point at a single flagship product it would not be on their list of hardware or software. It would be innovation itself. When we sat down with the Innovator at this company, the conversation quickly moved from products to why the company puts such a high premium on innovation. We found one response to our enquiry: “Innovation is something to strive for — something intrinsically valuable.” The company has innovated more in the last three years than in the last 10. Why, we wondered? We liked that answer as well. “If you are not innovating, you are declining. There is no such thing as a cash-cow security product anymore.” This has become the mantra for McAfee, a company that was born out of the growth of viruses in the late 1980s, especially since being acquired by Intel. It now has the funding to look long-term and is now less concerned about short-term results than on “innovative ownership of their space.” That spells staying power.

This Innovator took the position five years ago that the market would be supported by the security-connected enterprise, so it built an overall platform that integrates all of the components of the security stack. It is not just innovative, it is accelerating innovation at a faster pace. This allows the company’s ecosystem partners to slot into its platform. So it doesn’t just innovate, it enables innovation.

The approach to innovation, from a purely operational perspective, is itself creative. The company encourages “startups” to develop and run inside the company. As a result, the company can attract and keep the best and brightest engineers, an important aspect of success. “We have the best retention of engineers in the past 10 years,” we were told. “If you want to keep engineers, you have to give them interesting work.” That certainly seems to have worked out well for this Innovator that, quite literally, shaped the anti-malware market nearly 30 years ago.

AT A GLANCE

VENDOR: Fixmo
fixmo.com

FLAGSHIP PRODUCT: Fixmo EMP (Enterprise Mobility Platform)

COST: $5 per device per month

DECEMBER 2013 www.scmagazine.com

INNOVATION: Separates personal apps and data from organizational apps and data on tablets and smartphones in a BYOD environment.

GREATEST STRENGTH: Clear vision of the problem and the solution along with the ability to execute on the vision.

So what makes this, apparently straightforward, approach to securing organizational data on a mobile device innovative? When we looked at this for the first time last year, there was not the breadth of coverage that there is now and we thought that it was an innovative approach. The main reason then as now was that there is a real challenge in simply identifying at risk data in mobile devices that share space between personal and business data.

Personal apps may have access to areas of the device that, while appropriate for personal use, pose significant risk for business use. Fismo creatively solves the identification problem and that, once solved, opened the gate for securing the business data — while leaving the user relatively free to manage personal data in whatever way desired.

AT A GLANCE

VENDOR: PhishMe
phishme.com

FLAGSHIP PRODUCT: PhishMe Email Protection

COST: Ranges from $5 to $25 per user per year, depending on user count and term commitment; includes support.

INNOVATION: An overall platform that integrates all of the components of the security stack.

GREATEST STRENGTH: Rather than focus on products, the company focuses on solving problems.

PhishMe also has a unique benchmarking capability that compares anonymized results data with similar info from other customers. This helps organizations understand where they stand relative to other organizations that are potential targets. Once a scenario, its results are compared to the results of the same scenario run against other PhishMe customers. If we were giving awards for the most creative and unusual way to solve a tough security challenge, this Innovator would certainly be right at the top of our list.

McAfee/Intel

PERIMETER DEFENSE

Brimmer defense has, today, many facets. In the old days (five years ago?) we thought of perimeter defense as something a firewall did. Or, perhaps a firewall and an intrusion prevention system (IPS). Or some sort of gateway. Then we started converging those pieces into smart gateways and next-generation firewalls. That still is fine for the traditional enterprise, but today, we are seeing entire data centers moved into clouds, whether public or private. That begins an entirely different question: How do we protect the physical perimeter.

Several companies have struggled with this, and there are a few shining stars. However, the real benefits for companies that are hybrids — and that is a very large percentage of these days — are that the cloud is both a source of challenge and a source of high-powered analysis. Move the security to the endpoints, continue to protect the physical perimeter sensors at the endpoints and does the analytics in the cloud. Lots of benefits to that architecture as you will see. The other is a deep analysis tool that figures out what is hitting the physical perimeter and addresses it without impacting — in fact, usually improving to a real extreme without adding an included anti-malware product. In the other case, attacks are stopped by aggressive active response. Are these players innovative? We absolutely believe that they are. You’ll need to decide for yourself, of course, but in our

How do we protect a perimeter that does not, physically, exist?
Buzzword and its real meaning – used, though. APT has become a part of terminology as somewhat misused, and APTs. Barrier1 sees those bits as the bad guys’ art head on this year. It was the year of zero-days for all network traffic types in near real time. Usually when we talk to returning Innovators, our questions have a sort of “what have you done for us lately” ring to them. You want to be a bit careful when you ask these guys that kind of question, though. The answer is a bit like drinking from a fire hose.

“Usually when we ask Innovators how to be a bit careful when you ask them carefully since last year. The easy way to describe what the company does is to say it offloads security analysis to the cloud where it can be processed and where the analysis can take advantage of input from all of the company’s customer data. This lets the system react more accurately. One thing that we liked a lot is its inclusion of VirusTotal as the main malware analysis engine. By uploading malware samples – or suspected malware samples – to VirusTotal, the MetaFlows Security System (MSS) can take advantage of not only its own sensors but also of any existing malware samples. In addition, there is no need to update an anti-malware tool since VirusTotal does that automatically.”

A complex attack against specific targets over a long time – has been lost in the hype. Mandiant brought the term into the general information security jargon with its report on APT1, the Chinese hacking group. But there are important issues missed in APT1, the most important one in our view being the P: persistence. That is a major aspect of the Barrier1 process: detecting persistent threats using continuous scanning. That goes beyond scanning, though, according to this Innovator. Not only is continuous scanning necessary, intelligent threat management is the key that really turns the risk management lock. By remembering what it has seen and using that as a baseline, Barrier1 combines continuous scanning and intelligent threat management to detect mutating malware – a favorite technique of bad guys to keep the bugs in the system (persistent) and evade discovery.

“Brinqa’s approach – a baseline database to collect information. Data that feeds the Brinqa analytics process is not structured consistently, so why should an artificial format be imposed? The Brinqa schema-less model allows the free-form flow of information and data that characterizes today’s business environment. All Brinqa systems receive raw data to consume and Brinqa has more than 100 individual connectors for most types of sensors. Of course, those connectors will generate a lot of data and very little of it will be compatible with the rest. This is an example of the free-form nature of the data that Brinqa processes. Brinqa’s Risk Analytics Platform uses extremely sophisticated Big Data concepts to analyze risk and provide real solutions to mitigating what it finds. That sounds like every other GRC vendor, but every other GRC vendor Brinqa definitely is not. But once the data is collected, it needs to be analyzed. Using Big Data constructs, Brinqa develops data sets of data that result in understanding the real impact of the risks discovered. Applying machine learning and data mining to determine critical compliance and risk position reports can be generated on the fly. Part of what enables that rapid reporting is Brinqa’s approach – a baseline approach that are traditionally expensive, difficult to use and that for that reason often sit on the shelf, and they are breaking them down. These products are manageable, affordable in the context of what they provide and they actually perform the right tasks for the right people.”
Modulo Security

Modulo basically is a GRC (governance, risk, compliance) tool that is, mostly SaaS-based. As well, there is a platform-based version for large organizations that prefer on-premise hosting. However, saying that Modulo is a GRC platform is a little misleading, in the sense that it is mostly, SaaS-based. As a result, there are additional or new functions. This means ensuring that anything new that is being developed by Modulo is going to be brought into the system ensuring that reality complies with policy and doing all of this in real time.

VIRTUALIZATION & CLOUD SECURITY

This is the poster child for today’s networks. When we talk about virtualization, the cloud could not, on a practical level, exist. So it is entirely appropriate that we include cloud and virtualization security in this group. If there was ever a market segment where innovation rules the day, this one is it.

The two Innovators in this group are key players in the emerging notion of the software data center. One of the big challenges in virtualization and, indeed, cloud security, is the idea of a management layer. We always have had a management layer and, over the years, we have defined it differently from the operational perspective. Typically, though, it may be thought of as an out-of-band network that is dedicated to system management tasks and tools. That concept works when speaking of the virtual, but the virtual network environment is far more complicated than the traditional physical data center. There are additional or new paradigms at work here that preclude the traditional approach to managing the security of virtual networks. But for all of that, traditional methods are familiar, comfortable and, most of these days, effective. So it falls to the purveyors of management layer to the popular virtual environments – whether the operating environment, such as VMware or the cloud environment, such as AWS (Amazon Web Services)

The cloud is a business, not a technical construct.

HyTrust

We looked at this Innovator back in March of 2012. At that time, we saw it and its flagship product as emerging and we have been watching it ever since. HyTrust solves the problem of access control at the management plane in a software data center. Unlike a physical data center with locks on doors and racks (sometimes even on appliances themselves), a virtual data center must be protected virtually. That means figuring out who needs access to what – least privilege and access management – and how to enforce it. HyTrust is placed between the VM and the management plane of the software data center and deciphers who has elevated access rights to what virtual devices and what they can do with those rights and devices. Because the HyTrust product is, itself, a virtual appliance, it fits nicely into a cloud environment. Securing a cloud implementation is now practical and, from the perspective of compliance, credible. The cloud paradigm – with its business rather than technical construct – is not resistant to this problem of access control. HyTrust’s product is a big deal because it provides an enlightened view of the software data center, while enabling management of the VM and its security. But, the management tool’s backbone is also addressed; ensuring that the tools can be combined into a single console that executes a single holistic policy across all of the agents. This gives a flexible deployment allowing on-the-fly changes in management requirements. For example, the suite of management tools for a given VM deployment might be different when the VM is deployed to production from when it was in development or staging. At the same time, the concept of isolating the agent from the VM guest operating system is, as before, in place, protecting the VM from consequences of multiple agent deployments. Of course compliance is, as always, a major consideration. The centralized management of disparate agents across a software data center enables credible, reliable reporting about security and other management functions. This means ensuring that anything new that is being provided will be caught and brought into the system ensuring that reality complies with policy and doing all of this in real time.

While VMWare was the big push last year, Intigua is moving into other areas, especially the cloud, with support for AWS. This is a big deal because the cloud is not a technology. Rather, it is a business construct. That business construct can be problematic for software data center management, especially security management. While the technology may be solid, fitting into the constraints that cloud providers impose can be challenging. Intigua 2.0 addresses the cloud paradigm with the same creative finesse that it addresses the virtual technology. Problem solved.
HALL OF FAME 2013

The greatest pleasure that we have in writing this section each year is seeing who has the innovation and staying power to make it to the Hall of Fame. To be in the Hall, a company must have been selected for three years as an Innovator. That’s a tough go because it says that not only is it still around — survival is good, of course, but not enough here — but it is still innovating.

Many of our choices over the years also have appeared as Gartner Innovators in the Magic Quadrants. We like that because it says that our choices not only are technically out in front, but they have creative, sustainable business plans and roadmaps for the future. To short, they know their respective spaces and what their place there needs to be. Better how they can be...
Having unenthusiastically acquiesced to the bring-your-own-device (BYOD) revolution and, more recently, to the bring-your-own-app (BYOA) development, enterprises have begun to recognize that they need to get more control over permitted mobile app versions, app licensing (and its associated costs), and a means to maintain app security. To that end, many have begun considering and, in many cases, implementing their own mobile enterprise app stores (EAS). In fact, this year analyst firm Gartner projected that 25 percent of enterprises will have an EAS in place by 2017.

Enterprises with their own private app store in place will have a better handle on app licensing and maintain more consistency in terms of app versions across enterprise devices. Hopefully, that will ease the IT department’s app management burden while cutting costs. However, getting the app security that enterprises need may be more elusive.

Yes, having an EAS reduces the likelihood that employees will install apps that are malicious. By controlling which apps can be installed, the source of those apps, and limiting the available apps to those vetted by the enterprise makes the mobile ecosystem safer. And when an EAS can analyze apps for known malware, the enterprise’s overall state of security is further improved.

Yet, there is more to worry about when it comes to app security than maliciousness. Sure, some apps are malicious and make headlines, but what percentage of mobile apps – used by enterprise users – wind up being malicious? How much of a threat is that? It may become more of a problem as anti-malware systems struggle to detect things like malicious mobile ad networks that get linked into apps at run time. For the most part, malicious mobile apps aren’t an enterprise problem for those with an EAS.

But, it turns out that the level of security provided by the EAS is only as good as what the enterprise does during the app-verify process for each individual app.

A large multinational may already have many custom-made applications and it’s very likely that no one employee has a handle on all the company’s apps, but once the apps do somehow get corralled into the EAS, one wonders what testing was done on those apps – and by whom?

Unfortunately, most tools look at code quality and not code functionality. Can the enterprise say with certainty that its apps are invulnerable to attacks, follow best practices, aren’t over permisioned, and adequately protect stored and transmitted sensitive information?

Take, for example, a hospital system with a network of physicians covering a wide geographical area. Doctors may be recommending a conflicting set of apps for asthma, diabetes care, etc. Yes, an EAS solves this app-consistency problem when the organization standardizes on a few appropriately vetted apps. But, even then, how well versed in HIPAA regulations are the third-party app developers? Did the developer take into consideration the FDA’s latest requirements in terms of mobile apps? What sort of processes and procedures do the app developers have in place to verify that the apps take industry regulatory compliance requirements into consideration? Will developers be around a month – or year – from now to provide support for the apps on which the enterprise standardized?

In the end, it’s not the enterprise app store’s raison d’être to provide all the needed mobile app security. Each app has to be individually tested and analyzed. There’s no way around this if proper security and privacy protection is a goal for the apps in an enterprise’s app store.

Jack Walsh is the mobile security & special projects program manager at ICSA Labs, an independent division of Verizon.

Eliminate mobile app threats

Don’t hang your hat on enterprise app store security, says Jack Walsh at ICSA Labs.