Incident response has become a more complex art, says Rusty Agee, the city of Charlotte’s security engineer

**AT THE READY**

**NSA spying: Canada reacts**
How are the latest NSA spying revelations affecting Canadians’ use of the internet?  

**Dollars and sense**
Though it is difficult to quantify ROI for security initiatives, investment in application security is logical for the enterprise
A Breach Will Eventually Occur!

IS YOUR ENTERPRISE PREPARED?

MAKE ISACA YOUR ORGANIZATIONS BEST DEFENSE AGAINST CYBERATTACKS. LEARN MORE AT isaca.org/cyber.
Horse trading 2.0

Back in the day, for many American Indian tribes of the Great Plains, the horse was the commodity of choice. Not only did the animal serve well in times of war, but possession also indicated an owner’s and the overall tribe’s level of wealth. The more horses, the more moneyed.

Commodities change with time and across groups, of course. What has value for some, means little to nothing for others. Yet, for most modern-day collectives, it’s all about the money, right? Well, money and maybe power and reputation, too, that is. But how exactly one obtains those things is a different story.

Lately, though, data seems a driving commodity behind many initiatives. The U.S. government’s domestic data collection efforts — leaked by Edward Snowden — are all about power. Of course, politicos and others who have the power to surreptitiously undertake these efforts will say they’re keeping us safe from terrorists. But, as we’ve noted, the anti-terrorist impacts of these privacy-invading programs have yet to be proven.

But, I digress. My point is that information is a key underpinning all sorts of trade and holds both hard and soft values for those engaged in its transaction. For those looking to both harness and protect so-called Big Data, problems abound. IT security pros like you and the executive leaders for which you work understand Big Data analytics is where it’s at right now or, at least, where you need to get to. That is, if you can leverage the terabytes of information feeds that pour in from various network and security devices, identity and access management applications, compliance tools and operating systems to more deeply understand what’s happening across your infrastructures, then you can more effectively safeguard the terabytes of all the other Big Data, which encompasses customer information and intellectual property.

Of course, you’re not the only one who grasps this. As RSA’s Daniel Cohen wrote on his company’s blog last month, “Yes, the bad guys are getting there too — to the understanding that Big Data should matter more in their operations and that it will take more human-like, legitimate-looking behavior to trick detection systems into categorizing their activity as ‘un-risky.’”

Hence, just as organizations are increasingly trying to integrate more robust and advanced data analytics into their security operations so, too, are cyber criminals devising ways and enlisting technologies, such as plug-ins, to parse stolen data they’ve collected in order to make better use of it and, probably, make some more money and solidify reputations of, you guessed it, power, prestige and/or wealth. The strength of data, of information as a commodity, then, only continues to deepen as it satisfies so many disparate needs and wants. The hope is that the security and privacy of it will be considered as just as valuable by more officials and organizations.

Illena Armstrong is VP, editorial director of SC Magazine.

"...data seems a driving commodity behind many initiatives."
**WHAT IS SC CONGRESS 24/7?**
SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

**UPCOMING EVENTS**

**SC CONGRESS eSymposium**
September 24
Symposium: Mobile security
What about all those applications that end-users keep downloading? What about the data they want to download on them? Are legal ramifications how does the company stay compliant? We’ll provide some answers.

**SEPTMBER 24**

**eConference: Data security**
What are organizations doing to make sure the most important data they trade in is protected from criminals, taking advantage of the myriad vulnerabilities introduced by ever-widening, mobile and decentralized environments?

**OCTOBER 24**

**eSymposium: Advanced persistent threats**
Online thieves enlisting APTs are of a different ilk. Often patient and much more technically advanced, they infiltrate networks and surreptitiously steal critical data bit by bit, day by day, month by month. If a company reacts too hastily, it can quickly modify the coding on which their attacks are based and become well-hidden once again. So just how can they be stopped?

**FOR MORE INFO**
For further details on SC Congress 24/7 events, please contact Anthony Curry at anthony.curry@haymarketmedia.com.

**For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazine.com/sc-congress-247.**

---

**SC MAGAZINE EDITORIAL ADVISORY BOARD 2013**
Rich Baich, chief information security officer, Enterprise Technology Services; former chief information security officer, Wells Fargo & Co.
Greg Bull, global information protection and security head, partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Algeia
Jaime Chanana, managing director, CSO Board Consulting
Rufus Connell, research director, information technology, Frost & Sullivan
Dave Cullinane, CEO, Security Starfish; former chief information security officer, eBay
Mary Ann Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president, information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Symantec
Gene Friedriksen, global information security officer, PSCU; former chief information security officer, Tyco International
Maurice Hampton, technical account manager, Qualys

**EDITORIAL**

**VP, EDITORIAL** Ilenna Armstrong
Ilenna.armstrong@haymarketmedia.com

**EXECUTIVE EDITOR** Dan Kaplan
dan.kaplan@haymarketmedia.com

**MANAGING EDITOR** Greg Masters
greg.masters@haymarketmedia.com

**DIGITAL CONTENT COORDINATOR** Marcus Colón
marcus.colon@haymarketmedia.com

**REPORTER** Danielle Walker
danielle.walker@haymarketmedia.com

**REPORTER** Adam Greenberg
adam.greenberg@haymarketmedia.com

**TECHNOLOGY EDITOR** Peter Stephenson
peter.stephenson@haymarketmedia.com

**SCL LAB MANAGER** Mike Stephenson
mike.stephenson@haymarketmedia.com

**DIRECTOR OF SC LAB OPERATIONS** John Albian
john.albian@haymarketmedia.com

**SC LAB EDITORIAL ASSISTANT** Judy Traub
judy.traub@haymarketmedia.com

**PROGRAM DIRECTOR, SC CONGRESS** Eric Green
eric.green@haymarketmedia.com

**REGULAR CONTRIBUTORS**
David Cutiss, Ryan Goldberg, James Hale, Karen Epper Hoffman, Stephen Lueken, Deb Radcliffe, Jim Romeu

**ART DIRECTOR** Michael Strong
michael.strong@haymarketmedia.com

**PRODUCTION MANAGER** Kraai Van Baar
kraai.van.baar@haymarketmedia.com

**SC EVENTS**

**EVENTS DIRECTOR** Natasha Mulla
natasha.mulla@haymarketmedia.com

**EVENTS MANAGER** Anthony Curry
anthony.curry@haymarketmedia.com

**ASSOCIATE EVENTS MANAGER** Maggie Killar
maggie.killar@haymarketmedia.com

**SUBSCRIPTION INQUIRIES**

**CUSTOMER SERVICE** (800) 558-2703
EMAIL: subscriptions@haymarketmedia.com
WEB: www.scmagazine.com/subscriptions

---

**WHO’S WHO AT SC MAGAZINE**

**U.S. SALES**
**VP, SALES** David Stollman
(646) 638-6028 david.stollman@haymarketmedia.com
**REGIONAL SALES DIRECTOR** Mike Skurnick
(646) 638-6266 mike.skurnick@haymarketmedia.com
**WEST COAST SALES DIRECTOR**
Matthew Allington (451) 346-6400
matthew.allington@haymarketmedia.com
**EVENT SALES DIRECTOR**
Mike Alessie (646) 638-6002
mike.alessie@haymarketmedia.com
**ACCOUNT MANAGER** Dennis Koster
(646) 638-6029 dennis.koster@haymarketmedia.com
**ACCOUNT MANAGER** Samantha Amoroso
samantha.amoroso@haymarketmedia.com
**LEAD GENERATION CAMPAIGN MANAGER**
Jennifer Brown
jen.brown@haymarketmedia.com
**SALSA EDITORIAL ASSISTANT** Fiona Howell
(646) 638-6264 fiona.howell@haymarketmedia.com
**ACCOUNT EXECUTIVE, LICENSING AND REPRINTS**
Ellen Wong (646) 638-6102
ellen.wong@haymarketmedia.com
**SC MAGAZINE LIST RENTAL**
**REACH MARKETING**
**VP, MARKETING SOLUTIONS** Wayne Nagowski
(651) 205-5358 wayne.nagowski@reachmarketing.com
**ASSISTANT CIRCULATION MANAGER**
Joshua Wontlett (646) 638-6102
joshua.wontlett@haymarketmedia.com
**CUSTOMER DATA MANAGER**
Joshua Blair (646) 638-6048
joshua.blair@haymarketmedia.com
**MANAGEMENT**
CEO, Haymarket Media: Lee Mansiccolo
**EXECUTIVE VP** Tony Keeva

---

**The deadline for the 2014 SC Awards has been extended to Sept. 13!**
Visit awards.scmagazine.com to download your entry kit today.

**Nominations close Sept. 13, 2013**
Germany top producer of zombie IP addresses
During the past month, the EMEA region (Europe, Middle East and Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, Germany was the top producing country. For the other regions, the top producers were Argentina in South America, the United States in North America and India in the Asia-Pacific region. (Source: Symantec)

FARRAGUT, TENN. – Hackers breached the IT systems at Wild Wing Cafe to steal credit card numbers belonging to a “small number” of customers. The restaurant’s owner said the attackers were able to evade policies and protections, and the eatery encouraged customers to watch for fraudulent charges.

WASHINGTON, D.C. – Ten servers belonging to the National Highway Traffic Safety Administration were attacked. While the information housed on the servers is normally available to the public, the servers were taken offline in response to an alert from US-CERT. Countermeasures are ongoing, the highway board said.

BELGIUM – Hacker collective Rex Mundi exposed the names, email addresses and other personal data belonging to more than 6,000 users of telecom Numericable Belgium. Before posting the data, the attackers, who have a history of blackmail, unsuccessfully asked the company to pay a roughly $23,000 ransom.

RUSSIA – The government that has granted temporary asylum to NSA whistleblower Edward Snowden is trying to protect its own privacy with a new plan to purchase 20 typewriters for its Federal Protective Service. Officials want to increase the use of paper documents to limit the risk of hacking and spying.

THAILAND – A Pakistani member of the Pak Cyber Eaglez group compromised the website and database of the Police Nursing College in Thailand. The hacker – known as Sizzling Soul – leaked personal details of 64 people onto a Pastebin document, all in an effort to demonstrate a vulnerability on the site.

WASHINGTON, D.C. – Ten servers belonging to the National Highway Traffic Safety Administration were attacked. While the information housed on the servers is normally available to the public, the servers were taken offline in response to an alert from US-CERT. Countermeasures are ongoing, the highway board said.

MIAMI – A 29-year-old man was sentenced to more than seven years in prison after he pleaded guilty in April to identity theft and tax fraud charges. Charlton Escarmant was sentenced after he and a co-defendant admitted to filing false tax returns based on information stolen from Tallahassee Community College’s financial aid office.

FARRAGUT, TENN. – Hackers breached the IT systems at Wild Wing Cafe to steal credit card numbers belonging to a “small number” of customers. The restaurant’s owner said the attackers were able to evade policies and protections, and the eatery encouraged customers to watch for fraudulent charges.

MIAMI – A 29-year-old man was sentenced to more than seven years in prison after he pleaded guilty in April to identity theft and tax fraud charges. Charlton Escarmant was sentenced after he and a co-defendant admitted to filing false tax returns based on information stolen from Tallahassee Community College’s financial aid office.

RUSSIA – The government that has granted temporary asylum to NSA whistleblower Edward Snowden is trying to protect its own privacy with a new plan to purchase 20 typewriters for its Federal Protective Service. Officials want to increase the use of paper documents to limit the risk of hacking and spying.

THAILAND – A Pakistani member of the Pak Cyber Eaglez group compromised the website and database of the Police Nursing College in Thailand. The hacker – known as Sizzling Soul – leaked personal details of 64 people onto a Pastebin document, all in an effort to demonstrate a vulnerability on the site.
Malware Vertical encounter rate

<table>
<thead>
<tr>
<th>Position</th>
<th>Industry</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Retail and wholesale</td>
<td>154%</td>
</tr>
<tr>
<td>2</td>
<td>Food and beverage</td>
<td>100%</td>
</tr>
<tr>
<td>3</td>
<td>Health care</td>
<td>93%</td>
</tr>
<tr>
<td>4</td>
<td>Education</td>
<td>86%</td>
</tr>
<tr>
<td>5</td>
<td>IT and telecommunications</td>
<td>50%</td>
</tr>
<tr>
<td>6</td>
<td>Banking and finance</td>
<td>46%</td>
</tr>
<tr>
<td>7</td>
<td>Government</td>
<td>46%</td>
</tr>
</tbody>
</table>

The chart above reflects the encounter rate in July 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.

Unneeded microfiche records were discovered in a Texas park.

Top breaches in July Data loss

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texas Health Harris Methodist Hospital Fort Worth, Texas</td>
<td>Old microfiche records were discovered in a park, even though they should have been destroyed by a hospital contractor.</td>
<td>277,000</td>
</tr>
<tr>
<td>Ind. Family &amp; Social Services Admin. Indianapolis</td>
<td>A computer programming glitch resulted in the exposure of client health, financial, and employment information.</td>
<td>187,533</td>
</tr>
<tr>
<td>Citigroup New York</td>
<td>Customers’ sensitive information was exposed when not properly redacted for court records.</td>
<td>146,000</td>
</tr>
</tbody>
</table>

Total number of records containing sensitive personal information involved in breaches in the U.S. since January 2005: 608,945,544

Index of cyber security Perceived risk

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 security threats. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite.

Spam rate Volume by month for each region

<table>
<thead>
<tr>
<th>Region</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific</td>
<td>4.9B</td>
</tr>
<tr>
<td>Europe</td>
<td>2.8B</td>
</tr>
<tr>
<td>Africa &amp; Middle East</td>
<td>1.7B</td>
</tr>
<tr>
<td>North America</td>
<td>951.4M</td>
</tr>
<tr>
<td>South America</td>
<td>697.8M</td>
</tr>
</tbody>
</table>

Internet dangers Top 10 threats

<table>
<thead>
<tr>
<th>Name</th>
<th>Movement</th>
<th>Date first observed</th>
<th>Type</th>
<th>Week of Aug. 5</th>
<th>Weeks on list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gamarue.W</td>
<td>▲</td>
<td>06/28/13</td>
<td>Worm</td>
<td>Unlisted</td>
<td>0</td>
</tr>
<tr>
<td>Expire.gen!F</td>
<td>▲</td>
<td>03/30/11</td>
<td>Virus</td>
<td>Unlisted</td>
<td>0</td>
</tr>
<tr>
<td>Gamarue.N</td>
<td>▲</td>
<td>02/13/13</td>
<td>Worm</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Expire.BM</td>
<td>▲</td>
<td>06/25/13</td>
<td>Virus</td>
<td>Unlisted</td>
<td>0</td>
</tr>
<tr>
<td>Gepys.A</td>
<td>▲</td>
<td>04/09/13</td>
<td>Downloader</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>Vobus.AC</td>
<td>▲</td>
<td>12/06/10</td>
<td>Worm</td>
<td>Unlisted</td>
<td>0</td>
</tr>
<tr>
<td>Gamarue.U</td>
<td>▲</td>
<td>06/21/13</td>
<td>Worm</td>
<td>Unlisted</td>
<td>0</td>
</tr>
<tr>
<td>Gamarue.T</td>
<td>▲</td>
<td>06/18/13</td>
<td>Worm</td>
<td>Unlisted</td>
<td>0</td>
</tr>
<tr>
<td>Salty.AM</td>
<td>▲</td>
<td>09/26/10</td>
<td>Virus</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>Expire.BA</td>
<td>▲</td>
<td>08/16/12</td>
<td>Virus</td>
<td>Unlisted</td>
<td>0</td>
</tr>
</tbody>
</table>

Top 5 attacks used by U.S. hackers

1. Zero Access trojan
2. Pushdo trojan
3. Butterfly botnet
4. Zeus trojan
5. Alikele.A worm

Top 5 attacks used by foreign hackers

1. Zero Access trojan
2. Butterfly botnet
3. Pushdo trojan
4. Zeus trojan
5. Nyymain trojan

There were 35,728,157 attacks in the United States last month, primarily originating from Chicago, Phoenix, Los Angeles; New York; and Dallas. There were 51,984,274 foreign attacks last month, primarily originating from Tokyo; Bucharest, Romania; Sao Paulo, Brazil; Taipei, Taiwan; and Caracas, Venezuela.
Canada’s Royal Canadian Mounted Police swooped down on a data center in the Burnaby, B.C. area this month, seizing computers that they say may be linked to a $500 million botnet. The RCMP said that the computers had been used from control-and-command servers, the search warrant said. The servers were seized from a Burnaby co-location facility, Arima Networks, which rents server space to different companies, including White Falcon. White Falcon is owned by Dmitry Glazyrin, who was out of the country and unreachable at the time of writing. “He probably has hundreds of customers on his own that sells the space and equipment to,” said Curtis Look, president of Arima Networks. said of Glazyrin’s operation. “I think it’s all automated. You go to a website, and you order a server and you pay for it online.” White Falcon Communications was a still customer following the RCMP seizure. Look added.

Ontario Privacy Commissioner Ann Cavoukian has introduced a policy that she says will allow privacy and counterterrorism surveillance to exist in harmony. Called Privacy-Protective Surveillance, the policy would allow intelligence agencies to scan information for evidence relating to suspicious terrorist activity, while preserving personal information.

Not forgotten
The security community, along with family and friends of renowned researcher Barnaby Jack, were stunned to learn of the 35-year-old’s death only a week before he was set to give a highly anticipated talk on hacking pacemakers at last month’s Black Hat conference. Jack was well known for his cutting-edge research and previous Black Hat demos—such as his hack of two ATMs.

Not in the sky
“It isn’t pie in the sky to ask people to consider a system where we can accommodate both of these interests,” said Cavoukian, who unveiled the concept to Pentagon officials late last month.

Homomorphic encryption
A draft paper given to SC Magazine outlines the use of intelligent virtual agents that would be “blind” to irrelevant information, searching only for specific features of interest.

Homomorphic encryption—where operations can be performed on data without decrypting it—would allow encrypted data to be analyzed, the paper said. Law enforcement would then need a warrant to decrypt data flagged by analysts.

Academics have said that homomorphic encryption is currently computationally impractical, given the large amounts of computing power necessary.

Canadian firm Bionym has launched a wearable device offering heartbeat-based biometrics. Called Nymi, the $79 device is an electrocardiogram (ECG) sensor that monitors personal heartbeat characteristics. Once it has authenticated the user based on heartbeat, it communicates their identity to selected devices. The unit only authenticates using the heartbeat’s unique characteristics once.

The device must be registered with an app, which is available for iOS, Android, Windows and OS X. It uses a mixture of proximity sensing and gesture monitoring, allowing users to control devices by flicking their wrists, say the creators.

“The device should only worry about tech enthusiasts,” said Marcus Carey, principal developer at Bionym. “It should only stay concerned with techies.”

DefCon organizers should have discouraged feds from attending last month’s event.

Imagine someone at a firearms trade show saying they don’t like the Iraq War, so anyone affiliated with the government should stay away.

If that’s not an invasion of privacy, I don’t know what is.

In the past, I served in the military and at NSA, and during those times, I would have been considered a tool. Hackers associated with the government are just doing their job.

Most of the people I know in the industry are either government contractors, in possession of a clearance, or sell products to government. If we were to rule all of those people out, DefCon would be tiny.

If people are truly concerned about NSA hacking and privacy, then they should take up the issue with their politicians. Hacking events aren’t the place for politics, although they are surely a place for drama.

THE STATS
1.7b emails, phone calls and other type of communications collected by NSA each day.

I don’t care either way
Yes 28.48%
No 27.15%

To take our latest weekly poll, visit www.scmagazine.com

JOIN THE CONVERSATION

Twitter: @SCMagazine
Facebook: SCMagazine

DEF CON 2013: ANONYMITY EXPOSED
A week before presenting at Black Hat, researcher Barnaby Jack was found dead in his San Francisco home. Photo courtesy of Black Hat USA.
2 MINUTES ON... Anonymity exposed

It was a rude awakening to many when Edward Snowden sounded the whistle on the National Security Agency’s vast and indiscriminate surveillance program. Wiretapping, tailing and going undercover are not new investigative concepts, but the scale and targets of the agency’s digital spying apparatus were shocking, even to those who spent the past decade joking that the government is always watching.

With this in mind, those seeking to rebuff Big Brother and reach portions of the internet, known as the Deep Web, that aren’t indexed by traditional search engines. To ensure one’s online communications are kept safe from prying eyes, privacy seekers also have signed on with encrypted email services such as Silent Circle or Lavabit.

But the reality is, platforms promising secrecy aren’t off-limits to the government either. In August, 28-year-old Eric Eoin Marques was charged with distributing child porn on hidden services provider Freedom Hosting on the Tor network. The warrant against him coincided with the mass reveal of a Firefox vulnerability that, when exploited, tracked the location of Tor users.

Meanwhile, in a preemptive move in light of the Snowden leaks, Silent Circle and Lavabit suddenly suspended their services out of concern they’d be served with government warrants and subpoenas that requested the email records of subscribers.

“The surveillance landscape is far worse than it has ever been and I feel like everything we do is now observable,” Phil Zimmerman, a co-founder of Silent Circle and the inventor of PGP, told GigaOM. “All of our transactions and communications are all fused together into total information awareness apparatus. I don’t think any of this can be fixed merely by the application of cryptography. It is going to require some pushback in the policy space.”

Not all anonymous service providers oppose cooperating with the government. The Tor Project’s Executive Director Andrew Lewman said the anonymity network has collaborated with law enforcement previously, but added that government access to these private portals must be limited.

Lewman warned those desiring more privacy not to use just one anonymity service, explaining that “anyone who is relying on a single tool is already lost.”

30%-60% of the internet is unattainable via search.

Source: Industry estimates

JOBS MARKET
Me and my job

Geoff Linnell, group CIO, Celerant Consulting

How do you describe your job to average people?
The joy of my job is to look after 600 highly intelligent consultants. This is also my major security challenge, as our consultants travel significantly, spending five days a week on client sites.

Why did you get into IT security?
The dangers from the loss of confidential information were always clearly apparent. As the market has grown and developed, so has my passion and interest in information security. While now a CIO, the majority of my time is dedicated to protecting the company’s and clients’ information assets.

What is one of your biggest challenges?
To publicly demonstrate a commitment to protecting information, our board agreed to obtain ISO 27001. I recall stating, “Be careful what you wish for!” I promised I would attain this standard for the company within the year. However, once gained it has to be maintained, and I do not underestimate this challenge.

What keeps you up at night?
Memory sticks. Our consultants work closely in joint teams with clients. The need to share information and large files, often with unreliable internet connection, results in the constant use of memory sticks. We supply encrypted sticks, but I am concerned about an exposure or loss.

Of what are you most proud?
Seeing the behavioral change and improved awareness across the back office, as well as within projects, to accept and support the need for enhanced information security. I believe bring-your-own-device (BYOD) and other new initiatives will also benefit from the improved company culture.

For what would you use a magic IT security wand?
To have a behavior/attitude indicator on our monitoring dashboard so we could help consultants even before they know they need help.

Skills in demand
Companies who leverage the cloud have concerns over the security of their data. The migration has increased demand for incident response pros, including reverse engineers and malware analysts.

What it takes
In-depth knowledge of IP networking, security-related technologies, forensic tools and programming languages are critical, as is experience with encryption, penetration testing, vulnerability assessments and code obfuscation.

Compensation
Malware analyst roles start around $30K, reverse engineering positions can pay up to $70K, and managers often start around $175K to $200K.

Source: Adler Nissen, director of legal technology, Government Group

Briefs

Company news

Gary Kovacs, the former CTO of Mozilla, has joined AVG Technologies, an antivirus provider with North American headquarters in San Francisco, as CEO and managing director. In his role at AVG, he will oversee the company’s development and expansion across a number of offerings, including mobile, cloud and software solutions. At Mozilla, Kovacs was responsible for expanding the Mountain View, Calif.-based company’s desktop and mobile businesses. He was a key player in Mozilla’s creation and development of the Firefox browser, Linux-based desktops, mobile devices and mobile appliances. Kovacs previously served as general manager and vice president of mobile and devices at Adobe Systems.

Tom Heiser, president of security firm RSA, has transitioned to parent company EMC. There, Heiser will lead the company’s efforts in the cloud computing space. In an interim move, Art Coviello, RSA’s executive chairman, will take over Heiser’s responsibilities at RSA.

MobileSpaces, a Silver Spring, Md-based mobile security startup, has secured $8.6 million in funding from investment firms Marker and Accel Partners. With the financing, MobileSpaces, which secures 1.5 million applications in Apple’s App Store and Google Play, plans to enhance its sales and marketing presence to erect itself as a leader in the mobile security space.

Doug Johnson, the vice president and senior adviser for the American Bankers Association’s risk management policy division, has also taken on the role of vice chair of the Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security. Johnson assumes the role from James Wells III, the former chairman of FSSCC, who stepped down after completing his two-year term. FSSCC was established in 2002 and works closely with the U.S. Department of the Treasury.

AirTight Networks, a Mountain View, Calif.-based provider of Wi-Fi security solutions, has secured $10 million in funding led by investors Trident Capital and CMEA Capital. Its customer base consists of businesses in the government, financial, manufacturing, hospitality, health care, technology and retail sectors – and includes Pizza Hut, Taco Bell, the Vitamin Shoppe and Model’s Sporting Goods. The funding will help the company to expand.

Follow us on Facebook and Twitter

Doug Johnson, vice chair, FSSCC

AirTight Networks
Dan Srebnick
former CISO, city of New York

Global cyber warfare is
upon us. We CISOs
and CSOs are the gen-
erals in the global cyber war.
If you haven’t thought about
your role in these terms, then
you are ripe for ambush.

When I ran information
security for the city of New
York, I constantly reminded
my team that they are soldiers
on the front line of a global
cyber war with real-world con-
sequences. To say that nyc.gov
and the critical infrastructure
of Gotham have ‘target’ writ-
ten all over them is certainly
not an overstatement. This was
my daily reality for 14 years.

The threat is coming from
all directions. Foreign mili-
taries, terrorists, organized
criminals and industrial
thieves target us on a daily
basis. Some may know our
IT footprint better than we
do. Others have analyzed and
understood our weaknesses
better than we have. Does
that scare you? It should.

The United States and
other governments are put-
ing Big Data to work for
them and are analyzing our
communication patterns in
real time. If the U.S. can do
it today, can China, Russia,
India and perhaps Al-Qaeda
be far behind? Perhaps your
enemies know better than you
where your assets are
and which assets commu-
nicate. They will use that
information to do damage
to your business, your
customers or your nation.

The cloud, once the
answer to data center
expansion, just makes
it easier for thieves and
disrupters to get at
your data without your
knowledge. It is 10 p.m.
Do you know where your
data is?

Are your troops ready?
How’s your basic training?
Make sure that your security
awareness training for IT staff
covers how to handle high-
profile incidents. Evidence
preservation and intelligence
gathering must be in balance
with the need to restore ser-
vice, or you’ll soon repeat the
exercise without having gained
any insight into the cause.

A good general has the
respect and cooperation of the
troops. You can earn this by
getting out of your office and
going down to the trenches
and asking them if they con-
sider themselves ready.

Don’t do this at a formal
meeting where there might
be an inclination to paint a
rosy picture.

Get to know the best
network engineers, sys
admins and DBAs in your
organization. They know
things that won’t turn
up in your risk reports,
audits or vulnerability
management reports.

They know where the
weak underbelly of your
organization is and prob-
ably have some good ideas
on how to firm things up.

Make sure they know what
to do within the first five
minutes of the “big event.”

It is coming soon to your
enterprise.

Dan Srebnick is the owner of
Technical Merits, an infosec
strategy firm. He retired as
NYC’s CISO in May.

Ready the troops

Dan Srebnick
former CISO, city of New York

Global cyber warfare is
upon us. We CISOs
and CSOs are the gen-
erals in the global cyber war.
If you haven’t thought about
your role in these terms, then
you are ripe for ambush.

When I ran information
security for the city of New
York, I constantly reminded
my team that they are soldiers
on the front line of a global
cyber war with real-world con-
sequences. To say that nyc.gov
and the critical infrastructure
of Gotham have ‘target’ writ-
ten all over them is certainly
not an overstatement. This was
my daily reality for 14 years.

The threat is coming from
all directions. Foreign mili-
taries, terrorists, organized
criminals and industrial
thieves target us on a daily
basis. Some may know our
IT footprint better than we
do. Others have analyzed and
understood our weaknesses
better than we have. Does
that scare you? It should.

The United States and
other governments are put-
ing Big Data to work for
them and are analyzing our
communication patterns in
real time. If the U.S. can do
it today, can China, Russia,
India and perhaps Al-Qaeda
be far behind? Perhaps your
enemies know better than you
where your assets are
and which assets commu-
nicate. They will use that
information to do damage
to your business, your
customers or your nation.

The cloud, once the
answer to data center
expansion, just makes
it easier for thieves and
disrupters to get at
your data without your
knowledge. It is 10 p.m.
Do you know where your
data is?

Are your troops ready?
How’s your basic training?
Make sure that your security
awareness training for IT staff
covers how to handle high-
profile incidents. Evidence
preservation and intelligence
gathering must be in balance
with the need to restore ser-
vice, or you’ll soon repeat the
exercise without having gained
any insight into the cause.

A good general has the
respect and cooperation of the
troops. You can earn this by
getting out of your office and
going down to the trenches
and asking them if they con-
sider themselves ready.

Don’t do this at a formal
meeting where there might
be an inclination to paint a
rosy picture.

Get to know the best
network engineers, sys
admins and DBAs in your
organization. They know
things that won’t turn
up in your risk reports,
audits or vulnerability
management reports.

They know where the
weak underbelly of your
organization is and prob-
ably have some good ideas
on how to firm things up.

Make sure they know what
to do within the first five
minutes of the “big event.”

It is coming soon to your
enterprise.

Dan Srebnick is the owner of
Technical Merits, an infosec
strategy firm. He retired as
NYC’s CISO in May.

Ready the troops

Dan Srebnick
former CISO, city of New York

Global cyber warfare is
upon us. We CISOs
and CSOs are the gen-
erals in the global cyber war.
If you haven’t thought about
your role in these terms, then
you are ripe for ambush.

When I ran information
security for the city of New
York, I constantly reminded
my team that they are soldiers
on the front line of a global
cyber war with real-world con-
sequences. To say that nyc.gov
and the critical infrastructure
of Gotham have ‘target’ writ-
ten all over them is certainly
not an overstatement. This was
my daily reality for 14 years.

The threat is coming from
all directions. Foreign mili-
taries, terrorists, organized
criminals and industrial
thieves target us on a daily
basis. Some may know our
IT footprint better than we
do. Others have analyzed and
understood our weaknesses
better than we have. Does
that scare you? It should.

The United States and
other governments are put-
ing Big Data to work for
them and are analyzing our
communication patterns in
real time. If the U.S. can do
it today, can China, Russia,
India and perhaps Al-Qaeda
be far behind? Perhaps your
enemies know better than you
where your assets are
and which assets commu-
nicate. They will use that
information to do damage
to your business, your
customers or your nation.

The cloud, once the
answer to data center
expansion, just makes
it easier for thieves and
disrupters to get at
your data without your
knowledge. It is 10 p.m.
Do you know where your
data is?

Are your troops ready?
How’s your basic training?
Make sure that your security
awareness training for IT staff
covers how to handle high-
profile incidents. Evidence
preservation and intelligence
gathering must be in balance
with the need to restore ser-
vice, or you’ll soon repeat the
exercise without having gained
any insight into the cause.

A good general has the
respect and cooperation of the
troops. You can earn this by
getting out of your office and
going down to the trenches
and asking them if they con-
sider themselves ready.

Don’t do this at a formal
meeting where there might
be an inclination to paint a
rosy picture.

Get to know the best
network engineers, sys
admins and DBAs in your
organization. They know
things that won’t turn
up in your risk reports,
audits or vulnerability
management reports.

They know where the
weak underbelly of your
organization is and prob-
ably have some good ideas
on how to firm things up.

Make sure they know what
to do within the first five
minutes of the “big event.”

It is coming soon to your
enterprise.

Dan Srebnick is the owner of
Technical Merits, an infosec
strategy firm. He retired as
NYC’s CISO in May.
Opinion

No need for anti-phishing vigilantes

M any people want to do something positive in relation to security, and some of those individuals probably consider taking up arms against phishers. Compared with handling live malware, it seems considerably less risky. However, hidden depths lie beneath the surface and would-be phish hunters should keep the following advice in mind:

Anything you do on phishing pages that gains the owners’ attention (populating phish forms with fake data, for example) could potentially hand them lots of revealing information about you. Poorly implemented phish pages often have their data dumps pillaged by others—and at that point, “I fight phishers and here’s some of my details” is being posted to underground forums in the most obvious manner.

If you insist on wasting the time of a phisher by spamming them with fake entries, consider that you’re potentially wasting the time of others, too. Many organizations scout fresh data dumps, attempting to contact potential victims before their stolen information is used for malicious purposes. This task becomes a lot harder if they have to swim upstream through the digital equivalent of broken bottles and plastic bags, and even trickier if your fake data looks realistic enough to fool the phishers themselves. And there are other serious risks involved when dealing with phishers as well. For example, navigating phish page directories could lead you to drive-by malware or potentially illegal content, and nobody wants that on their system.

Leaving a phisher with a large collection of fake data is still leaving them with a haul of real data too. Instead, consider reporting the page to a site such as PhishTank. With this, you will have your part done, and others with more experience will have the site dealt with.

Fight the good fight, but don’t make it a Pyrrhic victory.

Biting the silver bullet

S ecurity technology investment is no guarantee of protection against the latest threats. Recent studies by the Ponemon Institute indicate that despite serious business investment in equipment, there was still a 58 percent year-on-year increase in malware incidents, with the average cost of a cyber attack incuring a massive $6.1 million penalty.

In order to truly improve data security, every business must first consider a few key things. What are you protecting? What is it worth to you? What are you protecting it against? And what are the consequences of failure? These questions also need to be asked repeatedly and regularly—the shifting demands of employees, customers and other stakeholders together with evolving compliance standards cannot be resolved by point products alone, however sophisticated.

The modern data security challenge is made even more complex by employees accessing company resources internally and externally by any means at hand, including untrusted cloud platforms and their own personal devices. Rarely intentionally malicious, these practices add intelligent identity management and granular user authentication as extra security overheads to a list that already includes data leakage, malware, exploits and hackers. These multilayered risk and security challenges can only be met with a blend of technology, consultancy, commitment, resolution and a genuine willingness to adapt.

IT managers must continue to mitigate all these issues by taking the smartest precautions that they can to manage them effectively and strike a balance between security, productivity and cost. A thoroughly planned, practical security strategy will always help to improve protection levels, while also reducing costs. Businesses must take a risk-based approach; develop objective security plans that are prioritized and actionable; gain a better understanding of actual risks, costs and benefits; and then invest time, money and effort primarily in those areas that are of greatest value.

Achieving this will always demand cultural change, collaboration and measured partnerships—and not merely a stack of sophisticated security equipment.

Christopher Boyd, senior threat researcher, Thread Track Security

Got something to say?

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

From the online mailbag

In response to an August news story, DefCon: Former DHS cyber official to private sector: Gov’t can’t help you with intelligence:

Getting the government to change any process, especially those for releasing information, and critically, classified information is like moving Mt. Everest one shoveful at a time. Change does not come fast to the government unless there is some visible, imminent, catastrophic threat, or worse, a realized catastrophic incident.

In response to a July news story, California data breach study indicates lack of encryption:

This is a fascinating study—and we can thank [California Attorney General] Kamala Harris for echoing something we’ve been saying for quite some time now: If organizations are not willing to take the necessary measures to protect information, they shouldn’t be storing it. At a time when free-floating information through social media and Big Data analytics is considered a huge benefit for organizations, it’s also important to be cognizant of potential threats posed to both individuals and organizations.

As the volume and sophistication of cyber attacks continues to rise, the need for data encryption is more important than ever.

SocialTJS

In response to a July opinion, Snowden NSA leaks should prompt fresh look at insider threat, by Tom Cross, director of research, Lancopoe:

At this point, the Obama administrations is as responsible for the leaks as Snowden is. Under Obama, there have been more than 150 prosecutions for espionage and leaking secrets by U.S. personnel and contractors and not a SINGLE conviction. That’s an atrocious record. Obama the enforcer, ha. Soft international and soft domestically.

In response to a news story, Schnucks supermarket chain discloses breach that stole 2.4 million credit card numbers:

These thieves are not anonymously using these cards online (probably because they don’t have the security codes that most websites require). They are actually printing these cards with these numbers and expiration dates and phony names. It’s very easy for the retailer to ask for identification on a credit transaction.

In response to June news story, OWASP Top 10 released for 2013:

The major change in the OWASP Top 10 is the recognition of component-based software development—specifically, the need to protect against components that are not secure. This is an important step given that modern day applications are constructed of components—up to 80 percent of each application is comprised of components. Many of these are open source, and managing and securing them is paramount to building trusted applications.

Mark Treaster

The opinions expressed in these letters are not necessarily those of SC Magazine.
Incident response has become a more complex art, says Rusty Agee, the city of Charlotte’s security leader. Karen Epper Hoffman reports.

By most accounts, last year’s Democratic National Convention (DNC) was a rousing success. And at least some small part of that is owing to Rusty Agee’s progressive approach to incident response (IR).

Not a politician or an event organizer, Agee is instead the information security engineer for the city of Charlotte, N.C., where the convention was held in early September 2012. A high-profile national forum, the DNC undoubtedly would have been a major target for hackers of all stripes, and yet the event went through with nary a major reported cyber security breach. With support from the city’s IR vendor, Agee says that if a major attack had occurred, the IT team was ready.

“We haven’t had any significant incidents to speak of for quite some time,” Agee says, conceding that the city still deals with the routine infected machines and malware outbreaks.

“When I was first doing security, we all worried about someone hacking into the network. But over the last few years, the industry as a whole has come to realize that you have the threat of [people] trying to hack in, and it’s a lot easier for users on the network to make mistakes…It’s caused us all to be a lot more proactive.”

Agee began working for the city of Charlotte’s network team in 1999 as a contractor before moving in-house and then to the security side in 2007. Since then, he has seen incident response evolve greatly. In his current position, he is responsible for maintaining the busy city’s network of 6,800 users across more than 100 locations, including fire stations, police satellite buildings, utilities, solid waste facilities and the transportation and engineering departments. One of his major decisions as the city’s top information security engineer came in 2010, when he decided to replace Charlotte’s outdated incident management system with a more up-to-date security information and event management (SIEM) system.

The old IR system was not only going into end of life, but while it was efficient at collecting logs, it was not easy to get the data out of it, Agee says. With the implementation of the new platform in early 2011, Agee and his team are now able to generate and collect logs and analyze data from multiple sources to obtain a better picture of what behavior is normal and what is suspicious. “Now we can drill down with a couple of clicks,” he says, adding that the new system offers an enhanced view of the network from before and after intrusion, and fits in well with the new role-based security that the city has implemented.

Major data breaches have not only become a weekly, if not daily, topic for the headlines, they are increasingly happening to some of the best-funded industries – including ones that are operating highly proficient networks. For instance, global consumer electronics firm Sony incurred widely reported back-to-back data breaches in April and May 2011 when hackers stole names, addresses and credit card data from as many as 77 million user accounts.
We all need to collaborate a lot more...”

Marc Bleicher, Bit9

In the heat of the moment, as you’re trying to mitigate the eventuality of a breach, mitigate the losses to customers,” Peter Tran, senior director for the Breach Investigations Report, “two-thirds financial risks, the losses to customers.” And, earlier this year, daily deal site Groupon was hit by an advanced persistent threat attack on the company’s popular PlayStation Network. RSA Security also was hit by a breach – “It’s not a matter of if, but when,” says Christopher Pogue, director at SpiderLabs, the advanced security team for Trustwave, a Chicago-based information security company. “Companies can no longer defend the fortress at every level. We need to help companies prepare for the inevitability of a breach, mitigate the financial risks, the losses to customers.”

According to Verizon’s 2013 Data Breach Investigations Report, two-thirds of breaches reported in 2012 took months or even more to discover—potentially because organizations hadn’t been so focused on keeping hackers and criminals out that many do not realize they are already in. Peter Tran, senior director for the advanced cyber defense practice at RSA, the security division of EMC, based in Hopkinton, Mass., says that based on his 15 years in IT security, he has seen adversaries embed themselves in organizations’ systems for as long as seven years without detection. Also, according to the Verizon report, in roughly seven out of 10 cases, breaches are discovered by external parties—in most cases, unrelated parties, such as internet service providers and intelligence organizations that track bad actors.

“The message increasingly is: ‘It’s not a matter of if, but when,’” says Rusty Agee, information security engineer for the city of Charlotte. Although it is a breach that few think will happen to them, says Agee, they realize that it is a breach that they are vulnerable. Most verticals are in the crosshairs of one bad actor or another.”

Fresh perspective

Enter a new approach to incident response, which is, as, says Chris Petersen, CTO and co-founder of LogRhythm, a Boulder, Colo.-based SIEM (security information and event management) provider (which is working with the city of Charlotte), says that he too has seen a defining shift in recent years—from people being focused on being breached and concerned with compliance to a place where awareness of potential attack has reached the executive board level. “The wheels have come off,” Petersen says. Players in the industry have recognized that their sense of security is gone. “The underlying forces are making them realize that they are vulnerable. Most verticals are in the crosshairs of one bad actor or another.”

There has been a lot of investment in the preventative-based technology, but now the threat is starting to change, and we’re seeing very advanced and highly targeted attacks and malware,” says John Vecchi, vice president of product strategy for the advanced threat protection group at Solaris Networks, a South Jordan, Utah-based Big Data security analytics company purchased in May by Blue Coat Systems. “This new breed of attack can slice through these security fortresses like a hot knife through butter.”

The prevalence, pervasiveness and perniciousness of such attacks has fueled a recent shift in thinking, according to Vecchi: Organizations need to be prepared for the inevitable and be effective at responding to incidents in a way that mitigates loss and damage and offers insights into how to prevent similar breaches in the future. This is informing and influencing how incident response is evolving in both terms of structure and focus. “We need to implement countermeasures and automate our response, and take various measures to mitigate the issue,” Petersen says. “This is informing and influencing how incident response is evolving in both terms of structure and focus,” Petersen says. “It’s certainly important in planning around those incidents—from a monetary and reputational standpoint.”

Marc Bleicher, senior incident response consultant for Bit9, a Waltham, Mass.-based security vendor, says he is seeing more collaboration within vertical industries about sharing the information regarding attacks. “Open source intelligence is more pervasive…especially when there are new threats in the news in the past nine months.” He says. It’s been a gradual evolution over the last three years since the Sony breach, he adds. “We all need to collaborate a lot more, change the past attitude of ‘we can’t let this information get out.’ It’s often the same actors and indicators showing up at different locations.”

Organizations are, in many cases, stepping up and proactively going after hackers with measures that include leaving decry data or inserting delays into the malicious scripts in order to throw off or slow them down. More companies are enlisting technologies that look closely at network behaviors, not just signature rules-based alerts, says RSA’s Tran, who adds that this is part of a mindset that is shifting to investigate clues. “They’re not waiting for the fire,” Tran says. “They’re going to see if they have anything smoldering now. They’re looking to detect an attack in motion.”

Ultimately, incident response technology needs to be easier to use—embodied with more automation—to enable a broader pool of talent without requiring years of forensic training, says Anthony Di Bello, strategic partnerships manager for Guidance Software, a Pasadena, Calif.-based digital forensic company. “All organizations are struggling with incident response,” Di Bello says. “Many companies are still lacking the necessary budget and the resources.”

Before and after

“It’s not just responding to the attack in motion that has changed, but how organizations prepare before potential attacks and how they handle the post-mortem and clean-up after incidents are discovered,” Tran describes it as the three Rs of incident response: readiness, response and recovery. “Just letting users know not to send out their personal information is a good start. But protecting the network. The corollary to that, as he sees it, is the lack of intelligence sharing across organizations. He admits, however, that threat intelligence collaboration is getting better, especially in verticals like financial services, which is ahead of the curve.

Some companies, when they have a bad incident, may want to consider bringing in third-party contractors to augment the staff so that regular team members do not get burnt out contending with day-to-day work and a big breach. Cross outlines how the IR team plans to collaborate with those companies, it must understand the consequences because some hackers, if they are spotted, may be sophisticated enough to “pivot and attack the network in a way that is harder to see.”

Trustwave’s Pogue recommends that organizations have a formal computer IR plan in place. A former EHS officer, Pogue likens such pre-incident planning to the same battle preparedness and training exercises soldiers must undergo. The biggest mistake an organization can make is “not preparing at all, having a pervasive but naïve feeling it will not happen to me,” he says.

Other common mistakes

Follow the money is the most important. Cross says. “Not just understanding what happened, but protecting the network. The corollary to that, as he sees it, is the lack of intelligence sharing across organizations. He admits, however, that threat intelligence collaboration is getting better, especially in verticals like financial services, which is ahead of the curve.

Pogue offers insights into how to prevent similar attacks, malware and more broad-based threats. “We are enlisting approaches that look closely at network behaviors, not just signature rules-based alerts, says RSA’s Tran, who adds that this is part of a mindset that is shifting to investigate clues. “They’re not waiting for the fire,” Tran says. “They’re going to see if they have anything smoldering now. They’re looking to detect an attack in motion.”

Ultimately, incident response technology needs to be easier to use—embodied in the out of service and wiping it clean—without doing the forensics out of service and wiping it clean—without doing the forensics...now. They’re not working this all out everyone is scrambling, “that’s no time to be working this all out everybody is scrambling, “that’s no time to be working this all out

Experts weigh in on how to prepare your organization for the evolving state of incident response:

Have an IR team and plan in place—now—“I highly recommend an incident response plan, with your players identified,” says Rusty Agee, information security engineer for the city of Charlotte, N.C. “In the heat of the moment, as you’re trying to mitigate the problem and do forensics, you don’t want to have to also figure out who to call on.”

Educate your users about the threat—While people have become more aware of the ongoing threat of malware and phishing attacks, more subtle and sophisticated threats may be beyond their view, says Agee. “Just letting users know not to send out their personal information is a good start.”

Don’t just pull the plug—Several experts point out how many of their client organizations react to an affected machine by just taking it off service and wiping it clean—without doing the forensics out of service and wiping it clean—without doing the forensics...now. They’re not working this all out everyone is scrambling, “that’s no time to be working this all out everybody is scrambling, “that’s no time to be working this all out

INCIDENT RESPONSE 2.0: The basics

Experts weigh in on how to prepare your organization for the evolving state of incident response:

Have an IR team and plan in place—now—“I highly recommend an incident response plan, with your players identified,” says Rusty Agee, information security engineer for the city of Charlotte, N.C. “In the heat of the moment, as you’re trying to mitigate the problem and do forensics, you don’t want to have to also figure out who to call on.”

Educate your users about the threat—While people have become more aware of the ongoing threat of malware and phishing attacks, more subtle and sophisticated threats may be beyond their view, says Agee. “Just letting users know not to send out their personal information is a good start.”

Don’t just pull the plug—Several experts point out how many of their client organizations react to an affected machine by just taking it off service and wiping it clean—without doing the forensics or investigation necessary to root out the deeper problem. “When something happens, some organizations scratch the offending machine and put it back on,” says Peter Tran, senior director for the advanced cyber defense practice at RSA. “It’s enterprise amnesia. They just want it out of their house.”

Know what ‘normal’ looks like—“Instead of approaching security as a formally, companies need to start living it every day,” says Marc Bleicher, senior incident response consultant for Bit9. “Pay attention to the news, he says, and understand your environment and really get a grasp on what ‘normal traffic looks like, what data is leaving, what’s coming in...Is it normal [at your organization] to have communication with China? Establish a safe clean baseline.”

Get support from top brass—“Make sure that there is C-level buy-in for your plan,” says Anthony Di Bello, strategic partnerships manager for Guidance Software. Once the attack hits, and everyone is scrambling, “that’s no time to be working this all out with the C-suite.”
A lot of Canadian internet traffic happens via the U.S.”

– Dragos Ruiu, founder of the CanSecWest conference

Encryption & privacy

CANADA REACTS

How are the latest NSA spying revelations affecting Canadians’ use of the internet? Danny Bradbury finds out.

A nn Cavoukian, the information and privacy commissioner for the province of Ontario, has a name for what the National Security Agency (NSA) has done – following revelations earlier this month about systematic anti-encryption measures by the intelligence organization which operates under the jurisdiction of the U.S. Department of Defense. “I call it surveillance by design, because they are intentionally designing the system so that they can easily surveil, and have a backdoor by whichever means they want,” she says.

Cavoukian uses these words carefully. She invented Privacy by Design, a method of protecting privacy by building core principles into new technologies. Developed in the 1990s, it was adopted as an international standard by data protection and privacy commissioners in 2010.

But revelations in the U.K. and U.S. media that the NSA has deliberately introduced weaknesses into cryptographic tools and standards for more than a decade makes this a difficult concept to follow these days.

We already knew about PRISM, a project that saw the NSA accessing data stored on cloud-based services in the United States. Under the more recently discovered Project Bullrun, the NSA worked deliberately with technology vendors to introduce weaknesses in the implementations of encryption technologies, according to documents supplied by whistleblower Edward Snowden, a former NSA contract employee.

Canadians have a right to be concerned about the latest revelations, says James Arlen, senior security adviser with Leviathan Security Group in Canada. “For everyone who has had their tin foil hat screwed on real tight, we believe you now,” he says. “You’re only paranoid when there’s no one out to get you.”

Now that we know for sure U.S. spy agencies have been secretly subverting the basis of our communications, what next? Do we need to take any more measures north of the border? Unfortunately, simply storing it here may no longer be enough.

Companies have long known about the dangers to data stored on U.S. soil – or in other countries using servers owned by U.S. corporations. The USA Patriot Act, signed into law in response to the attacks of Sept. 11, made it far easier for authorities to co-opt that data, and serve a service provider with a gag order preventing them from talking about it.

Until now, the idea was that by storing data with a Canadian cloud service provider, Canadian companies and individuals could avoid having the data pilfered by authorities south of the border. But Dragos Ruiu, a Canadian security consultant and founder of the CanSecWest conference, which focuses on applied digital security, is not so sure.

“There is a lot of talk right now about boomerang routing,” he says. “A lot of Canadian internet traffic happens via the U.S., even if it’s between different points in Canada.”

Early in September, the Washington Post published a new slide revealing an NSA project called Upstream, which collected communications on fiber cables and infrastructure as data flows past. It suggests that fiber links and out of the United States were being tapped. Presumably, then, data in transit could be in just as much danger as data at rest.

A lot of Canadian traffic travels via northern U.S. exchange points, such as Buffalo, says Ben Sapiro, co-founder of OpenCERT, a nonprofit Computer Emergency Response Team in Canada, launching in Q4. “If I had your and my IP addresses, I could do a traceroute and then say, ‘Oh, that’s a bad route,’” he says. “Maybe I use the Tor network, or a VPN service provider. The vast majority of users and corporations won’t do this.”

Even if they did, what guarantees do citizens or enterprises now have that a VPN wouldn’t be readable? And recent analysis by Rob Graham, head of Errata Security, suggests that Tor relays using 1024-bit keys can be decrypted by the NSA.

But perhaps Canadians needn’t look south of the border to be worried about data tapping. The Canadian government’s own surveillance policy is also under scrutiny. The Snowden documents revealed that the information needed to decrypt communications was available to a handful of senior officials within the Five Eyes community. Five Eyes, founded in 1946, is an international intelligence-sharing agreement between the United Kingdom, the United States, Canada, Australia and New Zealand.

Further, the operations of Canada’s own secretive foreign signals intelligence agency, CSEC, have also been called into question. Outgoing Commissioner Robert Décary said in his final report this June that “a small number of records suggested the possibility that some activities may have been directed at Canadians, contrary to law.”

The necessary records were unclear and incomplete, he said, adding that records relating to exchanges of information with Canada’s domestic intelligence service, CSIS, were also unclear.

But, OpenCERT’s Sapiro warns against what he calls “security nihilism,” adding that good security measures are still important, and that Canadians shouldn’t simply give up.

“Some parts of cryptography are broken,” Sapiro admits, but he argues that the organization that broke it is but a single adversary. “There are other threats that don’t have this capability. Do I still want to encrypt in encryption and use Tor and patch and build secure applications? Yes, because probably 99 percent of the things I have to worry about as a corporation and a private citizen will benefit from these.” In short, just because the NSA can see what’s travelling over your VPN, doesn’t mean that cyber crooks can, too.

It may be possible to secure your communications more effectively from the NSA, too. The shorter the cryptographic key, the more likely it is that the agency can crack it. Snowden said in an interview with the Guardian newspaper earlier in the summer that properly implemented encryption is still the best protection. Longer key lengths are a good protective measure, says Sapiro (2048-bit keys are a safer bet than 1024-bit keys).

On the positive side, Brian Bourne, founder of the Toronto-based SecTor security conference, argues that this could be a good thing for the Canadian security sector. “It’s creating more opportunities for Canadian companies,” he says, arguing that many companies in the U.S. may decide to store their data on Canadian soil and use Canadian products due to an increasing distrust of U.S. surveillance policy. “One reason that Canadian firms are getting funding is that they are Canada-based.”

While Canadians mull that issue over, Cavoukian is already working on a new concept: Privacy-Protective Surveillance (PPS) by Design, intended to deal with privacy concerns in a world where governments apparently form part of the threat vector. It’s an extension of the original Privacy by Design concept, she says, in which surveillance systems are designed to cherry pick only relevant data, and leave personally identifiable information untouched. Clearly, in this new post-Snowden environment, encryption standards are not the only ones that will have to be revised.
Policy management

THREE’S COMPANY

The promise of governance, risk and compliance technology is alluring, but getting it to work effectively is a different story, reports Alan Earls.

While governance, risk and compliance (GRC) management is nothing new, assembling these three disciplines continues to be challenging as companies look to optimize their compliance efforts to become more cost-efficient.

The growing focus on GRC as a single, unified framework grew out of the passage of the Sarbanes-Oxley Act of 2002 (SOX) and the requirement for publicly held U.S. companies to devise and implement governance controls to support the compliance mandates of SOX. Risk management, an implicit element in the SOX formulation, essentially came along for the ride, as companies recognized the possibility of addressing these topics from a holistic point of view.

But even if one is unfamiliar with GRC, the reality is that its activities are usually already occurring in one’s organization, he says. Internal audit has probably been evaluating processes and controls for years, or IT security has been managing compliance to various access rules. Similarly, business continuity programs are likely reviewing impacts and risks on a regular basis.

“They really function as a risk assessment, evaluate a control, governs according to a regulation or common framework, or evaluates performance, is addressing a GRC function,” says Patrick Potter, GRC strategist at RSA Archer Business Continuity and Audit, a Hopkinton, Mass.-based information technology as a service (ITaaS) provider.

However, implementing a GRC program can be overwhelming because it can touch every part of the organization, engaging different domains and cutting across many management perspectives. But, the good news is that the pieces do fit together and can integrate successfully, although success varies, says Renee Murphy, a senior analyst at Gartner.

“Many companies recognized the possibility of addressing these topics from a holistic point of view. But even if one is unfamiliar with GRC, the reality is that its activities are usually already occurring in one’s organization, he says. Internal audit has probably been evaluating processes and controls for years, or IT security has been managing compliance to various access rules. Similarly, business continuity programs are likely reviewing impacts and risks on a regular basis.

“Really, any function that assesses a risk, evaluates a control, or, alternatively, develop what he calls a ‘tempest-in-the-teapot syndrome,’ where the company ends up trying to do too much too fast.

“A correct and common cost/benefit view is important because this will drive better decisions and corresponding actions,” he says.

Meanwhile, one must continually refine and improve the program. “GRC is a big undertaking, but one that cannot be ignored in today’s world,” Potter says. “It won’t be perfect in the beginning, but planning with the destination in mind, the journey will yield results.”

Importantly, though, organizations should be sure to tie GRC efforts – risk in particular – to security, says Forrester’s Potter. “If you see an organization trying to make 1,500 servers and all its data completely bulletproof, that is all well and good, but leveraging risk management to focus efforts more on core processes and data can save you money,” she says.

Still, she admits, “If you go to 900 organizations you will get 900 different definitions of GRC.”

And, it is precisely that problem – the way GRC has become a kind of catchphrase for vendors and consultants – that alarms Paul Proctor, vice president and distinguished analyst at Gartner. The idea of linking GRC functions across an enterprise is laudable, but difficult to achieve, he says.

“If your organization lacks the maturity to do it successfully, you are not ready,” he says. For instance, Garber clients will sometimes pick five to 10 use cases for deployment of GRC across different areas of a company, but will find that over an 18-month timeframe they are only able to achieve success in one of those areas. “Rather than focusing on the top two or three use cases to start, they spread themselves too thin,” she says.

When he started OCEG, he saw many large companies struggling with these issues, he says. So, he was determined to create an organization that would promote the open sharing of ideas and best practices.

“The group’s mission from the beginning, he says, has resonated most with larger and more complex organizations. However, in the last two years, he has witnessed a renewed focus on the needs of smaller organizations and, at present, growth among the group has increased substantially.

“We believe nonprofit function best when they bring people to the table to solve common problems,” says Mitchell. “We develop standards that we publish on an open-source basis so that companies can easily build their own best practices on these guidelines.”
There was a noticeable chill in the air at Black Hat and DefCon, due to recent action taken against security researchers, reports Dan Kaplan

A few months ago, Matthew Green was asked to advise a small team of undergraduate students who were investigating possible security vulnerabilities in a state’s toll collection system. A part-time research associate at the University of Maryland, Green learned that the students found a way to uncover proprietary information about the system by calling up a publicly available webpage and entering data from public Wi-Fi traffic into a program that could mine data about the system. The students knew that the system was vulnerable and that they were about to do something that could be considered hacking.

Green knew the students he was asked to consult with weren’t up to anything nefarious, but that may not have been enough to ensure they avoided the interest of law enforcement. As a result, they stopped working on the project. “Someone could come along and say, ‘We can prosecute them,’” Green said. “It does have a chilling effect. You can do anything you want, until it involves something, however benign, against a real system. It’s very arbitrary, and it’s difficult to know where the lines are.”

The concern and worry expressed by the cryptography expert is rapidly becoming the norm in the security community, a collective of arguably the world’s most skilled and indefatigable computer enthusiasts. Because of recent examples in which the federal anti-hacking law, known as the Computer Fraud and Abuse Act (CFAA), has been interpreted in ways that permit aggressive prosecutions to be launched, researchers are significantly limiting or scrapping altogether projects that they have invested months or even years on – fearful that they will become the next Aaron Swartz or Andrew “Weev” Auernheimer, and unwilling to join a procession of digital martyrs that is expected to only grow over the next several years. Everyone, it seems, is feeling timid.

In the words of one, the current climate in which to conduct research is “terrifying.” Information security enthusiasts said the nearly 30-year-old CFAA is broadly worded, and if a researcher wants to make an example of a researcher, they easily can because the law, critics have argued, essentially criminalizes normal computer behavior and, to be charged, doesn’t require someone to have had breached security controls or accessed something without authorization.

So it should be no surprise that when the ethical hackers, commonly called white-hats, converged on Las Vegas last month for Black Hat and DefCon, considered the world’s two most preeminent security research conferences, there was something of a dark cloud hanging below the bright desert sun. This year has seen a huge number of submissions – Black Hat, for instance, put on a record 110 talks – but many of the presentations didn’t go quite as far as they should.

Take Brendan O’Connor, a law student at the University of Wisconsin, who also doubles as the CTO of security consultancy Malice Afterthought. O’Connor presented at Black Hat and DefCon on CreepyDOL, a low-cost system that can mine data from public Wi-Fi traffic to create a “really nice visualization engine” on specific people based on the websites with which they interact. It’s an example of how effortlessly one’s privacy can be infringed. The title of his talk was “CreepyDOL: Cheap, Distributed Stalking.”

Wi-Fi publicly sends out data about which sites users visit, so anyone who is listening in can, for example, acquire someone’s photo from an online dating site or their name from Facebook, O’Connor explains. By physically placing nodes – tiny sensor platforms – around a major city, one can amass a profile about a targeted individual.

But this is all theoretical because the bug could allow for the lights of a skyscraper to be switched off. “Essentially, prosecutorial misconduct or prosecutorial discretion used to harm has caused this awesome chilling effect,” said O’Connor, who authored an amicus brief that was recently filed and signed by about a dozen other researchers calling for the release of Auernheimer, the 27-year-old researcher and self-described internet troll who took advantage of an AT&T website flaw to expose the email addresses of roughly 120,000 iPad users, including some high-profile people like New York Mayor Michael Bloomberg.

But Auernheimer enlisted no hacking tools and bypassed no security technology to amass the information. Everything was publicly available. He and a colleague merely built a script that expedited the process of collecting the email addresses. Gawker wrote a story about the “hack,” but didn’t publish the personal information.

That didn’t prevent Auernheimer from being slapped with identity theft and conspiracy charges, with the
government arguing that he unlawfully accessed or exceeded authorized access to a protected computer. He lost his court battle, and in March, was sentenced to 41 months in prison.

By prosecuting white-hat researchers – even ones who have a muddled reputation, as Auerheimer does – they become more reticent about doing their work, despite the fact that it is typically performed for the public good and rarely for profit. Meanwhile, the treatment of digital researchers runs in stark contrast to those who have evaluated the safety of physical systems over the years, including automobile braking systems or the suspensions on a bridge.

FBI to go after Weev was,” said Shane McDougall, a veteran security researcher and principal partner at Tactical Intelligence, a strategy company. “Right now, hackers are the only ones pining these systems, because security researchers aren’t. [The FBI has] really done American consumers a disservice.”

Auerheimer’s plight may not have received as much publicity as it did if not destroyed all of the code he had developed for a research project he was working on, known as SchmoozeKit – described as a tool that mines multiple sites for information and can be used offensively or defensively by consumers or governments – even though he believed nothing he had done was illegal.

“It’s really not a good time right now to be a security researcher,” admitted McDougall, who was planning to present his work at next year’s Chaos Communication Congress in Germany. “I’d rather throw away 4½ months of code rather than do 8½ years in a federal prison.”

He said he likely will rebuild the code if Auerheimer wins his appeal. In the meantime, though, McDougall is a case study for any district attorney wondering if he or she has the power to force a security researcher to fold their hand.

Protecting the researchers Trey Ford, general manager of Black Hat, said the annual conference in Las Vegas supports researchers and wants to help them avoid any trouble. When their talk is accepted, presenters are offered assistance in disclosing any vulnerabilities they may have discovered to the appropriate vendors. In addition, they are encouraged to contact the Electronic Frontier Foundation (EFF), a digital rights advocacy group, for pro bono legal aid.

“We’re going to do everything we can to protect a researcher from themselves,” Ford said.

Despite this, researchers have become inured to entrapping the manufacturers of the products with which they tinker.

Sometimes, that has resulted in lawsuits or even court-levied gag and cease-and-desist orders. Rarely has it resulted in arrest, though at DefCon in 2001, Russian encryption expert Dmitry Sklyarov was charged under the federal Digital Millennium Copyright Act with violating copyrights on Adobe software. The charges eventually were dropped.

Since incidents such as that, security researchers have largely built a more positive relationship with the U.S. government – so much so that feds have been largely accepted, if not welcomed, at conferences like DefCon. But that all seems to have come crashing down with Swartz’s death, the Auerheimer conviction, and to an equal, although not entirely related, extent, the mass National Security Agency spying apparatus exposed by whistleblower Edward Snowden.

Ford blames the downward trend on case law, which he said makes it easy for prosecutors to mount cases against researchers. This results in shaping public opinion, and the average person becomes further confused about the positive role that ethical white-hat hackers play.

“It’s so easy to misinterpret what we’re doing, and without the right framework of support, we look like we’re doing bad things,” Ford said.

Charlie Miller, a regular presenter at security conferences across the world, and who is best known for his research into Apple devices and car computers, said his peers are especially unnerved to see the treatment of researchers play in society. “I think that right now, security is a mess, and the one thing we have going for us is a small number of people who make it their entire job to go and find these bugs,” he said. “Maybe they’re announcing it in splashy ways, but at least they’re announcing it.”

Not everyone is going to play it safe, however, either because they don’t know how far it is too far or because they are adamant about challenging the status quo.

But, even though a CFAA reform bill has been introduced in both the U.S. House and Senate, Ford said the outlook is likely to get worse before it gets better.

“The fact is, [these prosecutions] will ruin several people’s lives along the way,” Ford said. “That’s just how this works. It’s going to be someone from our ranks.”

An early version of this article appeared on our website.
Application security

Though it is difficult to quantify ROI for security initiatives, investment in application security is logical for the enterprise, reports Jim Romeo.

DOLLARS AND SENSE

In the past year, the University of California, Berkeley, has doubled its security budget—already in the millions—to guard against a multitude of network intrusions attempted every single day.

Like many other organizations, the school depends on extensive collaboration with developers and stakeholders, and uses sophisticated applications to solve complex problems. The preeminent challenge, however, is ensuring that these applications are capable of withstanding exploitation from external actors intent on accessing valuable proprietary and student data.

As application security continues to face challenges, so does corresponding spending to safeguard against known vulnerabilities. Which tools and technologies organizations invest in is a critical concern, though many point out that security objectives are often misaligned with actual needs.

A recent survey of 110 diverse IT organizations—sponsored by Oracle and conducted by IDC Research's CSO Custom Solutions Group—found that "most IT security resources in today's enterprise are allocated to protecting network assets, even though the majority of enterprises believe a database security breach would be the greatest risk to their business." While the findings indicate that nearly 66 percent apply an inside-out security strategy, only 35 percent base their strategy on outside-in protection.

When it comes to actual spending, 67 percent of IT security resources—excluding budget and staff time—are allocated to protecting the network layer, and a mere 23 percent of resources were allocated to protecting applications or databases.

This focus will help one select from the many different tools and technology. Shiny new security products, like servers, applications and databases, according to the same research. The study found that the majority expect to spend the same or more this year as compared to last, while next year, 59 percent expect to spend at an even higher level than at present. In fact, according to separate research conducted by Gartner, spending on IT security will top $86 billion by 2016.

David Canellos, president and CEO at PerspecSys, a McLean, Va.-based cloud data protection gateway solution provider, advises his clients to inventory their company's applications and data to know what is truly sensitive. He emphasizes the importance of mapping a security strategy to capital outlay. "The first step is to create a solid IT strategy to drive their investment road map," says Canellos.

Building that map

CSOs and CIOs are challenged with developing a carefully planned portfolio of security tools, techniques and personnel to strengthen applications and networks. Francis Cianfrocca, chairman and CEO of Bayshore Networks, a Staten Island, N.Y.-based provider of next-generation firewall technology, emphasizes the need to map out a security plan and says IT leaders could make uninformed investment decisions without one. "You need plans for multiple approaches: defense-in-depth, risk management or a combination of both," he says. "You will need to have a plan in place that shows what your posture is like and what you want it to be."

There is no cookie cutter or best practices approach for application security, he adds. "Industrials sectors, financial, manufacturing, service industries, etc., have not yet emerged with applications by market," says Cianfrocca. "The threat is far ahead of the best practices, and the gap between threat and ability to defend is always being tested."

Knowing your organization’s true security needs is elementary to an investment road map, says Brian Contos, VP and CISO of the advanced threat protection group at Blue Coat Systems, a Sunnyvale, Calif.-based provider of web surveillance, content filtering, security and WAN optimization solutions. "Don't invest in trends and products," he says. "Invest in solutions specific to your organizational needs. Shiny new security toys of today collect, dust tomorrow if they don't serve a specific, necessary purpose."

This focus will help one select from many different tools and technology. But, IT managers must proceed with caution.

"Do not take a vendor's behavior and performance claims as gospel," says Brian Monkman, perimeter security programs manager at Mechanicsburg, Pa.-based ICSC Labs, an independent division of Verizon which provides third-party testing and certification of security and health IT products.

“One enterprise’s infrastructure and traffic mix will be quite different from another,” he says. He further cautions against investments in security technology without regard to its specific application. ICSC has determined that product behavior and performance capabilities can vary significantly, depending on the environment and traffic mix a product has to handle. "Nothing beats robust proof-of-concept testing,” Monkman says.

But, he also emphasizes the importance of including training as a security investment. Training will enable staff to learn how to configure and manage a particular device. Such education, he says, should also target non-IT employees to demonstrate how to reduce vulnerability to common attacks—like phishing and social engineering—and offer basic online safety, such as instructing on the use of robust passwords and how to be aware of websites that might prove troublesome.

A focus on staff and work behavior is essential to a sound and secure working environment. “Typically, money is better invested in people and processes focused on security rather than technology, which continually changes,” says Jeff Krull, a partner and information technology expert in the governance and risk management group of ParenteBeard, an accounting firm based in Philadelphi. “An intrusion detection system is certainly helpful in identifying vast vulnerabilities, but, if no one reviews and reacts to the data, the investment does not prove effective.”

Invest in solutions specific to your organizational needs.

— Brian Contos, Blue Coat Systems

1. Investigate – Check the packages and libraries you incorporate into your application for known vulnerabilities. Search for the package names and versions on md.nist.gov to update packages to fixed versions. It’s a low-cost process that will improve application security.

2. Test – Use automated static testing to scan your code for common vulnerabilities, such as SQL injection and XSS. Follow the remediation recommendations to fix the code. Perform the testing early in the development cycle so code changes are less disruptive, saving valuable development time.

3. Prioritize – For risky apps that are internet-facing or handle financial info or PII, have a manual penetration tester review the app during user-testing phase. For best ROI, have them restrict testing to the issues that automated testing won’t find, such as sensitive data leakage, authorization errors and business logic vulnerabilities.

4. Educate – Use e-learning to train developers about common application security coding errors and how to avoid them. Make sure the classes use examples for the programming languages the developers are using.

5. Validate – Are you purchasing a commercial app or having a web or mobile app built for you? Put contractual requirements in place for the app developer to perform best practices one through three above. Seek third-party validation of this and require the app vendor to pay for it.

Chris Wysocki is the CTO and CISO of Veracode, an application security vendor based in Burlington, Mass. He provided us with best practices to achieve the most effective investment in application security.

1. Investigate – Check the packages and libraries you incorporate into your app for known vulnerabilities. Search for the package names and versions on md.nist.gov to update packages to fixed versions. It’s a low-cost process that will improve application security.

2. Test – Use automated static testing to scan your code for common vulnerabilities, such as SQL injection and XSS. Follow the remediation recommendations to fix the code. Perform the testing early in the development cycle so code changes are less disruptive, saving valuable development time.

3. Prioritize – For risky apps that are internet-facing or handle financial info or PII, have a manual penetration tester review the app during user-testing phase. For best ROI, have them restrict testing to the issues that automated testing won’t find, such as sensitive data leakage, authorization errors and business logic vulnerabilities.

4. Educate – Use e-learning to train developers about common application security coding errors and how to avoid them. Make sure the classes use examples for the programming languages the developers are using.

5. Validate – Are you purchasing a commercial app or having a web or mobile app built for you? Put contractual requirements in place for the app developer to perform best practices one through three above. Seek third-party validation of this and require the app vendor to pay for it.

— Brian Contos, Blue Coat Systems

In the past year, the University of California, Berkeley, has doubled its security budget—already in the millions—to guard against a multitude of network intrusions attempted every single day.

Like many other organizations, the school depends on extensive collaboration with developers and stakeholders, and uses sophisticated applications to solve complex problems. The preeminent challenge, however, is ensuring that these applications are capable of withstanding exploitation from external actors intent on accessing valuable proprietary and student data.
...we’re talking about limiting loss.”

—William Mabon, BAE Systems

Manohar Ganshani, a practice partner and network leader of governance risk and compliance at Wipro Consulting Services, a global information technology, consulting and outsourcing company with corporate headquarters in Bangalore, India. “What will be your response if at the end of year you find there were no events? Security investment is an expense that should be viewed to decrease the risk of loss and the cost of business operations. It does not create anything tangible. Therefore, doing a cost effectiveness analysis is more appropriate than calculating a return on security investment.” The truth is, ROI becomes more of an exercise in cost avoidance and limitation of loss, than revenue generation, he says.

“We should not talk about ROI with regard to security investments,” says William Mabon, director of cyber security products for BAE Systems, a global defense, aerospace and security company with U.S. headquarters in Arlington, Va. “We lose credibility with the CFO when we do. By definition, we’re not talking about security practices that are generating income. Rather, we’re talking about limiting loss.”

Mabon references two popular alternative frameworks: return on security investment (ROSI) and annualized loss expectancy (ALE). “ROSI, compared to ROI, replaces returns with the risk in dollars, multiplied by the percentage of the threat mitigated by the investment,” he says. “ALE is the anticipated loss from a single event multiplied by the expected rate of occurrence.”

Investment in IT security is a continuous process that must balance need with available budgetary resources. Security tools, technologies and best practices do not just mitigate IT security risk, but mitigate overall business risk posed from security threats on the IT landscape. CIOs, CSOs and other company leaders need to carefully evaluate all tools and solutions available for their specific need.

Enterprises should be asking vendors for evidence that their track record reflects continual development and improvement, says ICSA Labs’ Monkman. “Additionally, enterprises should look at the history of independent third-party security testing the vendor has subjected their product to.”

Monkman also says that just because security threats change daily, it doesn’t necessarily mean that an investment in a security solution or specific technology won’t last a while and stay ahead of threats.

Says Monkman, “Any network security product vendor worth its salt will be constantly running to stay ahead of the bad guys.”

BEST PRACTICES: App sec management

Saru Jain is a security consultant for Tech Mahindra in Mumbai, India. He offered up some basic, but essential management practices specific to application development to improve security effectiveness for any budget. They are as follows:

1. Integrate security into the software development lifecycle – Security should start from the conception stage and cover all stages of the development lifecycle, including operations reviews. This practice has a very high return – both in terms of time saved and in overall cost reduction – but more importantly it will ensure that vulnerabilities in the application have the best chance of getting weeded out.

2. Conduct regular assessment and audits of web applications – Web applications represent one of the weakest links in the stack and due to their exposure are also the most vulnerable target. Regular assessments helps in early detection of vulnerabilities and can protect against potential exploits.

3. Use multiple gatekeepers and a “defense-in-depth” strategy – Invest in security tools at the perimeter, in the network and for applications. Using a layered approach to security can significantly reduce the chances of a successful attack.

A U.K. college provides its “digital natives” with a secure environment that can be accessed anywhere from any device. Greg Masters reports.

To keep up with advancements in mobile technologies and the expansion of its many campuses, Birmingham Metropolitan College (BMC) faced a daunting challenge: Offering anytime/anywhere access – in a secure manner – to its students and staff, whether they were on campus, at end user workstations or on mobile devices at remote locations.

BMC consists of eight campuses around the city of Birmingham in the center of England, a two-hour train ride northwest from London. It has 35,000 students and 1,300 staff members, and provides services for a range of learners – from teenagers to college-level to post-graduate positions. Additionally, it offers continuing adult education courses and, working with global organizations, provides an apprenticeship program to train students for future positions.

Jamie Smith, director of systems and policy development at BMC, and his team, understood that new students were by nature “digital natives.” To maintain leadership in a competitive educational landscape, they were tasked with providing a curriculum model accessible from the campus, office and home. The goal was to create a seamless learning ecosystem. This included a cloud environment for classes throughout the college’s various programs, as well as new social community options for students and staff to help drive collaboration.

However, Smith and his team also knew that security had to be a priority in the implementation.

Smith’s team looked at technology offerings from several leading vendors, but ultimately decided to leverage IBM Virtual Desktop and IBM SmartCloud as Smith and his staff found that the virtual desktop
Case study

“The key point...is to use technology to...help reinvent education.”

— Jamie Smith, Birmingham Metropolitan College

offered new security benefits that were not achievable in a traditional desktop environment. And, Smith says, as the school adopted these new technologies, the security benefits of the cloud were an added bonus.

Also, Smith’s team was convinced that representatives from IBM were not merely trying to sell software, but were more interested in building a lasting partnership with the college. Further, the IBM solution offered the flexibility that the college needed to build its secure cloud and open community environment. IBM SmartCloud delivers secure and scalable hosted IT infrastructure with on-demand access to virtual server and storage resources, says Martin Borrett, director of the IBM Institute for Advanced Security Europe. “IBM protects cloud environments with cloud security strategies and a comprehensive portfolio of solutions that span the entire cloud lifecycle and all security domains,” he says. “With an emphasis on visibility, control and automation, IBM cloud security solutions help meet regulatory compliance and defend against the latest threats, delivering a robust, security-rich cloud tuned to your specific needs.”

The IBM solutions also take into account the required “safeguarding legislations” in the United Kingdom. The technology helps to ensure that students are not subject to any inappropriate materials on the collaborative social networking platforms provided by BMC. The implementation reaches across the entire BMC network, and Smith sees opportunities to implement further deployments in the near future, but no action is underway at the moment.

Implementing cloud-based and social media technologies has changed the way that BMC operates from a security perspective, Smith says. Educating students and staff on how to properly use the new cloud environment and social communities has been the biggest challenge, Smith says. “There are many ways to do this with the IBM solutions that the college is using, such as implementing an acceptable-use policy, tagging data to track important documents, as well as rigorous training and education,” says Smith.

But, there are always new threats with which to contend. Currently, Smith and his team are concerned with keeping up with the extreme pace of advanced persistent threats to network security. Other challenges include bring-your-own device (BYOD) and social media. But, the IT department at BMC is assured that new tools will be there to assist. “The key point for Birmingham Metropolitan College is to use technology to help achieve its goals to reinvent education,” says Smith.

Whether on campus or from remote locations, students and faculty at BMC can securely log in to the school’s network.

Your online life is an open book – maybe

Email security is not just about encryption. In fact, it is not always necessary to encrypt. The invitation to the company Christmas party probably is not confidential enough to warrant encryption, but a message that contains HIPAA information certainly is. Many of the products we looked at this month have the ability to apply a rule set and, if the rule that says “confidential” fires, the message is encrypted.

These products contain, then, a form of data leakage prevention (DLP) that applies to emails and their attachments. The tools look at the message and attachment in clear text and decides what to do with it. It may prevent the message from going entirely (it contains proprietary information that should not be exfiltrated from the organization), it may force encryption (the content is sensitive, but it can leave the organization), or it may do nothing and simply send the message (this is not sensitive at all, according to the rule set).

While we had fewer products than we expected for this group, those we did have were solid. Not all of these tools do the same thing, of course. Email security and management is a rather fuzzy description and the functionality offered can be equally fuzzy. For example, some of our products touting encryption provided onboard encryption, while some forwarded the email on to a third-party encryption gateway. Some provided secure mailboxes in the cloud which recipients could use to extract their encrypted messages, while some offered decrypting readers.

Most of the products were policy-driven – as one might expect. Policy based control is the current state of the practice for most information security tools and these are no exception. The policy engines tended to be robust and fairly easy to use, and system configuration generally was straightforward.

Overall, it was an interesting month with SC Lab Manager Mike Stephenson putting these products through their paces. The test bed was our usual for email-based products and we were pleased with the ease with which they set up and ran.

— Peter Stephenson, technology editor
Email security/content management

Keeping email secure is a multi-dimensional task, says Technology Editor Peter Stephenson.

The idea behind a comprehensive email security tool is that it must do whatever one needs it to do, and admins need to be able to implement and oversee it fairly easily. Users should not be troubled by it either, so ease of use and seamless deployment and administration all are important.

So, what do these tools actually do? One big thing that we saw was the increase in appliances that sit as front-end gateways and enforce email policies. That is a big plus for this year's group. Almost all are policy-driven – and the big moving force behind that functionality is compliance. Just as with many other product categories, compliance is driving email security and with compliance comes policy. The ability to turn regulatory requirements into executable, manageable, reportable policies is the cornerstone of much of today's security.

We still see organizations that conduct compliance audits for the sake of checking off the boxes on the audit form, but more and more organizations are hiring the bullet when it comes to cost and acquiring tools that do what needs to be done. Achieve compliance while actually keeping the enterprise more secure. These tools help speed us toward the day when “compliance does not equal security” may be a thing of the past. The products that we looked at this month certainly are headed in that direction.

Once one has determined what is needed in the environment, the path is clear to start looking at products. Let's begin by examining how to make that determination. First and foremost, potential buyers need to look at the third-party products and services with which the mail security tool will interface. The obvious one is Microsoft's Active Directory, but there are others. For example, will the user be encrypting email? Then, a tool that talks to the in-house encryption device/ software and tells it when to encrypt might be called for. Not all emails need to be encrypted, and if admins can take the decision out of the user's hands so much the better.

Interestingly, behind regulatory requirements – and, probably ahead of them from the end-user's perspective – is spam control. If one doesn't have a tool to control spam, look for a tool that includes that functionality. Another important piece of activity is anti-phishing capability. From a pure security – not just compliance – perspective, this is a big deal given that a huge percentage of breaches begin with phishing.

Anti-malware has been with us for a long time – as has encryption. However, the integrated nature of some of these products pulls us deeper into a secure environment by deeper analysis of both incoming and outgoing emails. As far as incoming, we care about spam, phishing and malware. For outgoing, we're concerned about data leakage prevention (DLP). This is another big deal, and this crop of products takes DLP very seriously.

That's primarily because there are myriad ways data can exfiltrate an enterprise. Not all of them are email, to be sure, but email is a big contributor to the problem. I faced a case a few years back where a well-meaning employee was sending Social Security numbers (SSN) to his public email so that they would not get lost as he changed jobs. He did not realize that the cut-over between email accounts took care of that. Had we not had DLP working at that moment, we never would have known. Tying DLP to an email gateway is an efficient way to stop that exfiltration.

In addition to multiple exfiltration channels, there are various types of data that can escape. Some need to be handled in unique ways. For example, there are regulatory requirements that drive DLP in the realm of personally identifiable information. There are none that govern how one manages exfiltration of trade secrets, but both are equally important. The problem is that it's relatively easy to spot a SSN on its way out onto the internet. It's not so easy to spot trade secrets. If one needs to make this distinction, make sure that the product selected has a lot of granularity and flexibility in its policy engine.

Specifications for email security and content management tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Provides email content filtering</th>
<th>Provides built-in email encryption</th>
<th>Scans outbound email for sensitive data</th>
<th>Scans email for viruses and spyware</th>
<th>Provides spam protection</th>
<th>Includes prebuilt regulatory compliance templates</th>
<th>Includes prebuilt email policy templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axway MailGate SC v5.2</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Barracuda Networks Spam &amp; Virus Firewall</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Cisco Email Security Appliance</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>EdgeWave ePrism Email Security v9.0</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>F-Secure Protection Service for Email v7.2</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Fortinet FortiMail</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>F-Secure Email Protection</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>McAfee Email Protection</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>WatchGuard Technologies XCS 570 v9.2</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
Axway MailGate SC

The MailGate SC from Axway incorporates email security with safeguard collaboration functions. It can provide full email security — including protection from inbound spam and viruses; outbound content management, including regulatory compliance policy management; and email encryption options, as well as additional secure file-sharing through its integrated DropZone Secure Collaboration feature. DropZone can be used by employees to securely share files both internally and externally without having to use other cloud-based file-sharing platforms.

We found the initial deployment and setup of the MailGate appliance to be straightforward and easy. Once we had the device connected to our network, we had to use a web browser to access the web-based setup wizard and management interface. The first time we accessed the appliance through the browser, we were directed through a setup wizard that helped us configure the basic settings, including network and IP settings, licensing and email relay settings. After we completed the wizard, we were able to access the administration interface through our browser.

The first time we noticed after logging into the web interface for the first time was the dashboard. The MailGate's dashboard provides a solid mix of system information and mail statistics in a lucid and organized layout. Aside from the dashboard, we found the rest of the management interface to be well-organized as well. We had no trouble navigating through the various menus to perform advanced configuration tasks. Further, we found this solution to possess some powerful email policy functions. The MailGate comes with some default policies in place, including regulatory compliance policies for GLBA and HIPAA, among others. All policies can be granularly applied based on several factors, including sender, recipient, content or tags.

Documentation was comprised of a number of PDF manuals and guides. Included were full user and administrator guides. The administrator and implementation guides provide an excellent amount of detail on how to deploy, configure and manage the appliance. The user guide is geared toward helping users get acquainted with the Secure Collaboration features of the appliance. We found all documentation to contain clear, step-by-step instructions and configuration examples, but while there were many screen shots throughout the administrator documentation, there were none in the user materials.

Axway offers customers both eight hours a day/five days a week and 24/7 technical support levels as part of a contract. Support options offered include phone- and email-based technical assistance, as well as access to a large online portal. This site contains several resources, including a knowledge base, product documentation and user discussion forums. Customers can also purchase mission critical support, which adds access to a dedicated technician and onsite help.

At a price starting at $8,000, we found this product to be an excellent value for the money. The MailGate SC offers many email security and policy options and secure file sharing and collaboration features in an easy to deploy and manage appliance. We found this tool could meet the needs of almost any size environment or organization — with a price to match.

Barracuda Networks

Spam and Virus Firewall

The Spam and Virus Firewall from Barracuda Networks provides solid inbound and outbound email security, functionality through a feature-rich appliance. This solution features protection from spam, phishing, spyware and viruses, along with email encryption and data leakage prevention policies to ensure that sensitive data is handled properly. For added scanning capabilities, the Spam and Virus Firewall can also be deployed in a hybrid configuration using Barracuda’s Cloud Protection Layer.

The initial setup and deployment of the offering took us just a few minutes to complete. To get the appliance up and running, we simply connected a keyboard and mouse to the appliance itself, which allowed us to access the console to configure network and IP information. Once the IP address was configured and the appliance was connected to the network we could access the web-based management console. Overall, we found this console to be easy to navigate due to an intuitive tab-based navigation structure. After a few minutes inside the console, we had all our mail settings configured, as well as an email policy. This product must be configured manually and there are no configuration wizards to assist with deployment. To speed up initial deployment, we would like to see a wizard that at least assists in the initial configuration.

We found this solution to contain a number of excellent policy options. Administrators can create email policy that filters attachment types, IP addresses, rate controls and sender and recipient filters. Aside from the various filters, this tool also includes a few predefined data leakage policies, such as credit card and Social Security numbers. The number of predefined policies is quite limited, but custom policies can be easily created with a few clicks of the mouse. Once policy is defined, the Spam and Virus Firewall can be set to scan the subject, body or attachments of an email, and take actions — such as block, quarantine, encrypt or redirect — based on content.

We found all documentation to contain a large amount of screen shots, diagrams and configuration examples, as well as clear, step-by-step instructions. Barracuda Networks offers basic eight-hours-a-day/five-days-a-week phone support at no cost to customers. Customers can also purchase additional aid, including enhanced 24/7 phone- and email-based technical assistance. Also available at no additional cost to customers are several online options, including a full product knowledge base, documentation downloads and a user community forum.

At a price just shy of $4,000 for the appliance, plus $1,399 annually for updates, we found this solution an excellent value for the money. While Barracuda Networks Spam and Virus Firewall does not come with as many predefined templates as other products in this space, it stands well on its own merits with easy configurability and flexible deployment options. We found it to contain a complete feature set that provides solid email security and encryption at a reasonable cost.
Cisco Email Security

The Cisco Email Security virtual appliance offers a full set of inbound and outbound email security and control features. With this product deployed, administrators can set granular inbound and outbound policies that control inbound spam and viruses along with outbound data leakage prevention and encryption, among other features. To ensure email is secured and handled properly both leaving and entering the enterprise, this solution features a combination of multi-anti virus and anti-spam engines, along with highly configurable email policy filters.

We found it to be straightforward to deploy and configure. We first had to download the OVF [open virtualization format] image of the appliance and import it into our VMware VSphere environment. Once we had the template imported, we started the appliance up. After it had completed booting, we were able to access the web-based management interface for configuration. When we accessed the management interface for the first time we were greeted by a setup wizard which helped us configure basic IP and network settings, as well as a security policy. Once the wizard was complete, we were able to fine-tune our configuration using the management console, which – with its clean and organized layout – we found easy to navigate.

We found this appliance can be deployed to suit all environment types – from small to large and everything in-between. The Cisco Email Security appliance offers a lot of configurability for features and policy. Filtering can be applied based on users and groups through integration with Active Directory, file types and keyword and dictionary matches. When policy rules are met, several actions can be taken on the message, including quarantine, encryption of the message, various notification options, and adding of disclaimers, among other choices. This tool can also be deployed in a hybrid scenario in which all inbound email is filtered by Cisco Cloud Email Service and outbound email is handled by the on-premises appliance. This provides additional flexibility for larger environments requiring more scalability.

Documentation included several installation and administration guides in PDF format. Also included was a short guide that provided details on deploying the virtual appliance in the network using VMware vSphere. We found all manuals to be well-organized and to contain clear, step-by-step installation and configuration instructions, as well as screen shots and configuration examples. Cisco provides software technical support as part of the subscription cost that customers are already paying. Support includes 24/7/365 phone- and email-based technical aid, as well as access to a large assistance area on the vendor website. This includes a knowledge base, user forum, product documentation downloads and many other resources.

At a cost of a little more than $3,800 for a one-year subscription for 100 to 199 users, we found this product to be a reasonable value for the money. The Cisco Email Security appliance includes a comprehensive feature set that is quite easy to manage and provides flexible deployment options. However, we did find that for some environments the subscription pricing model may be a little cost prohibitive.

Overall Rating ★★★★★
Strengths Full email security appliance with many deployment options.
Weaknesses Subscription-based pricing may become expensive on ongoing basis.
Verdict Solid product, though a bit pricey.

EdgeWave ePrism Email Security

The ePrism Email Security appliance from EdgeWave offers email security features such as inbound and outbound content filtering and email policy enforcement, anti-spam and anti-virus. This appliance features solid protection from malicious email threats, including denial-of-service attacks at the perimeter, and its Zero Minute Defense filter can identify emerging threats immediately and then create protection rules on the fly to block malicious or harmful email.

We had little trouble with the initial setup of the appliance, but we found the configuration to be slightly difficult. The initial setup is done by connecting the appliance to the network and then using a browser to access the initial setup wizard. This wizard contained clear steps and we were through it in just a few minutes. After the setup wizard was complete, we were taken to the web-based administration console. This is where we started to run into some confusion. Overall, we found this appliance to be slightly daunting to configure as we had to spend quite a bit of time getting comfortable navigating the management console and configuring the product.

With that said, this solution does feature some excellent policy and configuration options. Administrators can configure content filters and email policies that protect sensitive data from leaving the enterprise unprotected. Through the onboard data leakage prevention and encryption modules, if a message is found to contain sensitive data, rules can be put in place to require the message be encrypted before leaving the enterprise. Also, we found this solution to contain a good amount of predefined regulatory compliance filtering policies ready to go right out of the box. Adding to the overall flexibility is its deployment options. It can be deployed as an on-site appliance or hosted as a SaaS offering. Documentation included a getting-started guide along with an administrator guide and a few other pieces of supplemental manuals. The getting-started guide provided a good amount of detail to get the appliance up and running in the environment with a basic configuration. The administrator guide provided a good overview of configuring the appliance and its features. We found all documentation to contain a reasonable amount of screen shots and configuration examples along with clear, step-by-step instructions.

EdgeWave offers full 24/7 phone- and email-based technical support to customers as part of the ongoing subscription price. On top of phone and email assistance, customers can also access a large support area on the vendor website that includes many resources, such as a knowledge base, documentation downloads and videos tours. At a price starting at a one-time cost of $1,500 for the appliance itself, plus an ongoing subscription cost of $12 per mailbox per year, we found this to be a good value for the money. While the subscription-based model can be pricey on an ongoing basis, we found this product includes some excellent capabilities due to its hosted deployment model. EdgeWave’s ePrism Email Security is an overall good value once it is properly configured and running in the environment.

Overall Rating ★★★★★
Strengths Hosted email security suite with many configuration options.
Weaknesses Difficult to configure at first.
Verdict Take your time with this one; it takes a bit of learning to get it moving in the right direction.
F-Secure Protection Service for Email

The F-Secure Protection Service for Email is a fully hosted email security offering that can work in tandem with an already existing email server to provide a complete set of email security features. This hosted service is built on a platform from a strategic partner – the Proofpoint Email Security – and features protection from spam and other email-based threats, and offers email encryption, a highly configurable policy-based email firewall and integrated data leakage prevention.

Since this tool is hosted by F-Secure, we found initial setup to be quite easy and straightforward. To get started we simply had to login to our web-based management console and complete a few simple configuration steps to begin filtering email. Overall, we found the administration console to be easy to navigate with an intuitive layout. The only place we ran into trouble was becoming familiar with all the various menus and configuration options. With so many things to configure, we became slightly overwhelmed.

With that said, this solution features many comprehensive policy controls ready to go right out of the box. It features several regulatory compliance policy templates onboard, as well as many default rules to provide solid filtering and protection capability. We also found this product to integrate well into the existing environment with seamless integration with Microsoft’s Active Directory and Outlook. Documentation included a short quick-start guide and a full administrator guide. Much of the supporting material available, however, has not been fully updated to reflect the hosted service, so we found some of the guides to be confusing as they contained reference to Proofpoint’s products and not F-Secure’s. We would like to see an instruction set that is specifically written for the hosted service and not the available appliance version. We also found that while much of the documentation contained quite a few step-by-step configuration instructions, there was a lack of screen shots and configuration examples to help further illustrate advanced configuration tasks.

F-Secure offers eight-hours-a-day/five-days-a-week phone- and email-based basic technical assistance as part of the subscription fee. At an additional cost, customers can also gain 24/7 premium aid and other options, such as a dedicated support technician. All customers can also access a large online help area via the vendor website. This includes a full knowledge base, user forum, support news and resources and support contact information.

At a price starting at $12 per license per year and going as low as $2 per license per year, we found this tool to be a good value for the money. F-Secure Protection Service for Email is a feature-rich hosted email security platform that can meet the needs of almost any size environment. While it does require an ongoing subscription cost, it is completely hosted, so there is no overhead for equipment and hardware maintenance, which adds to its overall value. We also found that this offering is easy to configure and manage, so there is less administrative effort required on an ongoing basis.

Fortinet FortiMail-200D

The FortiMail 200D from Fortinet features many email security features bundled into an easy-to-manage appliance. It includes anti-virus, anti-spam, onboard identity-based encryption, and content filtering and data leakage prevention through the use of many predefined policies. This product also features solid email security and data leakage policy templates onboard and ready to go right out of the box. The FortiMail appliance comes preloaded with regulatory compliance templates for PCI DSS, HIPAA, GLB, and SOX to ensure sensitive data is handled properly if it needs to leave the organization. If data does need to leave securely, this solution provides flexible encryption options.

Documentation included quick-start, installation and administrator guides and other supplemental materials. The quick-start guide lucidly detailed the initial setup and configuration of the appliance, but, as we said, did contain an error. In the step for connecting to the web interface for the first time, it just gives the IP address as the URL, which is a problem because it appears that just putting the IP address defaults to the onboard user portal. To get to the management console, the URL needs to be amended with /admin. This small problem in the documentation required us to troubleshoot as to why we could not get access to the management console. After several factory resets, we looked in the administrator guide and found the proper address.

Fortinet offers eight-hours-a-day/five-days-a-week support for the first year as part of the initial purchase price. This plan includes access to both phone- and email-based technical assistance. Enterprises needing 24/7 aid can upgrade for a slight extra cost. All customers also get access to a large online support area that includes a knowledge base, user forums, documentation and product downloads, and video tutorials, among many other excellent resources.

At a price just shy of $5,700 for the appliance, one year of support and one year of anti-malware and anti-spam updates, we found this solution to be an excellent value for the money. While it may be designed for smaller branch office environments, it has the features and functionality of a large enterprise-class mail security appliance. We found that the combination of features and ease of use and management make this appliance an overall great value.
McAfee Email Protection

McAfee Email Protection offers full-scale email security and content management in a single appliance with flexible deployment options. This tool features scanning of both inbound and outbound mail and provides protection from spam, viruses and other malicious email content. This product also features several encryption options onboard and ready to go, as well as email compliance policy and data leakage prevention functionality.

This solution can be deployed as a virtual or hardware appliance, hosted service or hybrid installation. For our evaluation, we chose to deploy the virtual appliance. We found initial deployment to be quite easy. It took us little time to get the appliance up and running. To get started we first had to load the OVF [open virtualization format] template into our VMware vSphere environment and then we powered up the appliance. After that, we were greeted by a setup wizard which guided us through the steps necessary to get the appliance going with an initial configuration.

After we completed the wizard, we were able to do the rest of the configuration and management using the intuitive web-based management console. We instantly felt comfortable navigating around throughout the console and finalizing our configuration. This appliance comes preloaded with a plethora of compliance policy templates that are ready to go right out of the box. We found it to be quite easy to define email security policy using these templates along with the policy editor. We also found the dashboard to be well designed with many customizable views, including several helpful charts and activity graphs.

Documentation included a getting-started guide and a full administrator guide in PDF format. The getting-started guide was geared more toward the initial configuration of the appliance and overall management. We found the administrator guide to contain an excellent amount of detail and step-by-step configuration instructions, but it lacked screen shots and visuals.

As part of the subscription cost, McAfee offers a gold support program, which includes 24/7 phone- and email-based technical aid. Customers can also purchase additional assistance through a wide range of available options. Customers can also access a large support area on the vendor website that includes knowledge base, product documentation downloads, customer service portal, FAQs and many other tools.

At a subscription price ranging from $25 per user per year on the high end down to $4.75 per user per year, this product does come with a reasonable-size price tag. We found, however, that the McAfee Email Security platform is a solid value for the money for almost any size environment. Not only is it available as a virtual or hosted appliance to cut down on overall cost, it is easy to manage and includes a large amount of predefined templates and settings that are ready to go right out of the box.

WatchGuard XCS 880

The XCS (Extensible Content Security) Appliance from WatchGuard provides solid email security and email content management in one easy-to-manage appliance. This product features protection from email-based viruses, spam, spyware, phishing and malware attacks, along with scanning both inbound and outbound email for policy violations and data leakage.

We found it to be quite easy to deploy and configure. Once the appliance was connected to the network and powered up, we were able to access the web-based setup wizard. After completing the few short steps of the wizard, we were able to access the web-based management interface. The only issue we had with the initial deployment of the product was the awkward way that WatchGuard made us license the appliance. We had to go to the vendor website and register for an account, then register the appliance and license keys before we could activate the tool. We would have liked to see a more seamless process.

With that said, we did have an easy time with the rest of the appliance setup and configuration. We found the web-based management console to be easy and intuitive to navigate with a well-organized tab-top layout. One feature we found that really added to the overall ease of use and functionality of the appliance was the DLP Wizard. Rather than having us mess around trying to build data loss policy from scratch, this wizard helped us set policy based on identifiers, such as credit card numbers, identification numbers and medical and financial compliance terms. Further, the dashboard is quite informative with a clean minimal layout that provided an excellent overview of mail and web activity passing through the appliance.

Documentation included a short quick-start guide and a full online manual. The quick-start guide provided a good overview of how to get the appliance up and running with a basic configuration in just a few short steps. The online manual then provided in-depth detail on post-installation tasks, administration and advanced configuration. We found all documentation to provide clear, step-by-step instructions, configuration examples and screen shots.

As part of the purchase price, WatchGuard includes the first year of its 24/7 LiveSecurity Plus support program, which includes phone- and email-based technical aid and product updates. After the first year, customers must purchase additional assistance through an agreement. Customers also get no-cost access to a large support area on the vendor website. This includes a knowledge base, user forum, documentation downloads, customer support portal and many other helpful resources.

We found this product to have a good value for the money. While it may seem pricey at first – with the appliance coming in at just over $17,000 to get started – we found this to be a powerful tool with a lot of features and functionality for the price. This cost also does not include the email encryption module, which must be licensed separately. However, we still found this product to be an excellent value for larger environments that need robust email security and content management functionality.
Emerging products: Online fraud

Whether using your computer to buy products from an e-commerce vendor or to connect with your bank, criminals have a line on your transactions, says Peter Stephenson.

Account takeover, online fraud where there is no physical card, multifactor authentication for consumers, and website fraud analysis and prevention...these all are the meat and potatoes of online fraud management. This means we have a crop of products that fit that description nicely. These all are tools from established companies, so in that regard they are not exactly new emerging. But, there are two important aspects and make them appropriate for our online fraud detection emerging products: first, they are new versions of existing products that have shown significant growth as they have developed and, second, the whole area of online fraud detection is in its infancy, so any solutions to the online fraud challenge is, almost by definition, emerging.

That said, let's begin by taking a look at where these products fit into the fraud management arena. Today's users do several types of things online. They buy things – e-commerce using credit cards, but without, of course, presenting a physical card to the merchant. And, they bank – and by using typical ID/password pairs. In a client-side exploit, sophisticated or not, success depends on being able to harvest credentials. If there are no credentials to harvest, the fraudster is stopped in its tracks. That is one of the solutions to the online fraud problem that we address.

Another area is analytics related to websites. Since the websites are the real targets – remember that old saw about robbing banks because that's where the money is -- being able to catch fraud attempts at the website is a big deal. Add to those two, account takeover protection and risk analysis and you've rounded out this month's offerings. So without further ado, let's get on with it and have a look at our first product.

CA Technologies eComMinder with CA RiskMinder

Here's another situation where a customer is at risk – not only from fraudsters, but from the convenience of online buying. For decades we have preached that security should not get in the way of usability. Died-in-the-wool security pros took the position that one could have security or convenience, but both was out of the question. Of course that's not how it is today, for the most part, but in the world of online business transactions it is a tough tightrope to walk.

CA has this one nailed with its latest eComMinder with RiskMinder. This cloud-based service does nothing but protect the user against the risk of fraud when purchasing with a credit card online. eComMinder with RiskMinder starts out when the user logs into a participating online merchant site with a credit card. The merchant site sends a request for authentication to the card issuer and the card issuer responds to the user. It also responds to the merchant and, for that session, the user no longer needs to worry about fraud. There is a bit of backend communications between the merchant, the card issuer and the directory server, but these things go on in the background. The RiskMinder piece adds the dimension of real-time risk analysis and scoring based on a number of factors. Should the user want to perform high-risk transactions, the CA system can require strong authentication dynamically depending on how the administrator writes the policy. Overall, at a buck per card – substantially less when one starts looking at millions of cards – this is inexpensive fraud insurance.

RSA Silver Tail

Silver Tail is one of those companies that we’ve been watching a long time. They seem to have a pretty good lock on the application of analytics and Big Data analysis to the web. Back in their early days, we marveled at the number of key clicks they claimed to be able to process and analyze. But like the man said, “You ain’t seen nothin’ yet!” When RSA acquired Silver Tail, it was one of those marriages made in digital heaven. RSA has an impressive ecosystem of threat and fraud intelligence.

While RSA traditionally is proactive, Silver Tail has traditionally been reactive. Today, with the resources of RSA, Silver Tail is near real time without losing any of the reactive analytics that have made it such a powerful anti-fraud tool.

Silver Tail does something that really makes it stand apart from the crowd. It differentiates – very accurately – between criminals and legitimate customers by examining such things as velocity (how fast the user moves through a website and how much of the site they access in a short period of time), sequence of pages visited, and the origin of the user. This all is examined in the context of the user, the account, the session and known information about various fraudsters and how various types of frauds are committed.

There are several use cases for the Silver Tail tool, including various forms of account takeover and business logic abuse. But, beyond the deep analytics is the new user interface (UI). One of the hardest things to do in an analytic tool is provide clear visualization. The UI on the new Silver Tail beats anything we’ve ever seen for clarity, organization and comprehensive data display.

CA Technologies eComMinder with CA RiskMinder

| At a Glance | Product: eComMinder with CA RiskMinder | Company: CA Technologies | Price: Starts at $1 per card and decreases with volume |

What we liked: Manages card-not-present (CNP) transactions, Scalability and real-time response all in a single package. Best user interface we’ve seen yet.

RSA Silver Tail

| At a Glance | Product: RSA Silver Tail | Company: RSA, the security division of EMC | Price: Starts at $150,000,000 |

What we liked: Comprehensive protection for websites, Deep behavioral analytics, Scalability and real-time response all in a single package. Best user interface we’ve seen yet.
Trusteer Pinpoint Account Takeover Detection

Account takeover is one of the most prevalent of online crimes. The problem with account takeover is that it is difficult to separate legitimate transactions from fraudulent ones. Success – without a lot of false positives (or false negatives) – depends on a variety of techniques. Trusteer uses all of them.

Pinpoint Account Take Over Detection is part of a suite of Trusteer products that includes malware detection among others. The secret behind the product’s success is a combination of global data sources and its data correlation engine. This engine looks at the device ID, as well as account access, phishing incidents and malware. These are correlated with a global fraudster database and with the events themselves. If an event is out of kilter with the expected correct behavior, Pinpoint looks a bit closer. Tied into the events correlation is the database. This helps tie events to known behaviors, locations, etc., to arrive at a solid identification of a fraud event. Correlating all of the pieces ensures a high level of confidence when blocking a transaction. This is a straightforward product and, for financial institutions of most sizes, it makes a lot of sense to consider. Pricing is reasonable and there are multiple support options available. This is one of those times when technology can step in effectively when policy is difficult to enforce any other way. Enforcing a security policy that protects customers from themselves without impacting customer satisfaction is a great investment.

VASC Data Security MYDIGIPASS.COM

There are lots of ways to secure simple passwords. You could use a password vault on your PC or mobile device that has a master password and stores all of your other passwords in an encrypted container. You could use a service in the cloud that does just about the same thing. All of these have one flaw in common: They are storing a static password. MYDIGIPASS.COM does not store static passwords. Functionally, the user logs into a web app, which in turn queries the MYDIGIPASS.COM server. The server then logs in for the user. But there’s a bit more going on in the background. First, the user has put an app on their mobile device that reads a QR code on the site to which the user wishes to login. There is a first-time authentication ritual and after that the user simply navigates to the target website and clicks on the MYDIGIPASS.COM secure login button. The website redirects the browser to the authorization endpoint and the user then enters the MYDIGIPASS.COM password and authenticator and a one-time password is generated. The website then conducts a backend dialog with MYDIGIPASS.COM and exchanges the one-time authentication for a one-time token, which the website uses to authenticate the user. Users are then enrolled using a self-service model and if a user tries to login without pre-registering at the site, they are redirected to a registration page. The whole system is supported at the website – the bank, online merchant, etc. – and the cost of the service usually is passed on to the consumer. Adding MYDIGIPASS.COM to a website or application is also straightforward. VASC has a complete developer website that uses an API that is easy to assimilate.
When it comes to security, meeting minimum compliance requirements is not enough.

Robust enterprise security requires more than checking compliance boxes, says Diebold CSO Adam Williams.

When it comes to security, meeting the minimum to comply with third-party regulations is not enough. Too often, organizations focus mainly on meeting external compliance requirements – check one off the list and move on to the next. This practice can be dangerous, as it may expose the organization as attention shifts away from non-regulated channels.

Consider how regulatory standards focus on protecting specific data elements. Achieving compliance may offer companies a false sense of security, as part of their environment is heavily fortified, while other network segments and systems may be vulnerable.

Consequently, compliance does not necessarily equate to security. You must establish your own security protocols that go beyond compliance. And you shouldn’t consider your organization to be compliant until it is fully compliant with both external regulations and your internal security policies. Here are a few areas of focus:

Educate your organization. Most compliance programs require some learning initiative. A brochure may be enough to get that coveted compliance checklist. But, in many organizations, employees represent your biggest security risk. You need to turn them into your biggest strength. Help workers understand how their actions can affect your organization’s well-being. Show them how to be security conscious at work and in their everyday lives.

Hold a security awareness conference, and make it fun and engaging. Complement regular training with ongoing communication. Test your network repeatedly. The true test of a security program is what happens when your systems are threatened or compromised. Did your associates enable a breach to occur? Did they notice an anomaly? If so, did they notify your security team? The best way to obtain these answers is through visible security testing followed up by education.

Compliance requirements often dictate annual penetration testing, but once-a-year testing is limiting. Consider what may change in a year: new systems, software patches, employee turnover and more. Increasing testing frequency offers a year-round assessment of security awareness across your enterprise.

Make tests highly covert. For example, send an unannounced phishing email containing a malicious link. If staff members don’t click the link, that’s great. If they notify security, that’s even better. But if some click the link, you have an opportunity to educate employees about security practices.

Monitor threats in real time. To protect data assets, you need to know what’s happening on your network. And you need to know in real time. Compliance directives require a minimum level of monitoring. But organizations that make continuous, real-time monitoring a priority are more likely to detect threats before they proliferate.

Target data classification levels. Compliance requirements commonly protect specific data elements. But that doesn’t mean your policies have to target only individual elements. Instead, your security program can focus on data classification levels, ensuring those individual elements are covered.

Go beyond compliance. Expanding the role of security beyond obtaining compliance checkmarks is critical to securing your enterprise. When doing so, remember that technology is not a cure-all. You need a comprehensive security program that encompasses people, processes and technology – and goes beyond compliance. Only then can you say security is a priority.

Adam Williams is CSO of Diebold, a software, services and electronic security provider.
Download our mobile app

Access IT security on the go! SC Magazine – the trusted source of information for IT security professionals is now at your fingertips.

Get yours now!
http://app.lk/scmagazine