FEATURES:

CSO of the year

The entire organization needs to support security initiatives, says Forrest Smith, CISO, Nissan Americas. P20

The SMB dilemma
Small and midsized businesses are not exempt from cyber attack. P24

Government plays catchup
Security tools and services are available to block leaks of private data, but the government of Canada lags in adoption. PC1
If Muhammad Ali were a Network Security Solution
He’d be ForeScout CounterACT™

Lightning quick. Knock-out punch.

Access and device diversity, dynamic exposures and advanced threats. No problem. Just as Muhammad Ali was a boxing game-changer, ForeScout has changed the game of network security. Leveraging our ControlFabric™ technology, ForeScout delivers the continuous monitoring and mitigation necessary to enable business agility without compromising defenses. Be a game changer.


Knock out threats.
Download at forescout.com/ali_scmedia

ForeScout CounterACT™
If Muhammad Ali were a Network Security Solution
He’d be ForeScout CounterACT™

Lightning quick. Knock-out punch.

Access and device diversity, dynamic exposures and advanced threats. No problem. Just as Muhammad Ali was a boxing game-changer, ForeScout has changed the game of network security. Leveraging our ControlFabric™ technology, ForeScout delivers the continuous monitoring and mitigation necessary to enable business agility without compromising defenses. Be a game changer.


Knock out threats.
Download at forescout.com/ali_scmedia
Online safety for kids of all ages

There is a huge need for people to understand more about cyber threats.”

Target and other retail chains have made headlines recently after becoming victims of cyber attackers. In the aftermath, which saw millions of customers’ sensitive data compromised, these organizations have plenty to address. As part of this process, many often provide year-long free credit monitoring.

To the average Joe and Jane this offer sounds pretty helpful, but while such services can’t hurt, they likely fall short of expectations, too. Credit monitoring, according to experts, only susses out changes on a credit report that could indicate that someone is using personal information to open new accounts in a victim’s name. Since no Social Security numbers were compromised in the Target breach, this service founders.

As well, typically after a year is up, credit monitoring will become useless since an assumption kicks in that the risk to one’s information has passed.

I could say more on this specific topic, but I use it as an example to show that still there is a huge need for all the people who are engaging with technology and, as a result, all its cyber benefits and risks, to understand more about the threats and the many ways they can account for these before and after something goes down. There are a ton of initiatives out there to help on this front, but a couple that have cropped up recently are specifically worth mentioning.

First up is one from Prevendra Consulting and Christopher Burgess, former CISO of Cisco, who co-founded and now heads up the consultancy based in the state of Washington. Senior Online Safety, or SOS (senioronline-safety.com) provides assistance to an often-overlooked portion of our population who actively use the internet and are frequently targeted by online thieves. In addition to a blog that provides advice and tips to readers, SOS also is creating an app to send out daily online safety reminders to subscribers.

The second cool project is the brainchild of Christofer Hoff, a long-time industry expert, and some of his IT security friends who created HackKid (hackid.org), a nonprofit which aims to organize cyber security conferences for kids and their parents. The next HackKid Conference is set for April 19 and 20 in California at the San Jose Tech Museum of Innovation. Touted as “a new kind of conference,” it will focus on providing an interactive, hands-on experience for the entire family, with sessions on everything from staying safe online and cyber bullying to online gaming safety and software manipulation.

These are just some examples of how industry professionals are trying to bolster the knowledge of all of our friends and family members and they’re well worth a look. If you know of other valuable efforts, we at SC Magazine would welcome the opportunity to hear more about them.

Illena Armstrong is VP, editorial, of SC Magazine.

Dell™ SonicWALL™ next-gen firewalls provide a deeper level of network security and application control without affecting performance.

Not all next-generation firewalls are the same. Dell SonicWALL firewall appliances scan every byte of every packet while maintaining high performance and low latency. And, Dell SonicWALL network security provides high-performance SSL decryption and inspection, an intrusion prevention system that features sophisticated anti-evasion technology, context-aware application control and network-based malware protection that leverages the power of the cloud. Now your organization can stay productive while blocking sophisticated new threats.

Go deeper at: sonicwall.com/deep
planning for the rest of the year. We should expect and learn how these developments in the mobile arena and BYO-service, software technologies, and privacy issues abound. And though BYOD has been positive inroads, we examine programs that are showing many organizations still face myriad challenges in deploying just the right security solutions and the proper privacy practices. SAVANTURE

Gerhard Eschelbeck, chief technology officer, and senior vice-president of privacy practice, Oracle

Gene Fredriksen, global information security officer, PSID

Maurice Hampton, director, field operations, Qualys

Paul Kurtz, partner and chief operating officer, Good Harbor Consulting

Kris Lovejoy, general manager, BM Security Services

Tim Mathieu, chief security officer, Apigee

Stephen Northcutt, director, The SANS Institute

Randy Sanovic, owner RMS Consulting; former general director, information security; General Motors

Howard Schmidt, principal, HAK Security

Ariel Silverstone, chief security officer, GHN; former chief information security officer, Expedia

Justin Suomala, chief trust officer, Box; former chief information security officer, Yahoo

Craig Spiezle, executive director and president, Online Trust Alliance; former director, online safety technologies, Microsoft

Hord Tipton, director, (CISO): former chief information officer, U.S. Department of the Interior

Amit Yoran, senior vice-president, RSA, the security division of EMC

* emeritus
Iran top producer of zombie IP addresses

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

ATLANTA – Aleksandr Panin pleaded guilty to conspiracy to commit wire and bank fraud. The Russian man developed and distributed a banking malware called SpyEye that infected more than 1.4 million computers in the U.S. and abroad. Panin sold the malware to at least 150 people at $1,000 to $8,500 a pop.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

AUSTRALIA – A 16-year-old in Victoria discovered a security flaw in the website of Public Transport Victoria that allowed him to obtain a database that includes names, addresses, home and mobile phone numbers, email addresses, dates of birth, senior card ID numbers and extracts of credit card numbers.

DATA BANK

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

HIGH-LEVEL ACTIVITIES

MEDIUM-LEVEL ACTIVITIES

LOW-LEVEL ACTIVITIES

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.

MONTREAL – Telecommunications and media company Bell Canada announced that 22,421 usernames and passwords and five credit card numbers belonging to its small-business customers were posted online. The information was obtained by an attacker who hacked an Ottawa-based third-party supplier’s systems.

TORONTO – About 2,000 members of the Directors Guild of Canada may have had personal information compromised after a hacker accessed a database of plaintext passwords. The website, which stored information on its members, was shut down until the breach was contained.

ENGLAND – An email mistakenly sent to hundreds of Oxford University students contained data on about 50 of the worst-performing pupils at the prestigious school. The information was in an Excel document and included names, grades and degree subjects. The University said the incident is the result of a clerical error.

SOUTH KOREA – A worker at a credit ratings firm was arrested after allegedly copying names, Social Security numbers and credit card details of 20 million South Koreans to a USB stick with the intention of selling the information to phone marketing firms.

ALBERTA – Roughly 620,000 patients of Mediscripts Family Health Care Clinics may have data at risk after a laptop belonging to an IT consultant was stolen. The information on the laptop included names, dates of birth, provincial health card numbers, billing codes, billing amounts and diagnostic codes.
There were 2.3 million cyber attacks in the United States last month.

The Fortinet team is now logging around 1,500 Android samples per day.

There were 2.3 million cyber attacks in the United States last month.

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

663,607,378

(continued from a service provided by DataLossDB.org, hosted by the Open Security Foundation)

Top breaches in January

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neiman Marcus</td>
<td>Neiman Marcus confirmed its</td>
<td>1.1 million</td>
</tr>
<tr>
<td></td>
<td>database was hacked</td>
<td></td>
</tr>
<tr>
<td></td>
<td>around mid-December.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eye Surgery</td>
<td>A human resources employee</td>
<td>4,748</td>
</tr>
<tr>
<td>Education</td>
<td>allegedly downloaded the</td>
<td></td>
</tr>
<tr>
<td>Council</td>
<td>personal information of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>current and former DEW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>employees to a personal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device, according to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authorities.</td>
<td></td>
</tr>
<tr>
<td>South Carolina</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employment and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workforce</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Columbia, S.C.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Source: ICS, www.cybersecurityindex.com

Zombie IP addresses are recorded in Commtouch’s database as having sent spam in the past 24 hours. These are infected computers (zombies) that are unknowingly sending spam. Based on the IP address, the company can determine the country of the spam-zombie and then sums up the spam-zombies per country.

Source: CYREN (formerly Commtouch Software Online Labs)

Top 5 attacks used by foreign hackers

1. Zero Access trojan
2. Rerdom trojan
3. Cutwail trojan
4. Gamarue trojan
5. Redym trojan

Top 5 attacks used by U.S. hackers

1. Cutwail trojan
2. Rerdom trojan
3. Redym trojan
4. TDSS Downloader trojan
5. Gamarue trojan

Source: Dell SonicWALL

SC • March 2014 • www.scmagazine.com

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

Source: ICS, www.cybersecurityindex.com

DataBank

ThreatStats

There were 2.3 million cyber attacks in the United States last month.

Monthly evolution of mobile malware

Number of Android samples

- 2,000,000
- 1,500,000
- 1,000,000
- 500,000
- 300

Android samples per day

- 1,500
- 1,200
- 900
- 600
- 300

The Fortinet team is now logging around 1,500 Android samples per day.

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

Source: ICS, www.cybersecurityindex.com

Internet dangers

Top 10 threats

1. Zbot
   Movement: ▲
   Date first observed: 09/22/10
   Type: PasswordStealer
   Last month: 6
   Weeks on list: 1

2. Zbot/jen/AT
   Movement: ▲
   Date first observed: 07/20/13
   Type: PasswordStealer
   Last month: 3
   Weeks on list: 2

3. Lameche/B
   Movement: ▼
   Date first observed: 01/10/12
   Type: Downloader
   Last month: 1
   Weeks on list: 1

4. Expire/engF
   Movement: ▲
   Date first observed: 03/10/13
   Type: Virus
   Last month: 0
   Weeks on list: 0

5. Almanahe/B
   Movement: ▲
   Date first observed: 12/08/10/
   Type: Virus
   Last month: 0
   Weeks on list: 0

6. Benjamin
   Movement: ▲
   Date first observed: 03/10/11
   Type: Worm
   Last month: 0
   Weeks on list: 0

7. Virut/K
   Movement: ▲
   Date first observed: 12/11/10
   Type: Virus
   Last month: 0
   Weeks on list: 0

8. Zbot/A/JB
   Movement: ▲
   Date first observed: 08/01/13
   Type: PasswordStealer
   Last month: 0
   Weeks on list: 0

9. Expire/CA
   Movement: ▲
   Date first observed: 01/07/14
   Type: Virus
   Last month: 0
   Weeks on list: 0

10. Picosy/C
    Movement: ▲
    Date first observed: 01/08/11
    Type: Worm
    Last month: 0
    Weeks on list: 0

Source: Alcatel-Lucent Kindsight Security Labs

Top 5 attacks used by foreign hackers

1. Cutwail trojan
2. Rerdom trojan
3. Zero Access trojan
4. TDSS Downloader trojan
5. Gamarue trojan

Source: Dell SonicWALL

SMS spam

Volume by month for each region

Top 5 attacks used by U.S. hackers

1. Cutwail trojan
2. Rerdom trojan
3. Redym trojan
4. TDSS Downloader trojan
5. Gamarue trojan

Source: Dell SonicWALL

Top 5 attacks used by foreign hackers

1. Zero Access trojan
2. Rerdom trojan
3. Cutwail trojan
4. Gamarue trojan
5. Redym trojan

Source: Dell SonicWALL

Received spam

Top five regions

Source: Cloudmark

Internet dangers

Top 10 threats

1. Zbot
   Movement: ▲
   Date first observed: 09/22/10
   Type: PasswordStealer
   Last month: 6
   Weeks on list: 1

2. Zbot/jen/AT
   Movement: ▲
   Date first observed: 07/20/13
   Type: PasswordStealer
   Last month: 3
   Weeks on list: 2

3. Lameche/B
   Movement: ▼
   Date first observed: 01/10/12
   Type: Downloader
   Last month: 1
   Weeks on list: 1

4. Expire/engF
   Movement: ▲
   Date first observed: 03/10/13
   Type: Virus
   Last month: 0
   Weeks on list: 0

5. Almanahe/B
   Movement: ▲
   Date first observed: 12/08/10/
   Type: Virus
   Last month: 0
   Weeks on list: 0

6. Benjamin
   Movement: ▲
   Date first observed: 03/10/11
   Type: Worm
   Last month: 0
   Weeks on list: 0

7. Virut/K
   Movement: ▲
   Date first observed: 12/11/10
   Type: Virus
   Last month: 0
   Weeks on list: 0

8. Zbot/A/JB
   Movement: ▲
   Date first observed: 08/01/13
   Type: PasswordStealer
   Last month: 0
   Weeks on list: 0

9. Expire/CA
   Movement: ▲
   Date first observed: 01/07/14
   Type: Virus
   Last month: 0
   Weeks on list: 0

10. Picosy/C
    Movement: ▲
    Date first observed: 01/08/11
    Type: Worm
    Last month: 0
    Weeks on list: 0

Source: Alcatel-Lucent Kindsight Security Labs
Update

NEWS BRIEFS

The Canadian government has hired Wedge Networks, a provider of cloud-based security services, to secure its computing infrastructure. The services will be applied within data centers at Shared Services Canada, the government’s IT service.

Wedge Networks uses network virtualization, in which key network functions are carried out in software. This helps to provide security functions including traffic inspection, anti-malware and anti-spam services.

Shared Services Canada, announced in 2011, is the Canadian government’s attempt to consolidate its IT into a central department, reducing duplication and making its completing infrastructure more efficient. WedgeOS will protect information department, reducing duplica-

dian government’s attempt to

spam services.

security functions including traffic

work functions are carried out in

virtualization, in which key net-

government’s IT service.

provider of cloud-based security

Wedge Networks

,...

Arts and crafts retailer Michaels Stores may also have been hit by a breach.

Retail redux

After news broke that Target was hit by a major breach, a number of other retailers began alerting customers about poten-
tial data compromises. In late January, e.g., upscale retailer Neiman Marcus revealed that malware on its payment systems may have compromised 1.1 million customer card accounts and that around 2,400 payment cards had already been used fraudulently as a result of the incident.

Only first-time customers who made a purchase during this time window were affected, indicating that the attacker used a vulner-

Only first-time customers who made a purchase during this time window were affected, indicating that the attacker used a vulner-

Retail redux

After news broke that Target was hit by a major breach, a number of other retailers began alerting customers about poten-
tial data compromises. In late January, e.g., upscale retailer Neiman Marcus revealed that malware on its payment systems may have compromised 1.1 million customer card accounts and that around 2,400 payment cards had already been used fraudulently as a result of the incident.

Only first-time customers who made a purchase during this time window were affected, indicating that the attacker used a vulner-
abily to record information as it was entered.

The Albertan Information and Privacy Commissioner has formally asked the government to amend the province’s Health Information Act with mandatory breach reporting and notification measures.

The letter, from Commissioner Jill Clayton, came just a month after she launched an investiga-
tion into a privacy breach at the province’s Medicentre, in which a laptop containing the health information of 620,000 Canadians was stolen.

Nine jurisdictions in Canada have introduced health privacy legislation, six of which include

mandated breach reporting, she said. Currently, only Alberta’s Personal Information Protection Act requires an organization to report a privacy breach.

including privacy breach notifi-
cation and reporting requirements in all three of Alberta’s access and privacy laws is an important com-
ponent of protecting a person’s privacy rights and will help to put Alberta at the forefront of privacy protection,” she said.

Documents obtained by Canada’s CBC News via an access to information request last month also showed that Alberta Health Services workers were systematically sending faxes containing client health information to the wrong people. At one point, a custom homebuilder was receiving faxes intended for a home care fac-

The world is becoming hyper-

connected. We have already ac-
dmitted the fact that everything happens online. In the past
decade we moved from going to our bank branches to cashing in our check, to scanning it with our smartphones on the go.

We’re gone from reunion meet-
ings to Facebook walls, and from mall culture to online shopping. We have accepted the advancements that allow us to per-
form tasks easier from the comfort of our homes.

All of the services mentioned above are enter-
prises. They are the ones that provide platforms for our online activity, they are the ones that trade information and, unfortunately, they are the targets for data breaches that – in the end –

effect individuals.

Hackers don’t go for individuals, period.

It makes no financial sense. Hackers go for data holders, such as online stores that hold credit card information, etc., because the goal is capital gain. It is for that reason that regulation enforces the need to secure and audit data stored and transacted to keep individuals safe.

THE QUOTE

Simple is better than complex, and sooner is better than later…”

– Mark Schreiber, partner at Edwards Wildman Palmer and chair for the World Law Group, commenting on the need for a federal breach notification debate.

The Internet of Things is an enterprise problem.

The world is becoming hyper-connected. We have already accepted the fact that everything happens online. In the past decade we moved from going to our bank branches to cashing in our check, to scanning it with our smartphones on the go. We’re gone from reunion meetings to Facebook walls, and from mall culture to online shopping. We have accepted the advancements that allow us to perform tasks easier from the comfort of our homes.

All of the services mentioned above are enterprises. They are the ones that provide platforms for our online activity, they are the ones that trade information and, unfortunately, they are the targets for data breaches that – in the end – effect individuals.

Hackers don’t go for individuals, period. It makes no financial sense. Hackers go for data holders, such as online stores that hold credit card information, etc., because the goal is capital gain. It is for that reason that regulation enforces the need to secure and audit data stored and transacted to keep individuals safe.

Debate

The Internet of Things is not by itself a problem for enterprises (or at least, not a new one). While the Internet of Things will force massive changes in the way businesses interact with their customers, employees and products, it should be clear by now that change has become a constant for security practitioners. In fact, many trends that were first viewed by security executives as “problems” are now viewed as business opportunities. Every change forces enterprises to adapt, whether it be today’s explosion of mobile devices and cloud services or tomorrow’s Internet of Things.

So the question is then whether each enterprise is ready to deal with the data, security and identity management challenges that the Internet of Things will demand. Failure to be able to understand the relationships between people, products and data will leave business-essentially blind — and therefore not only highly vulnerable, but also unable to compete and thrive in a new, always-on economy.

THE MAGAZINE POLL

The Internet of Things is an enterprise problem.

The world is becoming hyper-connected. We have already accepted the fact that everything happens online. In the past decade we moved from going to our bank branches to cashing in our check, to scanning it with our smartphones on the go. We’re gone from reunion meetings to Facebook walls, and from mall culture to online shopping. We have accepted the advancements that allow us to perform tasks easier from the comfort of our homes.

All of the services mentioned above are enterprises. They are the ones that provide platforms for our online activity, they are the ones that trade information and, unfortunately, they are the targets for data breaches that – in the end – effect individuals.

Hackers don’t go for individuals, period. It makes no financial sense. Hackers go for data holders, such as online stores that hold credit card information, etc., because the goal is capital gain. It is for that reason that regulation enforces the need to secure and audit data stored and transacted to keep individuals safe.

THE MAGAZINE POLL

The Internet of Things is an enterprise problem.

The world is becoming hyper-connected. We have already accepted the fact that everything happens online. In the past decade we moved from going to our bank branches to cashing in our check, to scanning it with our smartphones on the go. We’re gone from reunion meetings to Facebook walls, and from mall culture to online shopping. We have accepted the advancements that allow us to perform tasks easier from the comfort of our homes.

All of the services mentioned above are enterprises. They are the ones that provide platforms for our online activity, they are the ones that trade information and, unfortunately, they are the targets for data breaches that – in the end – effect individuals.

Hackers don’t go for individuals, period. It makes no financial sense. Hackers go for data holders, such as online stores that hold credit card information, etc., because the goal is capital gain. It is for that reason that regulation enforces the need to secure and audit data stored and transacted to keep individuals safe.

THE MAGAZINE POLL

The Internet of Things is an enterprise problem.

The world is becoming hyper-connected. We have already accepted the fact that everything happens online. In the past decade we moved from going to our bank branches to cashing in our check, to scanning it with our smartphones on the go. We’re gone from reunion meetings to Facebook walls, and from mall culture to online shopping. We have accepted the advancements that allow us to perform tasks easier from the comfort of our homes.

All of the services mentioned above are enterprises. They are the ones that provide platforms for our online activity, they are the ones that trade information and, unfortunately, they are the targets for data breaches that – in the end – effect individuals.

Hackers don’t go for individuals, period. It makes no financial sense. Hackers go for data holders, such as online stores that hold credit card information, etc., because the goal is capital gain. It is for that reason that regulation enforces the need to secure and audit data stored and transacted to keep individuals safe.
The breach notification debate

The new year continued where it left off in 2013 – with a massive retailer breach. The Target, Neiman Marcus and Michaels incidents made headlines around the world. However, there was one positive outcome from these events – the discussion regarding a potential federal breach notification law was brought back to the forefront among government leaders.

It’s no secret that electronic personal information is a hot commodity for cyber criminals. While mega-retailers like the aforementioned have budgets to implement state-of-the-art security bells and whistles, miscreants always find a way in, circumventing controls and silently siphoning sensitive financial data. Although that may be inevitable, the quicker individuals are notified of a breach, the better chance they have to take proper measures and protect their assets.

Outside of specific industries, breach notification laws are enforced at the state level, with 46 states having notification requirements in place, according to the “Global Guide to Data Breach Notification, 2013,” a study by the World Law Group (WLG), a network of 53 independent law firms.

The current patchwork of requirements gives a lot of different committees “skin the game,” says Doug John- son, VP of risk management policy at the American Bankers Association. He believes these jurisdictional issues are big hurdles that have impeded the development of a federal standard.

“What you have is the individual states having the latitude to do their own thing,” Johnson says. “[This] makes it really difficult and makes for a cry for an adoption of a national standard.”

While politicians have taken a crack at drafting overarching legislation, such as the Personal Data Privacy and Security Act of 2014, the Data Security and Breach Notification Act of 2014, and Data Security Act of 2014, as of press time, all have stalled in committee.

Just like the requirements at the state level, the proposed federal drafts differ in defining a breach. Mark Schreiber, chair of the privacy and data protection group at law firm Edwards Wildman Palmer, and chair for the WLG, believes that while this is a part of the problem, it is easily resolved.

“Whatever definition [is] used, it would be better than the current polyglot of numerous state definitions, many of which don’t square up with each other,” he says. “There’s got to be a better solution than what we’ve got now.”

– Marcus Colón

40M payment card numbers and PII of 70 million customers were impacted in the recent Target breach.

How would you describe your job to average people?

John Gibson

My job is to assist customers with evaluating the levels of security risk in their environment and propose or implement mitigation and management solutions/controls.

Why did you get into IT?

Joshua Goldfarb

One, because it affords me the opportunity to understand the challenges affecting businesses in this extremely dynamic industry. The second, it is one of the more challenging disciplines in IT. The landscape changes at a rapid rate and as a result it provides the perfect combination of endorphins and adrenaline, whether good or bad. I’ve never had a dull day since I’ve been in IT security.

What was one of your biggest challenges?

Palo Alto Networks, a
Santa Clara, Calif.-based network security provider, has acquired Morta Security, a security firm in Silicon Valley. With the purchase, Morta migrates its team of experts on national infrastructure protection to Palo Alto. In addition, Palo Alto expects the acquisition to enhance its Wildfire offering for threat detection and prevention.

CipherCloud, a San Jose, Calif.-based cloud security firm, has acquired CloudUpNet- so that scanning and tagging capabilities for various classes of data, depending on privacy requirements, are available to customers. Through the acquisition, CipherCloud aims to offer a more holistic platform for securing cloud data.

Damballa, an Atlanta-based firm that provides advanced threat protection services, has added two security executives to its management team. David Earhart joins the company as senior vice president of worldwide field operations, and Julie Pres- iss comes on board as vice presi- dent of marketing. Earhart was previously senior vice president for CA Technologies’ security and field operations, while Presco formerly worked as head of mar- keting for Dell SecureWorks.

Skills in demand

Recent breaches have high- lighted the need for talented technologists with the ability to assess vulnerabilities long before they are under attack.

What it takes

Hands-on experience with reverse engineering, packet level programming and knowledge of digital forensics. Expertise in identifying vulner- abilities and understanding what it takes to “break” a system is critical. The ability to approach a system creatively and solve complex problems, paired with stellar documentation and communication skills.

Compensation

Junior level roles start around $90K, with senior levels often earning $130K to $150K – sometimes higher.

Source: Domini Clark, principal, executive and technical recruitment, Blackmere

Follow us on Facebook and Twitter

John Gibson

senior IT security officer, Thack Ltd.

How would you describe your job to average people?

My job is to assist customers with evaluating the levels of security risk in their environment and propose or implement mitigation and management solutions/controls.

Why did you get into IT?

Joshua Goldfarb

My job is to assist customers with evaluating the levels of security risk in their environment and propose or implement mitigation and management solutions/controls.

Why did you get into IT?

Joshua Goldfarb

firm BakerHostetler

a partner in the firm’s antitrust and trade regulation practice and as a national co-leader of its privacy and data protection team. Har- bour previously worked at multi- national law firm Norton Rose Fulbright, and also served nearly seven years as Federal Trade Commissioner. At BakerHostetler, she joins the firm’s Washington D.C. and New York offices.

Joshua Goldfarb has joined nPulse Technologies, a Charlotteville, Va.-based packet capture and Big Data analytics provider, as CISO. In the role, Gold- farb will help enhance security offerings for the company’s public and private sector customers. He formerly served as the chief of analysis for the United States Computer Emergency Readiness Team (US-CERT).

Ken Kuenne has joined Vaultive, a New York-based provider of cloud data encryption solutions, as senior director of channels. In the role, Kuenne will lead the company’s channel strategy by facilitating adoption of cloud-based services jointly with key partners.

Pamela Jonas Harbour has joined Cleveland based law firm BakerHostetler as a partner in the firm’s antitrust and trade regulation practice and as a national co-leader of its privacy and data protection team. Harbour previously worked at multi-national law firm Norton Rose Fulbright, and also served nearly seven years as Federal Trade Commissioner. At BakerHostetler, she joins the firm’s Washington D.C. and New York offices.

Joshua Goldfarb has joined nPulse Technologies, a Charlotteville, Va.-based packet capture and Big Data analytics provider, as CISO. In the role, Goldfarb will help enhance security offerings for the company’s public and private sector customers. He formerly served as the chief of analysis for the United States Computer Emergency Readiness Team (US-CERT).

Ken Kuenne has joined Vaultive, a New York-based provider of cloud data encryption solutions, as senior director of channels. In the role, Kuenne will lead the company’s channel strategy by facilitating adoption of cloud-based services jointly with key partners.

Pamela Jonas Harbour, partner, BakerHostetler

David Earhart, VP of worldwide field operations, Damballa

works, a privately held provider of SaaS application security. With the deal, CipherCloud expects to expand its CipherCloud platform to businesses in Jamaica.

Follow us on Facebook and Twitter
Driving the mission forward

Roland Cloutier
CSO, ADP

Focus is often not easily attainable in our profession. The needs of the organizations we protect are complex and the response required due to the criticality of the services we provide tends to put our multi-faceted operations in a state of flux. Add on increases in the threat environment, technology shifts and an explosion in size of threat surfaces, and your full-time job becomes chief prioritization officer.

There are many things we can do to drive our missions forward while we manage the process of our business protection evolution. The key to success is forward momentum. Any act that drives change, large or small, will help, starting with these three complicity fighting tactics.

Create controls assurance – Create a process to measure the suitability of your controls. Our programs are based on tried-and-true rules to security. Review the control, decide if it works as intended and make proactive decisions on whether to keep, remove and redistribute the operating cost to higher priority or change it.

Create urgency – Creating urgency is often mixed with the connotation of “selling security through fear.” These ideas could not be further apart. Urgency means that you’ve educated someone to facts that in turn drive action. Have a vendor do a proof-of-concept with a new technology that provides insight into a specific gap in your security program. Lead a fact-gathering business analysis using graphical data flows, application access and data sprawl with your business customer to provide them with a visualization of the impact to their business. Finally, spend time with your team taking them through the downstream residual impact of the operations you provide and instill a sense of mission urgency.

Being a good security practitioner means being a good business partner. The actions above demonstrate leadership, financial accountability, resource management and relationship management. But most importantly, they deliver actionable changes that increase the efficacy of our programs and get our business that much further up the maturity curve of protection.

Create momentum – Create momentum through action itself. To achieve this, create a list focusing on reducing risk and closing gaps in your environment. Site-specific issues, how they impact the business, how a change would reduce the risk and offer solutions. Next, create a critical asset protection program and put it to use to protect the crown jewels. Include steps to document assets, test, remediate and monitor using your existing resources when possible.

Headlines that push spurious information – like, “600 percent growth in mobile malware” – are not useful. The stories often do not provide sufficient context in order for readers to understand the true threat. People reading these headlines understandably might feel fear and doubt about their mobile devices.

To what does “600 percent growth” refer? Unfortunately, we are still living in a time that measures malware growth by the number of unique signatures. Modern malware is typically polymorphic in nature.

In other words, it is advantageous for the attacker to make each infection digitally unique. Desktop anti-virus companies have mostly divorced themselves from this measurement of unique signatures because of its loss of meaning. Tech journalism has kept it in their vocabulary for mobile devices because it helps them write sensational headlines.

It’s more useful to measure the rate of change of malware capabilities. Has mobile malware changed through time as dramatically as the headlines might imply?

Android suffers from SMS malware, which sends fraudulent text messages to premium numbers. SMS redirection malware steals one-time passcodes for banking fraud. These are examples of regionally focused malware that exploit Android’s app access to SMS and the platform’s option to sideload apps outside of Google Play. Before Android 4.3, the ability for a user to lock down app access to pictures, contacts and other shared objects has meant that malware has targeted those things too.

Apple’s iOS platform has had very few malware examples outside of those created by researchers like Charlie Miller, ultimately for benign purposes.

In comparison, one could write about the variations of desktop-top malware and fill pages with relevant content. The architecture of mobile operating systems is different than desktop. Knowing this should help mobile device users continue to use them – and without the feeling of dread that headlines imply.

30 seconds on...

➢ Avoid the void
One risky area where today’s security professional can often get slowed down is distinguishing the must-have projects and technologies from the need-to-do, Cloutier says.

➢ Overcome obstacles
Red tape, business cases, creating awareness and gaining support for new technologies can feel like the wheels of progress are pushing our programs backward rather than forward.

➢ On your toes
Although new threats, business needs and shrinking budgets can delay our initiatives, we must never confuse program process slowdowns with self-induced complacency.

Executives are the driving force behind cloud adoption...

Mobile: Behind the headlines

Trends: Beyond the hype

Coming into 2014, cloud computing, BYOx (bring your own device and other personal computing gadgets), and security awareness are predicted to be hot trends for IT security. To understand which trends are being validated versus those that might be a lot of hot air, we asked some of our most senior members for their perspectives.

To start, there was consensus that cloud computing is becoming a reality that will need to be addressed by every security department. Executives are the driving force behind cloud adoption – most likely due to proclaimed economic benefits. However, CISOs caution that the security implications of cloud computing are serious and will remain.

Surprisingly, with all the industry hype surrounding BYOx, Wisegate members agreed it’s not developed as expected. Realities of full adoption, such as support costs, compliance risks and usage reimbursement, can actually raise the total cost of ownership at a time when the TCO for company-owned PCs is dropping.

Another hype trend is security awareness, which many IT leaders believe may be unwarrented. Most agree that getting employees to pay attention to what they are doing and how it affects the security of their organization is still a challenge. Yet some believe the challenge is a worthy one.

Other Wisegate members agreed that often the best solutions to problems – hype or not – come from contering with other expert CISOs. “Often senior technology leaders struggle to get straight answers about IT,” said David Sherry, CISO at Brown University. “We need to connect to peers, who are the best source of pragmatic information on what works, what doesn’t, and key lessons learned.”

No matter what the viewpoints are on the hype versus reality, all security practitioners agree we will face significant challenges managing the growing complexity of IT security in the days ahead.
The fallacy of targeted attacks

It’s time to admit that the bad guys can always make a first move, says Damballa’s Manos Antonakakis.

O

ver the last few months, I’ve had the opportunity to visit, meet and hold extensive discussions with a variety of people across the security landscape. In the process, I’ve realized there is a great level of misconception around the detection or even prevention of targeted attacks and advanced threats.

First of all, prevention is simply not possible. If that problem were solvable, academia and industry would have solved it many years ago, and other types of threat detection companies simply wouldn’t exist. The attacker has the first move, thus the infection vector is bounded by the attacker’s skill sets. Now, let’s try to demystify the problems of detecting advanced and targeted threats and discuss to what extent we can rely on sandboxing-based technologies to solve the problems for our organizations.

By definition, an advanced threat will try to evade the most basic traditional defenses. In Computer Security 101, you learn that when you want to understand what malicious software does, you run it in a sandbox. The second thing you learn is that dynamic analysis of any code is not only doable, it is scaleable and it does not scale. It is undecidable due to some very fundamental computer science problems. Without delving too deep, it suffices to state that even when you have the malware, you cannot automatically tell what it is capable of doing. Thus, using sandboxing for the detection potential C&C communication is at best unreliable.

On the other hand, sandboxing does not scale for many reasons, including: You do not always have access to the binary (due to encryption, packers etc.); you do not a priori know the length of time you must execute the malware. Thus, if the malware sleeps, there’s nothing you can do; the malware authors have developed sophisticated techniques that detect sandboxing environment based on their network and system properties. But this is enough on advanced and sophisticated threats. Sandbox-based detection fails – we know that objectively and a priori. Now, let’s examine the targeted threats. Let’s try to get into the shoes of an attacker. It is quite reasonable to assume that the adversary will spend a significant amount of time crafting the attack vector. It is also quite reasonable to also assume that the adversary will not just push the targeted attack vector out in plain text, so sandboxing companies could trivially grab it.

The simplest way to achieve this is to sacrifice commodity RAT-like malware before the actual targeted malware drops. From the adversary’s standpoint, if you drop the first stage RAT-like malware and run in a sandbox, why would you proceed to use it to deploy your targeted threat? We really have to assume that the adversary is at least that smart, otherwise we are not chasing targeted malware, but rather novice attackers that create malware on their free time based on “open sourced” malware kits.

Realistically, can sandbox-based detection technologies help us defend against advanced malware or targeted threats? Yes, even after the malware as a “detection” trigger, is a battle that we will never win and we will always be behind the threat.

By definition, sandbox-based analysis tools are available to any adversary planning an attack (since they are commercial products, and available to the class of adversary planning an APT-class assault). Simple malware may be caught by sandboxies, they’re no doubt useful. But in the case of APT, the malware authors test their attacks before releasing them. Thus, it becomes tremendously difficult to detect, classify, and attribute APT threats via sandbox-based methods.

Manos Antonakakis is chief scientist at Damballa.

Got something to say?

From the online mailbag

In response to a January news item: Critical infrastruct-

cyber bill gets go-ahead from Homeland Security committee:

This legislation and related measures will best serve to provide intelligence agencies with additional fodder for an already bulging surveillance data warehouse, with little or no effect on the stated issue or worse, resulting in a spate of unintended consequences. Which issue would be better served by a well thought-out, well-executed combination of well-understood security measures, air gaps and private [non-internet connected] networks.

Joe Cocchini

In response to a January Opinion, Why wasn’t health-care.gov security properly tested?, by Michelle Drolet, founder. Towerwall:

In second paragraph: “David Kennedy, chief executive of Trusteedc, told CNBC that, ‘It’s really hard to go back and fix the security around it because security wasn’t built into it.’ I’m afraid the project failed before it got started then.

That’s unbelievable that in current times this could happen.

David Barnes

It’s what happens when you award contracts to the lowest bidder, weathertop

No doubt the purpose is for Google to gather even more data to support all of their data driven activities. Any benefits or detriments to users are purely incidental and, as they tell the EU, unin-

nential. And the NSA will like this, too.

Dawkinsfan2

In response to a December news story, Crooks steal money from ATMs using USB drives, experts weigh in:

Perhaps this indicates a need for better physical security. Presumably the ATMs in question have physical security to prevent the crooks from easily taking out the cash through a hole. Design of the physical security should recognize that access to the computer that controls the cash is most of the way to compromising the cash itself. This isn’t just an XP issue.

Bill Hartman

If ATMs have to run Windows, they should be prime candi-

dates for running Windows XP Embedded, which is intended for dedicated ship installations.

Slava Gomzin, Bitcoin Group that said that “Over the last 12 months, tokeniza-

tion users had 50 percent fewer security-related incidents than tokenization non-users.” The name of the study, released a few months ago, is “Tokenization Gets Traction.”

Ulf Mattsson, CTO, Protegrity

The intelligence community has gotten lazy and complacent, figuring that machines can do all their work. They can just sit back, relax, and let the super-computers start tickling off photos of terrorists and criminals instead. We won’t even get into the whole treating the symptoms instead of the disease argument, which a long-term solution to extremism is going to require.

The opinions expressed in these letters are not necessarily those of SC Magazine.

Letters

18 SC • March 2014 • www.scmagazine.com

www.scmagazine.com • March 2014 • SC 19
For many professionals in this space it can make or break a security strategy’s overall efficacy. As a result, some CSOs are becoming just as practiced at promoting their security initiatives as they are at actually implementing and managing them.

SC Magazine’s 2014 CSO of the Year, Forrest Smith, who is the senior manager of information security and CISO for Nissan Americas, says that establishing and diligently following through on an “internal marketing plan” helps “to build consensus across the organization” and reveals just how IT security works to facilitate wider business aims.

“If you expect everyone to support security initiatives, everyone from the top down needs to know what the security initiatives are and how to support the security team in meeting those objectives,” he explains.

To Lee Eaves, who works for Smith as manager for information security at Nissan, this way of thinking has contributed greatly to how company executives and workers alike view IT security.

“I’ve seen a significant evolution of Nissan’s security program over the past three years,” he says. “Forrest generated a strategic vision and added thought leadership to information security and its associated programs. Under his direction, Nissan created a business-centric, global information security incident response plan, digital forensic team, threat intelligence team, improved the use of information security tools and improved communications with business sponsors and executives.”

In addition to improving the company’s threat intelligence levels, Smith – who previously worked for IBM as a consultant, middleware architect and team lead – also developed the idea of “threat hunting,” he says. This allows his staff “to apply behavioral analytics to network and computing systems to identify anomalies.” And, although his team of full-time and contract employees continue to use traditional systems, such as intrusion detection, AV and others, they layer on top of these the “threat hunting” practice in an attempt to catch more “sophisticated, targeted attacks,” he explains.

Another big change in the past year occurred with the IT security organization moving out of the information systems department into corporate services. Among other things in the works, this move expanded IT security’s scope to include the management of engineering and manufacturing. “We are no longer solely the information systems security group, but instead we focus on threats across the organizations and across different types of devices,” says Smith.

The change also is aiding in the alignment of IT security and physical security, adds Brian Delauter, Smith’s boss, and the director of the corporate services division, which includes shipping and receiving, corporate vehicles, global aviation, facilities management, real estate and physical security divisions.

As well, it makes IT security much more autonomous, allowing for Smith and his crew to “shine the light on issues that don’t always make it up to leadership,” adds Delauter. “The net goal is to strengthen IT security for the enterprise. It’s always about the company. We’re going to be better tomorrow than we are today.”

Smith is critical to this process because he brings a “tremendous amount of knowledge and a pragmatic approach,” Delauter says, adding that Smith’s solid risk management approach to security helps the company’s executive leaders and business units prioritize corporate goals, marrying security goals to them, so that all the players are moving in the right direction.

Continuing to partner business with
security likely will result in IT security eventually standing on its own, with Smith reporting to the highest levels of the company—a goal of Delauter’s. As such, he definitely sees Smith moving into a position that is in line with his own level now.

“Forest” is very well regarded at the organization and we want to help him grow,” he says. “If we don’t, someone else will.”

Both Delauter and Eaves agree that Smith is more than deserving of SC Magazine’s CSO of the Year Award given these and other steps he’s taken to advance information security for Nissan.

“In the next 12 to 18 months, I think we’re going to see the growth of information security outside of the IT function,” says Eaves. “Forest has been able to communicate and demonstrate the strategic value of information security within our organization. As a result, he’s driving the sure of information security in all aspects of our business. Forest’s most valuable trait is the strategic vision and thought leadership that he brings to the security organization. Because we have a solid strategy, we are very visible and integrated into the different business units within Nissan.”

SC Magazine gained some insight directly from Smith, querying him about his concerns when it comes to safeguarding Nissan’s most critical assets, and more.

SC: What have been your major achievements in the last year?
FS: We expanded our team, focused on ensuring we have broad expertise. We focused less on finding the perfect security person and instead on finding experienced individuals who have valuable soft skills, and then we trained them. We’ve found this approach provides a more comprehensive and cohesive team. This also helped improve our communication within the company as these individuals were highly capable of communicating complex technical issues to our business units.

SC: What were the major challenges?
FS: I think the major challenge is the need to constantly review your priorities and evaluate whether certain tasks are really adding value. Due to the dynamically changing threat landscape, we constantly re-evaluate and prioritize the way we do things to be most effective.

At Nissan, we are frugal, yet successful, because we focus on security initiatives and activities that provide the greatest probability of reducing significant risks. I think there’s a general philosophy that to build a good security team, you must invest significantly in tools and people. While this is partially true, I also find that we don’t effectively use the tools we already have or could use them in a different way to become more effective at detecting or preventing threats. One of our biggest challenges is achieving maximum value from security investments and being innovative in how we use the tools we already have.

SC: Who in your organization helped with these achievements?
FS: We have support from all levels of management and the entire Nissan organization. We have a culture set by our CEO that every employee is responsible for protecting Nissan’s information assets. As such, the entire organization helps the information security team be successful.

SC: Do more companies care about security when dealing with vendors?
FS: I think companies and consumers care more about security and privacy now than they did several years ago. I suspect that soon consumers will heavily factor a company’s ability to secure private information before they purchase the purchase decision. I suspect this is going to propel information security into being an integral part of a company’s sales and marketing strategy.

SC: How would you describe today’s security threat landscape?
FS: I’ve seen a dramatic shift and increase in cyber crime, intellectual property theft and I am starting to see more “disruptive behavior” again. More importantly, these things are occurring across more types of devices.

There is a continuous lag in security technology’s ability to secure the changes that can stay ahead of the evolving threat landscape. In my opinion, the most promising technologies are those that use whitelists and focus on behavioral anomalies.

SC: What is your biggest gripe with the way security is done these days?
FS: I see an over-reliance by companies on outsourcing of critical security functions. I believe a key factor in deterring business-targeted threats is an intimate knowledge of your IT environment, which an outsourcer just doesn’t have. There is a place for outsourcing within the security organization, but a successful security organization must balance when to use and not use an outsourcing strategy.

SC: What are the threats you and others in your position must address this year?
FS: We need to find ways to enable and secure bring your-own-device (BYOD) and “moving to the cloud.” Evaluations of technology are not avoidable and we should embrace them. But, there are enormous complexities in securing both these areas, not to mention the legal considerations. We are going back to the drawing board to come up with innovative ways to make BYOD and cloud data initiatives more secure.

SC: What security technologies should companies have in place?
FS: The technology must have log collection/event correlation tools and application whitelisting. Log collection and event correlation tools allow the organization to dissect and analyze anomalous behaviors. Nearly every breach report discusses the lack of logging monitoring as a significant contributing factor. Application whitelisting prevents a very high percentage of malware and other unauthorized programs from running on workstations and servers.

SC: What about policies and programs?
FS: End-user information security education is the most overlooked program in security. Effective security education, beyond the mandatory annual training, makes a significant difference in reducing risk and can be done at minimal cost.

SC: What’s your best advice when it comes to building a security program?
FS: First, educate executive management until you gain their support. Second, a highly-skilled team is critical in meeting security objectives – be careful to choose quality over quantity.

Finally, investments should be prioritized based on risk. Generally, speaking, the security functions struggle with prioritizing investments and being agile enough to change them when the threat landscape changes.

SC: Is there an ideal hierarchical structure when it comes to ensuring IT security is being addressed adequately?
FS: Earlier this year, Nissan changed the reporting structure and my organization was moved outside of IS into corporate services.

I believe the ideal hierarchical structure to ensure IT security is addressed adequately is for the security organization to report to the CEO as opposed to the CIO. This is important because the role of the CIO has expanded over the years, and the information systems organization differ from those of the security organization. With many companies considering cyber security a high risk, the separation of duties between information security and information systems will become important to auditors and shareholders.

SC: How do you make sure leaders understand compliance requirements so you get the required support?
FS: We separate compliance from information security. Compliance is considered an operational activity with oversight from internal audit. While there is some overlap in these activities, the objectives are different. Compliance tends to focus on validating compliance with specifically defined controls and regulations. Our information security team focuses on protecting sensitive data from an ever-evolving threat landscape.

SC: With which privacy regulations (in the U.S. and abroad) must you comply?
FS: There are many privacy regulations at the U.S. state and federal level and in many other countries in which we do business. Our privacy objective is to keep the commitment to our consumers to safeguard their data. We have robust information security programs and internal controls to achieve this objective.

SC: What advice would you give to individuals looking to enter the field of information security?
FS: Hiring talented information security practitioners has been one of my greatest challenges. My best advice is to be patient—I’ve taken six to nine months to fill some positions. Recently, our recruiting has focused on skills that are complementary to information security. For example, an internal auditor develops skills that are easily morphed into a threat analyst. We have had much success in hiring people with complementary skill sets, but without information security experience, and then providing them with training and mentoring.

SC: How will the role of the CSO look in the future?
FS: I think the role will be more business integrated. The CSO’s responsibilities will expand and probably ultimately evolve into managing total risk to the company. There’s enormous potential job growth in this space because, as technology continues to expand, and as the Internet of Things concept grows, the need for risk management and security will grow exponentially. Those companies that do security well will succeed and those that don’t will struggle.

A more extensive version of this Q&A is available on our website.

FORREST SMITH:
CISO, Nissan Americas

...educate executive management until you gain their support...
Federal departments and agencies are implementing procedures...  

– Kelly James, Treasury Board of Canada Secretariat

Security tools and services are available to block leaks of private data, but the government of Canada lags in adoption, reports Jesse Staniforth.

At the very beginning of 2014, a startling story pertaining to the federal government of Canada’s data security appeared on the website of National Post. Citing fallout from a series of massive breaches of private data, the news outlet reported that departments across the federal government were considering an all-out ban on USB keys and other portable storage devices.

The article followed up on a story from a week earlier that the Department of Aboriginal Affairs and Northern Development Canada was considering a USB-device ban, and that other bodies – of Aboriginal Affairs and Northern and other portable storage devices.

A report on the effort to ban mobile devices listed four other USB-key losses, as well as six lost BlackBerry smartphones, two lost laptops, and a possibly stolen iPad as having been investigated by PWGSC.

The Canadian Food Inspection Agency – Kelly James says, “Federal departments and agencies are implementing procedures that address the requirement for the secure safeguard of information, particularly personal information and other kinds of sensitive information.” James affirms that the Treasury Board of Canada Secretariat is at work on “a policy implementation guideline for the secure use of portable data storage devices (including USBs),” which is scheduled to become available to the public via the Treasury Board website “very soon.”

“This new policy will provide direction to departments and agencies on their responsibilities regarding the use of portable data storage devices within the government of Canada, including the appropriate storage, transport, clearing of information assets stored on the devices and disposal of the devices,” James explains.

Bureaucratic obstacles

This much does not reassure Cedric Jeannot, CEO of I Think Security, a Kitchener, Ontario-based firm that specializes in data-centric security approaches. In his opinion, bureaucratic obstacles prevent the Canadian government from embracing the robust security solutions that major corporations employ to protect their bottom lines, a situation that results in a continuing threat to the private information of millions of Canadians.

“When a conglomerate like Procter & Gamble chooses security, they choose the best,” Jeannot says. “With the government, that ‘when’ is always postponed. They’re trying to make a difference, but they have to play politics. Someone has to approve it. There’s limits on what your department can do.”

By the time a department can approve a security procedure, often the software they’re considering employing has become obsolete, meaning large portions of the discussion must begin all over. Not to mention that when change occurs, it’s often under duress, which Jeannot says is a recipe for disaster.

“When adoption of new technology finally happens, it’s usually because my back is against the wall – what am I going to do?” he says. “That’s usually the worst decision you can make.”

Tony Abou-Assaleh, CEO of TitanFile, a cloud-computing provider based in Halifax, Nova Scotia, concurs. “One of the obstacles is that there are so many different systems used by different agencies, departments and ministries,” he says. “These systems generally don’t talk very well to each other, they’re very heterogeneous. And they impact different budgets. Even if they’ve identified the right technology, they’re happy with it, it’s secure and solves all their problems, to actually go and implement it is going to be very challenging.”

But identifying the right technology is perhaps the biggest stumbling block of all. At least Jeannot and Abou-Assaleh agree that banning USB devices is a strategy that will yield little in increased security.

“If they ban USB devices and they allow Dropbox, or if they later ban Dropbox but allow standard insecure email communications, all they have done is shifted the public focus from the immediate problem without addressing the overall issue,” says Abou-Assaleh. Jeannot agrees. “The problem is not banning USBs,” he says. “You’re fixing the consequences but not the source of the problem. But, even strengthening security of USB devices is not enough, Jeannot maintains. Considering the $270,000 that HRSDC spent last year to distribute 2,338 encrypted USB keys and 40 encrypted external hard drives to its employees, he’s dismissive.

“Encrypted USB devices only solve one of about 10 problems,” he says. "Of course it’s better than unencrypted devices. The thing is it’s just patching a hole on the left side, but what are you doing on the right side? Do you have appropriate protection on other ways of communicating? How comprehensive is the security?”

Jeannot doesn’t believe the government currently has a framework for understanding how information flows and how the information is gathered in order to secure it. “They do one thing at a time,” he says. “They see a mobile problem, so they address mobile issues now. It’s a shorter fix.”

For Abou-Assaleh as well, the key to understanding federal security problems begins by considering the confusion over what is happening in the government’s systems. “If we read reports from the Privacy Commissioner of Canada,” he says, “we will see that the issue is not only in the number of breaches happening, but the number of breaches that are not being tracked, monitored and reported.”

In many cases, he adds, it is not even known what the impact of a breach is.

In order to provide adequate protection, the government needs to work with a system that balances end-user access to information with the ability to preserve privacy and prevent unauthor- ized access. “Management needs to have visibility into reporting so that they know when a breach happens, and what is the extent of the impact,” says Abou-Assaleh.
Federal policy

Naturally, given the nature of his company, Abou-Assaleh believes that a well-secured cloud would provide the best protection for the federal government’s documents. While he notes that cloud computing developed a reputation as insecure because its early development focused more on ease of use and cost-effectiveness than it did on security measures, he argues that times have changed.

His company, TitanFile, is one of several pioneering key management for cloud computing, which he believes provides resilient protection against threats. “If you look at the traditional cloud provider that claims to be a secure provider, the service provider maintains ownership of the encryption key,” he says. “Which means that if the service provider is compromised, all the data is compromised at once. It’s a huge risk. The alternative of that is to segregate management of encryption keys from management of the data.”

In this way, he says, if the federal government employs a key management solution on premises, but outsources document storage and management to the cloud, then segregation of responsibility is achieved. The only way that the security in such a system could be compromised, he says, would be if both the data and the keys were each individually breached.

Abou-Assaleh is far from alone in advocating cloud solutions for the federal government’s security problems. Jeannot, however, is not convinced that the cloud offers adequate protection for critical data, because the end-user will too often be inclined to look for ways to circumvent it for their own convenience.

“You can’t block people from doing things because that is not providing real security,” says Jeannot. “It might seem like you are, because you’re blocking people from using mobile devices when you’ve had a mobile-device problem, but people are going to find a way around it.”

Moving to a cloud system, Jeannot acknowledges, would bring many “massive advantages” to the federal government, particularly with regard to streamlining data access and improving efficiency.

“The problem is,” he says, “if you have all your eggs in one basket, and the basket gets broken, you’re in trouble. So, security is a critical piece in terms of the cloud, because if you don’t get the security right, it’s going to be worse than before.”

As long as you don’t address security properly, you can’t move to the cloud—which would be the right way to do it, he adds. “What they do instead is they block people from using services, and people just find a way around it.”

As far as Jeannot is concerned, data-centric security circumvents worries about breached lines of security. “Who cares about your company’s perimeter?” he says. “If someone gets in, you’re screwed. So you might as well secure the document itself. You can’t operate under the assumption that you can keep people out.”

There’s a lot of foreign companies which have a lot of resources and a lot of very clever people, he says. “If people want to get in, they can, period. It’s just a matter of how long it’ll take them.”

Jeanot’s approach, then, is to make secured data difficult and economically trying to access so potential attackers will pass on to easier targets. “It’s very much like the analogy of if a bear is running after you,” he laughs. “You don’t need to be the fastest runner, you just need to be the second worst.”

However, Abou-Assaleh stands by the power of well-implemented cloud security. Nonetheless, he and Jeannot agree again that no matter what the government determines is the strongest method for protecting the data of Canadians, they shouldn’t expect to see it implemented quickly.

“We cannot really expect the federal government to be a pioneer in adopting new technology,” Abou-Assaleh says. “For good reason: Because you want the technology to prove itself, before you risk your infrastructure on it.”

Not to mention, adds Jeannot, there’s no government program for testing new technological approaches to security. “Because the government doesn’t want to tell you, ‘We have a massive security problem with mobile devices.’ It would be like saying, ‘We have huge vulnerabilities – come and attack us!’”

Since that security problem exists, however – and is being investigated at the moment by the Privacy Commissioner for Canada – solutions are necessary as soon as they become agreed upon.

“We don’t need better engineers,” says Jeannot. “Technology to address data loss and cyber security exists. But it’s not implemented. They need to have a comprehensive security approach around all their information, whether it’s cloud or mobile, that includes all those things so you can address it the right way.”

If Bank of America or J.P. Morgan is doing it, there’s no reason the Canadian government shouldn’t be doing it, he argues. “The technology is there and the best practices exist, but you have to be willing to change, rather than pretending there’s no problem.”

Abou-Assaleh, for his part, is cautiously optimistic that it can be done, so long as it’s done right. “In my opinion, the best approach is to do it one step at a time,” he says. “Find one, two or three departments that are willing to collaborate on an initiative. Start there, prove that it works, and then spread it incrementally throughout Canada.”

...if you have all your eggs in one basket...you’re in trouble.”

― Cedric Jeannot, CEO, I Think Security
Small and midsized businesses are not exempt from cyber attack, reports James Hale.

Companies with fewer than 500 employees are used to running lean operations. And, in most sectors, operations have only gotten leaner since 2008. Chances are, online security has not been a leading area of new investment, underpinned by the justification that digital criminals are only looking for the big score.

And that kind of thinking can have its own implications for the bottom line, according to industry observers, to say nothing of seriously negative impacts on the reputation of small- and midsized businesses (SMBs) and their relationship with customers whose information has been compromised.

“The days of SMBs flying under the radar are over,” says Steve Schlarman, GRC strategist with RSA, the security division of Hopkinton, Mass.-based EMC.

“In this environment, you have to know the overall landscape, determine what’s at risk and develop a strategy to protect it,” says Davis.

He and others recommend making a member of the senior management team responsible, and ensuring there is funding to put safeguards in place.

“Fundamental change occurs when your IT people report to the CFO,” says Eric Chiu, president and co-founder of Mountain View, Calif.-based HyTrust. He says that IT departments are adept at looking for faster and cheaper ways of getting a job done, something that resonates when the issue of limited resources rules strategic planning.

That mindset has to change,” says Chiu, adding that security does not need to be costly if companies implement strategies to safeguard essential data.

Frequently, solutions can be scaled to suit the size and budget of organizations, and data and systems can be prioritized based on how critical they are to the company and its stakeholders.

“Eventually,” he says, “look at everything, assume that an attacker is already on your network and monitor all your activity.”

As he considers the prescriptive approach for SMBs, “holistic” is the word that RSA’s Schlarman also applies. “Understanding how data gets handled is the key,” he says. “It’s easier to start with the physical network and its entry points. That makes it easier to think about the virtual realm.”

He adds that thinking like the enemy does not hurt, either, recommending that organizations consider the worst things that could happen and ask questions about where the security holes are.

“The bad guys are good at identifying those holes, so if you’re only focused on keeping the hordes of barbarians from the front door, the ninjas can still be crawling in your windows.”

It sounds like the ultimate no-brainer, says Kristine Briggs, Neerbais’s vice president of operations, “but writing down everything concerning your security risks and your potential response helps. Write it down, and really discuss it seriously. If senior management and other parts of your company are on a different page, it’s a problem.”

“I don’t think companies should ever contract out their security strategy,” she says. “And, regardless of what you decide to outsource, you have to really apply due diligence. Even with the largest vendors, you can't make assumptions that you’re being protected adequately.”

Eric Chiu agrees. “Fundamentally, you should keep security as an internal function,” he says. “Outsourcing will always be your least-cost option, but you lose your oversight. A lot of suppliers will have no idea if you’ve been attacked.”

And, no matter how good they are, vendors can’t think of everything, says Schlarman. “Someone has to connect the dots among all the assets in your network, and that should be you.”

Only those actually running a business can grasp the true nature of what could be at risk if a DDoS or other type of attack is successful. What would the cost be in terms of reputation, service interruption or fraud? Schlarman says that while SMBs can outsourcing some things, someone inside the organization — someone with fiscal responsibility — must have oversight.

“If you do outsource, you have to really pay attention to your service level agreements,” he says. “Vendors can’t and won’t think of everything. When the cost of failure is this high, you can’t afford to give up accountability.”

Well-run SMBs know how to balance control and outsourcing, concludes Corero’s Stepphenson. “You have to know your own business and have total oversight. Only after you’re in that position can you really assess your risks, understand the threats and be proactive about your security.”

### TIPS FOR SMBs: Batten down

When it comes to assuring a security profile for SMBs, Kristine Briggs, Neerbais’s vice president of operations, preaches four key principles:

1. **Understand your risk tolerance and create a written security strategy.**
2. **Create a great security team and focus on continuous improvement.**
3. **Develop an easy-to-understand risk management framework and share it throughout your company; and**
4. **Determine the essential elements within your security budget.**

The last one depends on what kind of company you are,” she says. “But there are always some ‘must haves’ like spam control, network segmentation, anti-spyware, and overall security awareness.”
Zero-day vulnerabilities

LESS THAN ZERO?

Organizations are struggling with how to more quickly account for and guard against zero-day vulnerabilities, reports Karen Epper Hoffman.

For information security professionals, zero is much more than nothing.

Zero-day vulnerabilities – holes in software that are not generally known nor protected against – are indeed a growing concern for organizations as criminals get increasingly savvier about how to use these liabilities to their favor. In the end, experts say, it is becoming a race between how fast software makers and researchers can uncover these holes – which most commonly target Microsoft, Adobe and Java software – and criminals get increasingly savvy about how to use these liabilities to their favor.

Mark Elliott, founder and executive vice president of Zscaler, says the number of bugs.

“Things like development life cycles that put emphasis on security and require security-focused testing help reduce the number of bugs,” says 

Additionally, companies are investing in exploit mitigation technologies – like memory protections sandboxes or Microsoft’s Enhanced Mitigation Experience Toolkit, which Williams says can make it “much more challenging for vulnerabilities to result in useful code execution.”

Nonetheless, when they do hit, zero-day exploits can be more damaging than most because they strike where no one is looking and can remain undetected owing to the fact that much current security software seeks out malicious code based on known signatures.

“Zero days are incredibly valuable to the attackers...they don’t want people to know it exists, and [the length of time] between when they discover it and when they disclose it can vary,” says Mark Elliott, founder and executive vice president of Quanti Technologies.

Or, in the words of Allen Harper, chief hacker and executive vice president of Tangible: “We have a blind spot growing in the security field and that’s zero-day.”

Alex Cox, principal security researcher for RSA FirstWatch, says zero-day exploits targeting Java in particular “tend to be the most damaging as many enterprises don’t have a solid patching process for it, and vulnerabilities tend to be exploitable for a longer period of time between patch cycles.”

But, other experts point out that while the threat certainly hovers, actual damage has of yet been minimal. “The continued string of high-profile compromises, to Adobe source code in particular, has the potential to cause an explosion of zero-days, but we haven’t really seen that yet,” says Cox. “The potential is there, just unrealized as of yet. I’d say that the use of zero-days has increased along the same line as the threat. That is, as the bad guys’ sophistication has increased, so has their ability to use zero-days in their attacks.”

In fact, says Williams, the growth rate of zero-day threats is set by the number of people attempting to exploit users of the internet. “We’re seeing a much more targeted use of zero-day threats these days,” he says.

Michael Sutton, vice president of security research for Zscaler, says the landscape for zero-day vulnerabilities has evolved significantly in recent years as software makers, Microsoft in particular, have gotten increasingly better about putting out patches, and organizations have become more adept at shortening the patch cycle. Instead, it’s no longer the “low-hanging fruit” of simple vulnerabilities, Sutton says. “It’s not getting worse so much in terms of sheer volume, it’s the severity of the threats and the length of time they are taking to come to the surface to get to where a vendor can address them,” Sutton says.

In the meantime, there is a lot of money to be made in zero-day vulnerabilities, by the criminal underground and nation-states alike.

Anup Ghosh, CEO and founder of Invincia, believes the problem will get bigger come April, when support for Windows XP ends, and new vulnerabilities may keep cropping up without getting fixed. “We’re about to enter a period where zero-days will be very common on Windows XP machines, with no patches available,” Ghosh says.

Jeff Davis, vice president for engineering at Quanti, agrees that this causes a problem, especially since 30 percent of PCs are estimated to run the Windows XP operating system.

With more and trickier zero-day exploits on the horizon, what can organizations do to streamline the process so that they can account for these vulnerabilities, find them and protect against them?

“You can’t patch what you don’t know about,” Sutton points out, adding that all organizations need to start with a well-oiled patch management process which monitors public sources, as well as commercial feeds, for reports of potential zero-day vulnerabilities. Monitoring, he says, also must take into account the fact that employees are bringing new computing assets into the corporate environment – creating a need to update patching on new devices.

Stefan Frei, research vice president for NSS Labs, points out that not all exploits do affect the latest versions of a program or an operating system. Having the latest versions installed and kept up-to-date is effective in preventing known exploits and zero-days that affect older versions – for example, a zero-day for IE 7 which is ineffective against IE 10, he says. Further, the latest versions of operating systems typically deploy exploit mitigation techniques to protect the OS and programs running from exploitation, which at least make it much harder to successfully exploit the box. To benefit from these protection features, he recommends upgrading XP boxes or older operating systems.

“If you are a high-value target, assume you are compromised by zero-days, unpatched programs or internal attackers,” Frei says. “As 100 percent protection is an illusion, be prepared to detect a breach early and have a process to handle it. Many protection suites promote ‘ahead of the threat’ protection, but often fail to even block long-known exploits in our tests.”

Nonetheless, when they do hit, zero-day exploits can be more damaging than most because they strike where no one is looking and can remain undetected owing to the fact that employees are bringing new computing assets into the corporate environment – creating a need to update patching on new devices.

Williams believes the best way to mitigate zero-day events is defense-in-depth. “The trouble with these is that the attackers can be committed to avoiding detection – this is why they are using a zero-day in the first place,” he says. “By using multiple security devices with different detection engines one can maximize coverage. Additionally, opting in to telemetry systems can help vendors enhance coverage.”

Ultimately, says Sutton, it’s always going to be an arms race and the bad guys will always have the advantage. “They only need to find one chink in the armor.” He recommends that companies also look to security solutions that rely on behavioral analysis and sandboxing. “Treat everything as untrusted,” he says.
Connection issues prompted an educational service in Illinois to find a solution to speed distribution of teaching materials. Greg Masters reports.

It’s all about connections, but it’s not always about who you know. In the case of an education service in Illinois, it’s about what tools are used to facilitate communication.

Libertyville, Ill.-based Ombudsman Educational Services (OES) was having issues with its network connectivity, and this was unacceptable for an education service needing to provide teaching materials to students across 120 school districts.

OES is a division of Educational Services of America (ESA), a leading provider of behavior therapy and alternative and special education programs for children and young adults. ESA provides services to thousands of children and adults with special needs at its 130 schools.

“Connection issues is a concern in the educational environment,” says Harold Ragland, director of network infrastructure, and Blayne Potter, WAN administrator, led the charge.

Being an OES customer, the team decided to try its access points product. “We were using Fortigates for security and decided to try the FortiAPs when they were available,” says Ragland. “The testing went great and by using the Fortigates as WLAN controllers, our network complexity was reduced as was the capital expenditure of our future expansions by eliminating the other vendor’s controller.” An additional benefit, he says, was that operating expenses also were lowered by having fewer devices to cover with support.

Having the ability to provide teaching materials and video to its students via the WLAN is a basic requirement, Ragland says.

His team also wanted to reduce the costs of its new Learning Center deployments. “Not needing a traditional Cat5 [Ethernet cabling standard] infrastructure reduced cost and network build-out time,” he says. “We can build a Learning Center network in one day.” Deployment was very smooth, he adds. “We were up and running in 30 minutes.”

Managing the APs directly from the central location, such as a data center, provides through FortiManager or FortiAnalyzer products, so a network manager needs only one screen to understand issues on the network and provide assistance with troubleshooting or reporting at any time. Meanwhile, Ombudsman/ESA is expanding rapidly and plans on installing Fortigates and FortiAPs in all its new schools.

At press time, 80 percent of the locations are 100 percent wireless. And, as new threats arise every day, the Fortinet implementation helps the facility keep students and faculty safe, as well as prevent access to unwanted sites and blocking malware and viruses.

What differentiates the Fortinet offering is that the wireless network is an overlay to the enterprise security network in competing offerings, Sundstrom explains. Wireless users are mapped to the wireless network first and then remapped onto company-wide security policies in a ‘best efforts’ manner.

“Not only are there security risks in a multilayer access approach, there is ultimately a higher total cost of ownership,” says Sundstrom. “Whether the overlay network is controller- or cloud-based, both have higher costs due either to extra hardware costs or monthly and annual recurring managed services costs.” Fortinet, he adds, does not charge a separate annual fee for the ongoing wireless controller interface or a monthly or annual fee for each access point.

The Fortinet wireless solution supports multiple methods for updating equipment, either directly from the Fortigate or from the FortiManager centralized management software, Sundstrom says. Centralized profiles associated with access points, enable updates to be easily pushed out from a central location, such as a data center, based on the needs of each profile.

Additionally, access points can be updated individually if the network manager is having trouble with one specific access point. Reporting identifies any issues and drill downs are available to immediately isolate and fix them.

Case study

EASING LEARNING

Connection issues prompted an educational service in Illinois to find a solution to speed distribution of teaching materials. Greg Masters reports.

FortiAPs are deployed in all 130 schools and the enterprise’s headquarters. Fortinet touches the entire company across all divisions, which allows Ombudsman to report status per the Child Protection Act. The entity also has the capability to uncover and mitigate rogue APs, which could possibly allow for their users’ personal information to be leaked.

Fortinet has combined security and access into a complete solution, says Neil Sundstrom, VP wireless solutions at Fortinet. “A controller for the wireless access points is built into every Fortigate UTM appliance, delivering a single pane of glass for management of both the wired users and the wireless users.”

Owing to this combination, a network manager can provide the same user, device and application security policies to both the wired and wireless users, he adds.

Detailed reporting on the network, users, applications and devices is provided through FortiManager or FortiAnalyzer products, so a network manager needs only one screen to understand issues on the network and provide assistance with troubleshooting or reporting at any time. Meanwhile, Ombudsman/ESA is expanding rapidly and plans on installing Fortigates and FortiAPs in all its new schools.

At press time, 80 percent of the locations are 100 percent wireless. And, as new threats arise every day, the Fortinet implementation helps the facility keep students and faculty safe, as well as prevent access to unwanted sites and blocking malware and viruses.

What differentiates the Fortinet offering is that the wireless network is an overlay to the enterprise security network in competing offerings, Sundstrom explains. Wireless users are mapped to the wireless network first and then remapped onto company-wide security policies in a ‘best efforts’ manner.

“Not only are there security risks in a multilayer access approach, there is ultimately a higher total cost of ownership,” says Sundstrom. “Whether the overlay network is controller- or cloud-based, both have higher costs due either to extra hardware costs or monthly and annual recurring managed services costs.” Fortinet, he adds, does not charge a separate annual fee for the ongoing wireless controller interface or a monthly or annual fee for each access point.

The Fortinet wireless solution supports multiple methods for updating equipment, either directly from the Fortigate or from the FortiManager centralized management software, Sundstrom says. Centralized profiles associated with access points, enable updates to be easily pushed out from a central location, such as a data center, based on the needs of each profile.

Additionally, access points can be updated individually if the network manager is having trouble with one specific access point. Reporting identifies any issues and drill downs are available to immediately isolate and fix them.

We can build a Learning Center network in one day.”

—Harold Ragland, director of projects, Ombudsman
A spate of recent DDoS attacks forced banks to change their threat response — and that’s a good thing, reports Teri Robinson.

When the first wave of distributed denial-of-service (DDoS) attacks hit several, large financial institutions in the fall of 2012, a scramble ensued to get websites back up and quell the fears of understandably rattled customers. By the time the third and final wave rolled through in early 2013, banks had learned how to shut down attacks quickly and had taken significant steps to restore the public’s faith.

While the concentration of incursions left in their wake a heightened awareness, the series also ushered in major changes to the way banks handle such incidents, marked by an unprecedented level of communication among banks, their executives, government agencies and customers.

Although bigger banks have learned to mitigate the impact of DDoS attacks, and indeed the large-scale campaigns have tapered off, experts say the financial industry, particularly smaller banks, are still at risk. There’s little doubt that DDoS attacks on the rise — a Digital Attack Map, developed by Google and threat monitoring company Arbor Networks, shows that the U.S. is one of two countries to get hit every day for a five-month period in 2013 — and these strikes and the threat of further attacks pose a significant threat.

“Knocking over” banks is nothing new. Frank and Jesse James, Butch and Sundance, Bonnie and Clyde, Willie Sutton all have relentlessly — and often successfully — tried to breach whatever passed as the top-of-the-line bank security forces within the Iranian government were lured by money buried deep in the bank vault. The large-scale DDoS campaigns of 2012 and 2013, by and large, were driven by ideology, with no other goal but to shake things up and grab headlines. And, that they did, with the first attacks — breathing in their scope and impact — coming on the eve of the 2012 presidential election to maximize their PR value.

The nature of the attacks originally led security experts to believe that the campaigns were the work of forces within the Iranian government — a charge that officials there have denied. “The big difference in 2013 is nation-states started using (DDoS attacks) as tools for retribution for the onslaught, though they couldn’t prevent the attacks, even with pointed warnings, they quickly shut them down with minimal disruption.”

“Banks became more proficient in stopping DDoS or mitigating the effect,” says Al Pascual, analyst at Javelin Strategy & Research.

A new strategy
That the financial institutions were able to minimize the impact of the third wave speaks to the aggressive — and in some cases, unprecedented — tactics taken in the wake of the first attacks and which quickly evolved traditional bank strategy for dealing with cyber incidents.

Not surprisingly, as a first line of defense, banks took advantage of the tremendous amount of bandwidth at their disposal and simply over-provisioned. Just as adding eight additional lanes to a busy six-lane interstate highway would relieve traffic congestion, the extra bandwidth let normal banking activity proceed — even as large volumes of junk traffic passed through their networks.

“They have a decent amount of bandwidth,” says Pascual. “And over provisioning is tried and true.” Rerouting traffic to alternative sites also helped balance the load and smooth traffic flow.

The financial institutions also turned to anomaly detection, identifying attributes that characterized an impending attack, and conducted regular scans of their systems to uncover zero-day exploits. Larger banks, too, could afford the luxury of expensive appliances that analyze traffic and separate the good from the bad, with bad traffic routed off of the website.

But the real progress against the hackers came after financial institutions broke with established protocol and opened the communication lines in all discretionary attacks.

In the past, financial institutions had remained almost pathologically tight-lipped when targeted by cyber criminals. To preserve their reputations and, in part, to prevent further panic, they had quietly mitigated network problems. But, caught in waves of such sweeping and public attacks that slipped by their defenses, these organizations had virtually no choice but to exchange information with other financial institutions, flagging servers and IP addresses that might indicate the beginnings of additional attacks.

“At first, they weren’t talking and they got hit hard,” says Pascual. “When they talked they could stop the attacks. They were all in the same boat — [being attacked] by the same people.”

The dialog among banks quickly moved up the food chain to the executive suite, where CIOs and other top management uncharacteristically shared information with their counterparts at other financial institutions and became an integral part of the battle to counter future DDoS strikes. “It became a CEO-level issue in large financial institutions,” says John Carlson, executive vice president of BITS, the technology division of the Financial Services Roundtable. Javelin’s Pascual agrees, noting that banks had always communicated about fraud, but at

“The first campaign was launched against 10 of the biggest names in banking – HSBC Holdings, Citibank, Capital One, JPMorgan Chase, U.S. Bancorp, SunTrust Banks, Bank of America, PNC, Wells Fargo and Regions Bank. Initially, the financial institutions were caught off guard and slow to react as large volumes of unwanted traffic flooded their networks, blocking customers from their accounts and otherwise disrupting business.

But, if there were any doubts that banks were under siege, It-Ad Din al-Qassam dispelled them by issuing a series of warnings on Pastebin and IP addresses that might indicate the beginning of additional attacks.

“We have a decent amount of bandwidth,” says Pascual. “And over provisioning is tried and true.” Rerouting traffic to alternative sites also helped balance the load and smooth traffic flow.

The financial institutions also turned to anomaly detection, identifying attributes that characterized an impending attack, and conducted regular scans of their systems to uncover zero-day exploits. Larger banks, too, could afford the luxury of expensive appliances that analyze traffic and separate the good from the bad, with bad traffic routed off of the website.

But the real progress against the hackers came after financial institutions broke with established protocol and opened the communication lines in all discretionary attacks.

In the past, financial institutions had remained almost pathologically tight-lipped when targeted by cyber criminals. To preserve their reputations and, in part, to prevent further panic, they had quietly mitigated network problems. But, caught in waves of such sweeping and public attacks that slipped by their defenses, these organizations had virtually no choice but to exchange information with other financial institutions, flagging servers and IP addresses that might indicate the beginnings of additional attacks.

“At first, they weren’t talking and they got hit hard, says Pascual. “When they talked they could stop the attacks. They were all in the same boat — [being attacked] by the same people.”

The dialog among banks quickly moved up the food chain to the executive suite, where CIOs and other top management uncharacteristically shared information with their counterparts at other financial institutions and became an integral part of the battle to counter future DDoS strikes. “It became a CEO-level issue in large financial institutions,” says John Carlson, executive vice president of BITS, the technology division of the Financial Services Roundtable. Javelin’s Pascual agrees, noting that banks had always communicated about fraud, but at

The nature of the attacks originally led security experts to believe that the campaigns were the work of forces within the Iranian government — a charge that officials there have denied. “The big difference in 2013 is nation-states started using (DDoS attacks) as tools for retribution for the onslaught, though they couldn’t prevent the attacks, even with pointed warnings, they quickly shut them down with minimal disruption.”

“Banks became more proficient in stopping DDoS or mitigating the effect,” says Al Pascual, analyst at Javelin Strategy & Research.

A new strategy
That the financial institutions were able to minimize the impact of the third wave speaks to the aggressive — and in some cases, unprecedented — tactics taken in the wake of the first attacks and which quickly evolved traditional bank strategy for dealing with cyber incidents.

Not surprisingly, as a first line of defense, banks took advantage of the tremendous amount of bandwidth at their disposal and simply over-provisioned. Just as adding eight additional lanes to a busy six-lane interstate highway would relieve traffic congestion, the extra bandwidth let normal banking activity proceed — even as large volumes of junk traffic passed through their networks.

“They have a decent amount of bandwidth,” says Pascual. “And over provisioning is tried and true.” Rerouting traffic to alternative sites also helped balance the load and smooth traffic flow.

The financial institutions also turned to anomaly detection, identifying attributes that characterized an impending attack, and conducted regular scans of their systems to uncover zero-day exploits. Larger banks, too, could afford the luxury of expensive appliances that analyze traffic and separate the good from the bad, with bad traffic routed off of the website.

But the real progress against the hackers came after financial institutions broke with established protocol and opened the communication lines in all discretionary attacks.

In the past, financial institutions had remained almost pathologically tight-lipped when targeted by cyber criminals. To preserve their reputations and, in part, to prevent further panic, they had quietly mitigated network problems. But, caught in waves of such sweeping and public attacks that slipped by their defenses, these organizations had virtually no choice but to exchange information with other financial institutions, flagging servers and IP addresses that might indicate the beginnings of additional attacks.

“At first, they weren’t talking and they got hit hard, says Pascual. “When they talked they could stop the attacks. They were all in the same boat — [being attacked] by the same people.”

The dialog among banks quickly moved up the food chain to the executive suite, where CIOs and other top management uncharacteristically shared information with their counterparts at other financial institutions and became an integral part of the battle to counter future DDoS strikes. “It became a CEO-level issue in large financial institutions,” says John Carlson, executive vice president of BITS, the technology division of the Financial Services Roundtable. Javelin’s Pascual agrees, noting that banks had always communicated about fraud, but at

“Banks became more proficient in stopping DDoS…”

— Al Pascual, analyst, Javelin Strategy & Research
It became a CEO-level issue in large financial institutions.

— John Carlson, executive vice president, BITS

DDoS attacks

lower levels of the organization, like the IT and security departments.

Indeed, says Ashley Stephenson, CEO at Correro Network Security, CEOs often, like everyone else, “found out about attacks on the news.”

In the aftermath of the 2012 attacks, CEOs set up and took notice and met regularly with other industry groups, like the American Bankers Association (ABA) and Financial Services Information Sharing and Analysis Center (FS-ISAC). The DDoS. Financial Services Roundtable, which represents 100 of the largest financial institutions, brought bank leaders together to discuss the attacks and hash out solutions.

Executive involvement helped drive awareness down throughout the organization and sparked a concerted campaign to educate employees. By schooling workers, banks increased the likelihood that they would not only recognize potential threats but would understand the protocols they should follow — from reporting suspicious activity to activating security measures before a threat spun into an outright attack.

This well-informed constituency and united front were instrumental in managing the DDoS threat.

Likewise, banks openly and freely exchanged information and worked closely with regulators, ISPs and government agencies — such as the Treasury Department, DHS, the FBI and the Secret Service — to identify solutions and to hash out guidelines for mitigating the impact of attacks and thwarting future campaigns. The attacks were “a catalyst for the industry and government to step up and focus on cyber security,” says Carlson. “It’s like flooding a highway with traffic to bring things to a halt,” not blowing a bridge that the cars are trying to get across.

Financial institutions have a vested interest in keeping accounts visible to account holders. Customers play a critical role in bank security — no one more diligently monitors bank accounts than the account-holders themselves. “Half of fraud is detected by customers,” says Pascual. When spam and other unwanted traffic obscures normal banking activities, customers simply aren’t able to engage in that critical monitoring. Instead of scaring off customers, the admission that banks had been under attack — and the subsequent campaign to educate account holders — paid off and their fears never bubbled over into full-scale panic.

It helped, too, that the attacks dwindled and large banks seemingly moved out of the crosshairs of the and their decision to launch the DDoS strikes. If the point was to dazzle and draw attention to their cause, then Pascual and Carlson don’t anticipate an escalation in DDoS attacks because the industry is now more adept at spotting attacks and they’re not as likely to draw headlines.

No rest for the wary

While the heat may be off banking giants for the time being, security gurus don’t expect DDoS threats to disappear, but rather to shift in nature.

As a 2012 Christmas Eve attack against San Francisco Bank of the West demonstrated, DDoS attacks are effective smokescreens for tapping and draining accounts. In that case, cyber criminals walked away with more than $900,000. And unlike bank robbers of old, they didn’t have to risk life and limb or shoot their way out of a bank lobby.

DDoS attacks
Unified threat management

These tools are the first line of defense in protecting the enterprise network from malware, but selecting the right option depends on requirements, says Technology Editor Peter Stephenson.

T
he definition of unified threat management (UTM) has evolved over the years since the term was coined in 2004. Today it has become a bit of a catchall for gateway-type devices that perform a bevy of security tasks. We are even beginning to see UTM products for the virtual world. So, it was no particular surprise this month when we saw the dichotomy of a mature though still evolving product type.

The whole idea behind a UTM is that one takes to the enterprise a handful of security tools that belong at the gateway, puts them all in the same box, lets them talk to each other and share data, and then manages the tools under a single pane of glass. Pretty good in theory, but how well does it work?

To answer that question we need to look at the issues that a UTM is intended to address. The first thing we can look at — and this is one of the traditional functions — is the firewall. Firewalls benefit from bandwidth and data. As well, especially if they are application layer firewalls, they benefit from being able to do deep-packet inspection. They also produce data — in that they collect the results of access attempts that result in denies. Well-configured firewalls, in some cases, also make pretty good data leakage prevention tools.

The aspect that really benefits from lots of data is the intrusion prevention system (IPS). The IPS makes judgements based on the full contents of the packet, especially the header, of course, but payload can be extremely important. While we don’t need deep detail in many cases for alerting, or even blocking, there are certainly situations that demand a closer look at the data. Particularly when there may be malware involved, the IPS can act as a companion to the anti-virus (AV) gateway. The AV gateway can act in a number of ways. Of course it looks at data coming into the network, but it also can provide the connections to the backend — i.e., the endpoint devices. Kibh and kim to these two gateways we have the email and content filtering functionality. All of these inspection tools acting together have two significant features: they do a lot of analysis and they take a lot of resources. Performing an AV scan, comparing reputation against white- and blacklists, looking at firewall rules all take resources — on the network and, especially, in the UTM device itself.

This is a hard assignment this month. We saw several really superb products and shoppers are really going to need to analyze unique requirements closely to make the right choice. Often in this column, readers hear that all the tools we examine are competent so they won’t go too far wrong selecting, in most cases. Not this month. The differences between these products are subtle. Your choice will depend on such things as your network architecture, your bandwidth requirements, what kind of a target you are (bank, manufacturer, government agency, etc.) and what your overall attack surface is.

Probably the most important piece of today’s UTM is the AV engine. Just about every major attack has a malware component, and much of the malware is zero-day. You need a better-than-competent AV tool in that environment. So the big question is whether you select a tool that uses its own AV engine or someone else’s. Both have advantages, often involving cost. Generally speaking, if you already are using an AV tool at the endpoints that you like, pick a UTM that can work well with it. One of the ways to defeat single point of failure not involving bandwidth is to focus on defense-in-depth. By that I mean that because there are two things that can go wrong at the gateway – failure or overloading — when you start dropping packets you take the chance that you will drop something to which the UTM needs to alert you.

The bottom line: These tools are your first line of defense. Select them carefully to meet your requirements — and don’t forget to take into account your plans, if any, to virtualize or go to the cloud — and over-build a bit when it comes to managing bandwidth. It’s better to have your UTM loading some than it is to have it groan under a load. Now, on to this month’s products.

Erratum: On page 46 of the January issue, we erred in quoting a price for the license cost of the Swivel Secure Swivel Appliance. It should have read: The license price for the license cost of the Swivel Secure Swivel Appliance is $94 to $1.28 per user. Our apologies for the error.

• March 2014 • www.scmagazine.com

PRODUCT SECTION

GROUP TEST | UTM

Specifications for unified threat management tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Firewall</th>
<th>Intrusion prevention</th>
<th>Gateway anti-virus</th>
<th>Gateway anti-spam</th>
<th>Web content filtering</th>
<th>Email content filtering</th>
<th>Application control</th>
<th>Integrates with client-side anti-malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Software Technologies Next Generation Threat Prevention Appliance</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
<tr>
<td>Cyberoam Technologies Pvt Ltd CR200NG-XP v10.04.5</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
<tr>
<td>Dell SonicWALL NSA 4600 v6.1.1.5</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
<tr>
<td>Fortinet FortiGate 140D-PoE</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
<tr>
<td>SecPoint Protector P800 v24.5.4</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
<tr>
<td>VASCO Data Security aXguard Gatekeeper v7.7.1</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
<tr>
<td>WatchGuard Technologies XTM 545</td>
<td>● ● ● ● ● ● ○</td>
<td>● ● ●</td>
<td>● ● ● ● ● ●</td>
<td>●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>● ● ● ● ●</td>
<td>○</td>
</tr>
</tbody>
</table>
Check Point Next Generation Threat Prevention Appliance

The Threat Prevention Appliance from Check Point Technologies provides a solid security platform that can be customized with the addition of several software blades. This tool can be loaded with blades for firewall, identity awareness, an intrusion prevention system, as well as a SmartEvent blade – all of which can be managed from one web-based management interface. The firewall blade features the same technology that drives Check Point’s FireWall-1, ensuring solid security at the gateway. The identity awareness blade provides full identity-based security policy capabilities with Active Directory integration. The IPS blade offers a full-featured intrusion prevention system to complement the firewall blade for added security. Finally, the SmartEvent blade provides a security event management and analysis platform that delivers real-time, graphical threat management data and reporting.

We found deployment and management of this appliance to be simple and straightforward. After unboxing the device and connecting it to the network, we simply had to access a web-based setup wizard to complete the initial configuration process. After the setup wizard was complete, we had a basic configuration on the appliance which could then be tweaked from the intuitive web-based management interface. Overall, we found the offering quite easy to manage via the Gaia web user interface. This interface provides easy access to all the management functions of the appliance directly in a web browser.

Aside from easy management, this solution is loaded with features and driven by a high-performance policy engine. Policy can be tailored to users and groups within Active Directory ensuring the appropriate policy and security controls are assigned as needed. Security policy can include URL and web filtering, as well as application control policies. To prevent zero-day attacks these controls are combined with a set of security functions, including anti-virus, spam protection, bot detection and a threat emulation platform. Documentation included quick-start and getting-started guides along with a plethora of PDF manuals and administration materials. The quick-start and getting-started guides provided clear instructions on how to get the appliance up and running with an initial configuration. We found all documentation to be well-organized and to include clear, step-by-step configuration instruction and screen shots.

Check Point provides several levels of assistance available to customers via a support and maintenance subscription. Plans include standard, premium and elite tiers, which offer various levels of phone- and email-based technical aid along with onsite options and response times. Customers can also access a large online area via the website. This includes a knowledge base, user forum, product downloads, technical documentation and other helpful resources.

At a price of $31,000 fully loaded, this product carries quite the price tag. We find the Check Point Next Generation Threat Appliance to be quite powerful, but also quite expensive. Overall, we find this product to be a good value for environments that need a high performance UTM.

Cyberoam Technologies Pvt Ltd
CR200iNG-XP

The CR200iNG-XP from Cyberoam Technologies offers full-scale, best-of-breed protection including an intrusion prevention system, gateway anti-virus, spam prevention at the gateway, web content filtering and a web application firewall – all driven by Cyberoam’s identity-based Layered Technology. This tool also provides granular controls over applications in use throughout the network.

We found this tool to be simple to deploy. After installing the correct network interface card module we were able to connect the tool to our network and access the web-based management interface via the default IP address of the appliance. Once logged into the appliance, we were able to run the configuration wizard to get it up and running with an initial configuration. The setup wizard not only helped us set IP and network settings, but also helped us set an initial security policy based on three different pre-defined templates. These include a monitor-only setting, general setting or strict policy.

Once we completed the setup wizard, we were able to access the web management interface to begin tweaking our configuration. We found the management interface to be well-organized and to be easy-to-navigate. We did find that the general policy setting that we configured in the setup wizard gave us a good policy base with which to work, so we had to simply add a few settings and tweak a few others and we were up and running with a pretty solid configuration. We also noticed that this product features flexible deployment options that can fit into almost any environment. The CR200iNG-XP can be deployed in a gateway mode for networks that require full firewall and perimeter security, or it can be deployed in bridge mode to integrate with existing security devices.

Cyberoam provides the user with a very complete and easy-to-follow quick-start guide. Screen shots accompany every step of the configuration process. The user guide also outlines if the end-user would like to configure the device in gateway mode or bridge mode. The guide also outlines the GUI dashboard and what the user should be observing during the setup process of the device. Additional contacts and resources for assistance or trouble shooting are provided and easy to find within the guide. A complete user guide is also provided as a PDF file within the device itself. Once again, the user guide is easy-to-read and is formatted so users have a successful installation process. The guide has numerous screen shots to assist the end-user, as well as configuration examples to fit within a company’s architecture.

This product starts with a base price of around $4,200 and requires security subscriptions to enable features and functions. The security subscriptions are available in various levels – ranging from $2,000 to around $4,000 per year – to enable features, such as malware protection and the intrusion prevention system. These subscriptions also include support costs. With all that said, we find this tool to be an excellent value for the money. The Cyberoam CR200iNG-XP incorporates a solid feature set with a reasonable cost for an overall good value.
Dell SonicWALL NSA 4600

The NSA 4600 from Dell SonicWALL incorporates next-generation firewall technology combined with a multi-core hardware platform to provide robust protection at the perimeter of even some of the most demanding networks. This appliance features a fully configurable deep packet inspection firewall, intrusion prevention system, application control, gateway-based malware protection, and URL and web filtering, which can all be managed centrally from a single high-performance platform.

We found overall deployment of this product to be simple and straightforward. Before setting up the appliance, we had to register for a MySonicWALL account and decide on our deployment scenario. Once we were ready to begin the deployment, we simply had to plug in the appliance and connect it to the network. After connecting it to the network, we were able to access the web-based setup wizard via the appliance default IP address. The setup wizard included all the steps to get the NSA 4600 up and running with an initial configuration, including deployment mode settings.

After initial configuration was complete, we were able to see the true power of this appliance through the web-based management interface. The NSA 4600 includes many highly configurable options and features, along with a multitude of visualization and analysis functions. One function we found particularly liked was the application visualization feature. Using this, administrators can get deep insight into real-time network application traffic and create policies to ensure complete security and control over network use.

SonicWALL provides a straightforward getting-started guide which provides graphics and user tips to assist the admin with a better understanding of the product, as well as setup. The SonicWALL website has done a strong job of putting all the admin guides into a well-laid-out and easy-to-find catalog. There are also video tutorials, technical notes, FAQ list, and knowledge base that is continuously updated to better able the user to become more acquainted with the device. The admin guide is user friendly and contains many helpful charts and graphs for a successful deployment.

The company offers numerous support options and levels to fit the needs of the customer – beginning with basic no cost support that includes a 90-day limited software warranty and one-year hardware warranty. Also included in the basic support are video tutorials, documentation, user forums and a knowledge base. Fee-based support options are in both eight hours-a day/five days-a week and 24/7, as well as one- to six-year durations. Fee-based support options include chat, email, web and telephone support, as well as software/firmware updates.

At a price just over $8,000 for the hardware fully loaded with one year of intrusion prevention service, gateway anti-virus, spyware protection, content filtering service, application intelligence, control and visualization and 24/7 support, we find this product to be an excellent value for the money. The Dell SonicWALL NSA 4600 provides an exceptional amount of hardware capability with a robust feature set at a reasonable cost.

Fortinet FortiGate-140D-POE

The FortiGate-140D-POE from Fortinet offers a built-in firewall, intrusion prevention system, application control, web and email filtering and anti-virus in one solid appliance. Driven by the Fortinet FortiOS platform, this tool provides robust protection at the gateway that is easy to configure and easy to manage. The FortiGate also features the FortiGuard Botnet database which prevents bot infection through the use of IP reputations.

Fortinet has continued to streamline its install and setup process to make deploying the FortiGate easier and easier year after year. This year, we noticed continued support of web-, CLI- and application-based (through the use of the FortiExplorer application) installation options, but we also noticed that the appliance now can be configured using an iPad or iPhone through the use of an app as well. Regardless of the method of deployment, we found this appliance easy to get up and running in no time at all through the use of an easy-to-follow setup wizard. At the completion of the wizard, we were able to manage the appliance from the web-based management interface.

The web-based interface of the FortiGate is also continuing on the path that was started in some of last year’s versions. We noticed that all of the parts of the chunky, old management interface are now completely gone and the interface is clean and easy to navigate, as well as customizable with many dashboard widgets and other excellent features. Aside from the easy management of the appliance, this product also features capabilities to integrate with a FortiGate wireless access point that can feed data to backend analytics software about wireless network use. This capability – coupled with the FortiGate’s solid protection functions – make it a solid network protection device.

The documentation includes a quick-start and numerous administrator guides to set up the device to meet the needs of your organization. The quick-start guide is well formatted and easy to use. There are plenty of graphics to assist the user during deployment. The separation of admin guides into sections is well laid out and provides the user with just the information that is need to configure the device, i.e. firewall, VoIP, log reporting, VDOMs, etc. The admin guides are easy to understand and take the user through the needed configuration process step by step. There are also numerous notes and tips that provide key information as the user works through each process of the configuration.

Fortinet offers eight-hours-a-day/five-days-a-week support that is bundled into the price of the device or 24/7 support for a nominal yearly upgrade fee. Fortinet presents two different support levels: Premium Support Gold and Premium Support Global Gold. Both premium packages provide customers with their own technical account manager (TAM) as a single point of contact should a problem arise.

At a price just over $4,000, we find this product to be an excellent value for the money. The FortiGate-140D-POE offers solid perimeter defense – as seen in much larger and more expensive systems – at a price that is reasonable for smaller environments without compromising functionality.
SecPoint Protector P800

The Protector UTM appliance from SecPoint offers a full set of features packed into a single device. To ensure security across the entire network, this product features a firewall, intrusion prevention system, anti-virus and anti-malware, spam protection and web content filtering capability, along with built-in vulnerability assessment functionality. The anti-virus component of the system is driven by anti-virus engines from ClamAV, Bindefender and Kaspersky and can and will be active at the same time.

Overall, we found this appliance to be easy to deploy and configure. The initial setup consisted of connecting the appliance to the network and browsing to the default IP address of the product via a web browser. Once there, we were guided through a short setup wizard that allowed us to set the network settings and licensing information along with time and date settings. After the initial setup was complete, we were able to access the appliance’s web-based management interface. We found this to be easy to navigate with an intuitive and well-organized layout. The Protector can be easily deployed in-line at the gateway without the need to reconfigure the entire network. This model allows for easy configuration with minimal downtime, as well as possible configuration errors that would lead to a decrease in protection functions.

The first thing we noticed when logging into the appliance for the first time was the dashboard, which is known as the Control Center. This featured an excellent overview of the appliance, active features and alert information. On the right side of the dashboard there is a section of alert meters that give a lucid visual overview of recent events, such as spam or viruses, which can then be clicked on for more information. Aside from its ease of management, this appliance also has solid policy options, including user-based policy that can be integrated directly with Active Directory users and groups. This user- and group-based policy engine can be used to assign not only web filtering policies, but also anti-virus and spam protection policies.

SecPoint provides a quick install guide that is straightforward and user friendly. It provides the user with different installation diagrams according to the model of the device. SecPoint uses both screen shots and images to navigate the user to system configuration. The admin guide, offered via CD format, comes either on the device or users can go to the website to obtain the manual. The admin guide is thorough and easy to understand. Screen shots provide the user with a step-by-step walkthrough of the configuration. The website also contains a large FAQ library.

SecPoint support includes 24/7 live chat assistance where users having problems can receive quick answers to their questions. Email aid is also included. To further assist the user, SecPoint provides customers with access to its user forum and online community videos.

With a price starting just shy of $700 for a five-user license, this product can be quite pricey for larger environments. However, we find the SecPoint Protector to be a good value for the money overall, based on its ease of use and comprehensive feature set.

VASCO aXsGUARD Gatekeeper

The aXsGUARD Gatekeeper from VASCO Data Security is more than just a simple UTM. This product provides a complete secure remote access platform that incorporates many perimeter security functions. The Gatekeeper can be driven by one of four available software bundles, allowing for flexibility of features and functions based on need. The standard software bundle provides a good base of functionality, including a firewall, intrusion prevention system, web content filtering, spam protection and anti-virus at the gateway. Beyond the perimeter security offerings, the Gatekeeper can also integrate with the company’s Digipass strong authentication platform for added security.

For our evaluation we took a look at the Gatekeeper Virtual Appliance. We began our installation by simply mounting the provided ISO file to our virtual machine configured per the instructions in the installation guide. Once we booted our virtual machine, the installation process began right away and after a few short steps the appliance was up and running. After the install was complete, we were able to browse to the web-based management interface via a web browser to begin configuration of the product. Upon first login to the interface, we were greeted with a short configuration wizard that allowed us to set up some basic administrative information and configure the user account.

After the initial configuration, we were finally able to access the actual management interface and begin our in-depth configuration. We found the management interface to be fairly well-organized and we were able to get accustomed to managing the product after a few minutes of clicking around. Overall, we had a pretty easy time of managing the appliance, but found there was a lot of manual configuration that had to be done after the setup was complete. This product does include a great amount of functionality, but is far from plug and play. With that said, the appliance offers some highly configurable and flexible options that can be set to work in many different types of environments.

Documentation included an installation guide for the virtual appliance, administrator guide and several other supplemental guides for configuring all the various functions of the appliance. Overall, we found all the documentation to be well-organized and to include a large amount of easy-to-follow, step-by-step configuration instructions along with screen shots and diagrams. VASCO offers eight hours a day, five days a week phone- and email-based technical support as part of the purchase price for the first year. After the first year, customers can purchase assistance renewal at an additional cost. Customers can also purchase 24/7 support and other specialized options as well. VASCO also offers a large support area available to all customers via its website. This area includes product downloads, technical documentation, a knowledge base and a few other resources.

At a price just shy of $200 for the virtual appliance, we find this solution to be a good value for the money. The aXsGUARD Gatekeeper provides a large amount of configurable security and remote access features that are included, but some are also licensed per user as well, so that price can easily go up based on type of functionality.
WatchGuard XTM 545

The XTM 545 from WatchGuard provides an excellent mix of best-of-breed functions and an easy-to-manage platform for robust perimeter security. WatchGuard takes an interesting approach to the perimeter security problem. This product leverages solid protection from industry leaders across the various security categories, including Websense for web filtering, AVG for gateway anti-virus, CommTouch for spam protection, and Trend Micro for intrusion prevention. This combination of vendors ensures full-scale gateway protection from today’s threats.

Initial setup was straightforward and only took a few minutes. The initial setup consisted of connecting to the appliance via a web browser and running through a short setup wizard, which helped us set network and licensing settings. After the setup wizard was complete, we were able to access the web-based administration interface. Overall, we found the management interface to be easy to navigate and to include intuitive configuration menus. The navigation structure was also well-organized and we found it easy to move around throughout the interface. We also found the appliance features and functions easy to manage and the device was active with just a few clicks of the mouse.

Beyond the best-of-breed security features included in the XTM appliance, WatchGuard has also included its new Dimension platform. This provides a comprehensive suite of visibility and reporting tools that allow for easy analysis of possible threats or security issues. This functionality is composed of a combination of dashboard views that include various threat assessment maps and visuals of data to quickly identify problems and deploy security policies. We found that the combination of these solid reporting and analysis tools and a highly configurable policy engine make this appliance an excellent contender for almost any environments.

The WatchGuard quick-start guide is just that: quick and to the point. However, small, it quickly takes users through items included in the box. The WatchGuard website provides a robust admin guide. The web guide is well laid out – from the introduction to the XTM product to data loss prevention features. The admin guide uses a step-by-step method with screen shots to assist the user during configuration. For further assistance, along with the admin guide, the WatchGuard website includes configuration examples, FAQ, user forums, video tutorials and a knowledge base.

WatchGuard offers three support levels: Plus is basic no-cost assistance that includes a one-year security bundle, phone and web support, software updates, new feature releases, advanced hardware replacement, customer portal access and the user forum. The gold and platinum levels are fee based and include priority upgrades, four-hour hardware replacement and remote installation.

At a price just over $8,000 for the appliance fully loaded with a year subscription of security services, we find the WatchGuard XTM to be an excellent value for the money for pretty much any environment. This appliance offers an affordable mix of solid security features that are easy to manage, along with a robust reporting and analysis platform.

SOMETHING NEW

Each quarter, Technology Editor Peter Stephenson and his team at the SC Lab address emerging technologies and markets.

The purpose is to look at segments in the information assurance space that represent new technologies, needs and capabilities. In those emerging areas there always are new entries and old pros that want to expand into the space.

We will be looking at both – and bringing you the companies and products that we believe will shape the future.

Emerging products: Virtual system security

Progress is far more rapid in the virtual realm than it ever was in the physical, says Technology Editor Peter Stephenson.

This month we take a look at some interesting approaches to security for virtual environments. No two of the companies and products we looked at did this important type of security the same way.

One of the interesting aspects of virtual systems security is that it looks a lot like security in the physical data center back in the day. Now we are entering the era of the software data center and it almost seems as if we are going back to square one. That said, progress is far more rapid in the virtual than it ever was in the physical. An example of that is this and next month, we are examining UTM and SIEMs.

For a long time it appeared that these two product types would converge into a single hybrid. For the most part, that hasn’t happened yet, despite many years of trying.

However, in the virtual realm, things move a lot faster – even though they sometimes seem to start back at the beginning. What I mean by that is that in the virtual world, we still tend to see point solutions to point problems. For example, one of our products this month addresses malware. Another addresses the management plane, while another deals with compliance monitoring and enforcement. Amazingly, few products for security in the virtual use the cloud as a security paradigm. One would think that cloud services would be a natural environment for protecting software-defined data centers since the technology behind the cloud is virtualization.

We are beginning to see virtual security providers take this approach, and the pace certainly is accelerating. Another area where we are starting to see some movement is in light agent/agentless deployments. These behave in the virtual much the same way similar deployments in the physical behave. They offload most of the processing to a virtual appliance in the software-defined data center, similar to the way a gateway operates in the physical data center. The agent, if there is one, sits on a virtual machine and communicates with the virtual appliance. Then the appliance does the heavy lifting, reducing the performance load on the virtual machine.

The products that we tested this month are a good cross-section of the types of offerings that we see in the virtual security marketplace. That takes a bit of explaining. There really are two virtual security product types. One provides security to the enterprise virtually (that usually means that it is cloud-based), while the other provides security for virtual systems. It is the latter that we are interested in this month. There are a couple of corollary issues.

First, we need to consider the security of individual virtual machines. That is a combination of security and isolation. Especially in public cloud environments where multiple organizations share the same virtual resources they both can prove challenging. It is not desirable for one organization to have access to the other organization’s virtual environment – for obvious security and privacy reasons.

The other area of concern is the hypervisor. Compromising the hypervisor potentially compromises the rest of the virtual data center.

Today’s products for securing virtual data centers are beginning to address both of these interrelated requirements. As usual, though, it is a game of leapfrog with the bad guys.

Further, in 2012, virtualization bloggers were pointing out that there were no credible hypervisor attacks. Well, maybe there were, but at least there were no direct hypervisor attacks. However, way back in 2009, Gartner was telling us that hypervisor attacks were “inevitable.” The truth is that today, in 2014, hypervisor attacks are a reality. In fact, the CVE listing shows 44 of them and some go back as far as 2007. Those old attacks were pretty specialized, of course – one addressed the virtualization in the Xbox, for example – but hackers were thinking about how to exploit those vulnerabilities even then.

With all of that in mind, let’s have a look at some of the more interesting products for securing your virtual environment.
EMERGING PRODUCTS | VIRTUAL SOLUTIONS

Bitdefender GravityZone

Take a security server in your virtual environment, add tools on each of the virtual servers you want to protect, throw in a control center in the cloud and you have what you need to protect against malware in the virtual world. While you’re at it, never mind what virtual environment/hypervisor you’re running, from VMware to Amazon Web Services (AWS), GravityZone has you covered. GravityZone is a hypervisor-agnostic security system that manages all of the types of devices on your enterprise so that malware is far less a worry than with just about any other approach. It's easy to deploy, transparent to users and is about as dependable as it can get. It is a neat solution to a messy problem. That problem – threats borne by malware – is messy for a lot of reasons. The obvious is that malware is messy. But not quite as obvious is that anti-malware can be equally messy in a virtual environment. First, updates and agents are needed. In a large virtual environment, that is a lot going on and it’s going on at the expense of the performance of the environment. What is needed to fix that is an agentless or lightweight agent approach and a server that sits on the hypervisor so it can get to everything on the system easily. That describes GravityZone well. The GravityZone control center sits on the hypervisor of your virtual data center. It communicates with the Bitdefender cloud and from the cloud gets its updates, which it then applies to its scans. Only the single scan engine does the work. This is prefer- able to the AV storms that can be caused by thousands of virtual machines performing decentralized scans simultaneously. The impact on the performance of the virtual data center is far less with GravityZone's centralized approach.

AT A GLANCE
Product GravityZone
Company Bitdefender
http://enterprise.bitdefender.com
Price $1,327 per year for 10 virtual servers.
What it does Hypervisor-agnostic security for virtual endpoints running on Citrix, VMware, Microsoft, Oracle and RedHat platforms.
What we liked Hypervisor agnostic.

Catbird 6.0

One area of difficulty in virtual data centers is compliance monitoring. This is such a big driver that just about every security vendor claims its product or cloud service provides it. The fact is that “compliance” has become such an overused hypeword that it almost has no meaning anymore. Until, that is, you come across a product like Catbird 6.0. Catbird has a high-level view of everything in the virtual enterprise that must be monitored and reported in order to meet regulatory requirements. That perspective is exactly what managers and auditors need to appreciate the status of the system both for good security management and reporting. The knowledge that Catbird 6.0 provides empowers the comprehensive security management of big virtual data centers. The paradigm used by Catbird is the trust zone. This is an old, tried-and-true security concept and – with its obvious complexity – quite appropriate in the virtual world. Trust zones in Catbird 6.0 operate similarly to organizational units (OUs) in Active Directory. When a new asset is added to the enterprise, it goes into the appropriate trust zone. At that point, appropriate policies are applied. Regulatory requirements are mapped directly to the policy so there is a direct correlation between the regulatory requirements and the actual configuration of the asset. Specific compliance areas cover the bases well for all regulatory requirements, making this product a solid provider of critical information to managers, auditors and system administrators alike. Oh, and one of the best things about this product? It doesn’t just report on policy – it actually enforces it. That makes Catbird 6.0 a sort of one-stop compliance management shop.

AT A GLANCE
Product Catbird 6.0
Company Catbird	
catbird.com
Price $1,400 per socket per year.
What it does Compliance automation.
What we liked Automated and continuous policy enforcement and compliance monitoring; fast understanding for administrators of asset status through innovative visualizations.

5nine Cloud Security for Hyper-V

There are a lot of virtual applications, especially security applications, that focus on VMware. And there are some that are hypervisor agnostic. But this is the only virtual security product of its type exclusive to Microsoft Hyper-V. For the Hyper-V cloud provider with a multi-tenant environment, Cloud Security enables good granularity for the security administrators of the various tenants. Each tenant can manage its own virtual machines, but the extent of that management is controlled by the enterprise administrator. This layered, role-based security is very “Microsofty,” and administrators in MS shops will feel right at home. The product provides a virtual stateful inspection firewall, an anti-virus system and an intrusion detection system. This functionality is tied together in a compact management console with the familiar MS look and feel. The anti-virus engine – Vipre – also has an extension that 5nine calls Active Protection. That basically is a real-time AV service placed on the virtual machine itself. It provides real-time protection while the other AV engine provides scanning. The scanning is incremental so the AV explosion is kept to the minimum. The IDS is based on Snort and new rules take only a couple of clicks to create. The firewall is a filtering extension to the virtual switch and operates in kernel mode. Because this product is tightly coupled to Hyper-V, there is a lot of functionality that results. For example, there is a plugin for MS VMCENTER that allows the security administrator to manage from that.

AT A GLANCE
Product 5nine Cloud Security for Hyper-V
Company 5nine Software
5nine.com
Price $499 per two CPU per year.
What it does Provides security in a virtual environment for Hyper-V systems.
What we liked Security tightly coupled to Microsoft Hyper-V.

HyTrust CloudControl

This is a security automation product for use in a VMware environment. It’s designed to manage security in a virtual environment by addressing the issue of concentration of risk inherent in the software-defined data center. The idea of concentration of risk is an interesting one that, perhaps, is not quite as obvious as it should be. In a physical data center there are many – sometimes a profusion of – physical servers. There may be multiple administrators dedicated to specific systems and, generally, everything is spread out so that a catastrophic failure or compromise is less likely since data and servers are somewhat decentralized. Compare that with a virtual data center, which is much smaller physically, and administrators may have unfettered (and unmonitored) access across the entire system. That is where the notion of concentration of risk comes in. That which is easy to access is easy to compromise. Add the possibility for a public cloud where your data is, essentially, outside your direct control, and you have a compact target for attack. So a solution to that challenge needs to be built from the ground up to address both the environment and the threats. That is exactly what HyTrust CloudControl does. CloudControl supports strong authentication, role-based access control, role of four eyes (two-person) enforcement, policy enforcement, root password auditing, and infrastructure hardening. It can integrate with Intel’s TXT system as well. Also, CloudControl is an excellent security administration tool from the perspectives of compliance and analysis. The menus and drill-downs are lucid and practical, and the tight integration with VMware and Active Directory adds to the product’s versatility and power.

AT A GLANCE
Product CloudControl
Company HyTrust	
http://hytrust.com/
Price Enterprise pricing starts at $61,750 for a single data center site with 20 ESXi CPU sockets; a free community edition for up to three hosts is also available.
What it does Cloud security automation mitigates the concentration of risk caused by virtualization.
What we liked Protection of the management infrastructure internally.
EMERGING PRODUCTS | VIRTUAL SOLUTIONS

Intigua 2.6

This is one of those why-didn’t-I-think-of-that tools that is deceptively easy to think about and use, but really, under the hood, has lots of moving parts.

The software-defined data center is a moving target. And, because it is easy to change up a virtual environment, we have no qualms about doing it frequently when the need arises. The constraints that usually slow us down in the physical world – e.g., cost, space, performance, power and network requirements – don’t really exist in the virtual world. So, if we need another server, 30 minutes later it’s up, provisioned and ready for production. This flexibility generates nearly endless management headaches.

Those headaches are exactly what Intigua was forged to alleviate. It takes the complicated and makes it manageable. An easy way to think about what this product does is to think of it as a management layer that addresses the entire virtual environment: compute, storage and network. As a management layer, it addresses all of the issues that must be addressed in a virtual environment: configuration, security, backup and various types of monitoring. The pleasing thing about that is that each resource – or server – is addressed in the unique manner that it needs to be.

So if you are running a particular database management system as the platform for your organized data, the requirements of that database management system are addressed in the manner that they need to be addressed. If there are multiple iterations of that DBMS in your virtual enterprise, the agent is deployed once. That makes this system extremely scalable and, in fact, its most friendly environment is the very large virtual enterprise.

PrivateCore vCage

Trust no one. It’s not just an X-Files slogan, it’s the only way to assure a computing environment. It is the basis for the notion of trusted computing. When we look at major breaches where the adversary has used techniques such as memory scraping, we realize that any bit of the computing footprint that is left unprotected – no matter how small – offers a vector for compromise. vCage is exactly what it sounds like it is: a virtual cage around a computing asset.

Today, we are increasingly accepting that it is a high probability that our computing infrastructure already has been compromised. Malware introduced by phishing or drive-by attacks may sit dormant for extended periods in our enterprise before it starts harvesting sensitive information. Much of that malware is zero-day and, as long as it keeps quiet, is not picked up by our scanners. When it activates, though, it’s likely too late.

vCage uses the trusted computing notion of attestation. This is tested proof that an asset is clean and protected. Typically, data is encrypted in motion and at rest. But it isn’t encrypted when it is executing – in memory. One of the things that is exposed in memory is the encryption key. If that is extracted, the entire system is compromised. vCage protects data everywhere in the computing platform.

The vCage host is packaged as a stateless live image Linux KVM on a RAM disk – boot from it and attest it with the management server. Nothing outside the CPU is in clear text. The vCage manages the entire computing infrastructure, including memory.

Digital forensic incident response in a box

My regular readers know that I love forensics and I love innovation. Give me both in a single product and you have my attention.

With its new CIRT (Cyber Intelligence and Response Technology), AccessData Group has knocked one out of the ballpark. The framework contains everything needed to perform digital forensic incident response (DFIR). This is a full lifecycle – from detecting to analyzing to remediating – and it’s all in a single package.

If we stop and think about the forensic process, we see that there are some key aspects from a DFIR perspective. First, we want to know that an incident is occurring/has occurred. Second, we want to know the nature of the incident. Third, we want to perform detailed analysis, even if our environment is thousands or tens of thousands of computers. And finally, having found the root cause, we want to clean up the network and get on with business. And, we want to do all of that with minimal disruption to our users.

Beginning with detection, CIRT integrates with a SIEM. There is a lot happening on the network and the SIEM is the device most likely to see it all. We also get removable media monitoring and analysis in the middle decryption of SSL data streams. Once we know that something is going on, we need to figure out what it is. That’s where the network- and host-based packet capture and IOC’s (indicators of compromise) come into the picture.

This all is bolstered by ongoing threats and indicators of compromise (IOC) feeds to keep the detection piece current. Finally, CIRT remediates problems automatically and saves anything needed saving for further analysis. A user has detected the incident, analyzed it and remediated damage – all with a single suite of tools operating in a single pane of glass.

Visualization is solid. This is a critical issue when there is so much data. Like most similar systems, hosts on the network report back using data collected by agents. These can be persistent or volatile (dissolvable), and the persistent agents do the analysis locally, sending results only back to the central control point. This lessens network impact significantly.

An important aspect of CIRT is project management. The project is the paradigm that CIRT uses, and setting up a project is straightforward. There are places in the project definition forms to establish who is in each of many roles and project flows, including such functions as legal and outside consultants, as well as all of those other functions that one would expect.

Overall, I have not seen a more complete approach to managing security from the forensic perspective. Indeed, this is the first I’ve seen that really addresses that – or responds to cyber incidents, especially in large environments, a milieu for which this is very well suited. If one really wants to integrate security management and digital forensic response in a single system that can help address compliance and the other issues that devolve around information security, this is not only your best choice, today it is your only choice.

– Peter Stephenson, technology editor

FIRST LOOK

Digital forensic incident response in a box

Price: $300 per server per year.

What it does Virtual management for virtual environments.

What we liked Simplicity of managing complex virtual computing environments with constantly changing requirements.

Intigua 2.6

Company: Intigua

Price: $330 per server per year.

What it does Virtual management for virtual environments.

What we liked Simplicity of managing complex virtual computing environments with constantly changing requirements.

PrivateCore vCage

Company: PrivateCore

Price: $1,000/month for up to 20 servers for vCage Manager.

What it does Secures servers with software-based attestation, full-memory encryption and OS hardening, providing a foundation for trusted computing.

What we liked Instantiates the concept that a system likely is already compromised into a trusted computing model that includes the entire computing infrastructure, including memory.

CIRT (Cyber Intelligence and Response Technology)

Company: AccessData Group

Price: Tiered per-node pricing starts at $65/node, plus $50,000 for network forensics functionality. Annual support is 20 percent of base price.

What it does: Digital forensic incident response under a single pane of glass with hooks into compliance, eDiscovery, project management and remediation.

What we liked: This is the ultimate tool available today for forensic management of all of the aspects of information security.

What we didn’t like: There is nothing here not to like.
MARCH
> SANS Cyber Guardian 2014
March 3-8
The fourth annual SANS Cyber Guardian event will take place in Baltimore this time around featuring three baseline courses. Venue: Baltimore
Contact: sans.org/info/143297

> DFIRCON 2014
March 5-10
This digital forensics and incident response (DFIR)-focused event has a number of training courses and expert speakers. Venue: Monterey, Calif.
Contact: sans.org/info/143302

> HCS Summit - Orlando 2014
March 12-18
Thirteenth annual gathering will be held in Lake Buena Vista, Fla., on March 17-18, with in-depth, hands-on pre-technical courses on March 12-16. Venue: Lake Buena Vista, Fla.
Contact: sans.org/info/143307

> SC Congress London
March 20
Mobile safeguards, insider threats, privacy, cloud security, UK cyber criminals…This free, live event is for IT professionals concerned with all aspects of data security. Following up on the success of SC Congress events in New York, Chicago, and Toronto, we are expanding to the UK with expert guidance, practical solutions and timely info to help organizations both big and small, commercial and government, combat today’s cyber criminals. Venue: London
Contact: congress.scmagazine.com/page.cfm/link=94

> SecureWorld 2014
March 25-26
Boston SecureWorld 2014 will offer two days of presentations by industry leaders from around the world. Highlights of this year’s event include keynotes, more than 30 exhibitors on the show floor and access to interactive show app. Venue: Boston
Contact: secureworldexpo.com

> Black Hat Asia 2014
March 25-28
Black Hat is returning to the Far East for the first time since 2008. Connecting the world’s leading information security professionals and practitioners, this event features two days of trainings on March 25 and 26, followed by two days of briefings and workshops on March 27 and 28. Venue: Singapore
Contact: blackhat.com/asia-14/

> AWS Summit 2014
March 26
The annual Amazon Web Services gathering is a free, one-day event where attendees can hear about the latest AWS services, learn best practices from AWS engineers, gain new skills in hands-on labs, and get questions answered. Keynote sessions feature Andy Jassy, SVP, Amazon Web Services and leaders from start-ups and enterprises. Venue: San Francisco
Contact: aws.amazon.com/aws-summit-2014/san-francisco/

> Apps World North America
March 25-28
Showcasing 16 niche workshop tracks, covering mobile marketing and advertising, HTML5, mobile payments, and more. New workshops include API strategies and retail workshops. There are free workshops aimed at developers tackling the key challenges of the mobile app industry. Venue: San Francisco
Contact: apps-world.net

APRIL
> SANS Abu Dhabi 2014
April 26-May 1
Taking place in The Hilton International, Abu Dhabi from Saturday April 26th to Thursday May 1st, SANS once again invites information security professionals to take part in six days of training. Venue: Abu Dhabi
Contact: sans.org/info/145915

> InfoSecurity Europe
April 29-May 1
Featuring more than 325 exhibitors, a range of new products and services, a free education program and more than 13,000 unique visitors from every segment of the industry. Venue: London
Contact: infosfer.co.uk

JUNE
> DFIR Summit 2014
June 3-10
The seventh annual Forensics and Incident Response Summit will again be held in the live musical capital of the world. The Summit will focus on high quality and relevant content as well as panel discussions in digital forensics and incident response. Venue: Austin, Texas
Contact: sans.org/info/145920

Events
Seminars

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

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.
A CIO for whom I once worked used to try to convince me that the battle for private data is already lost. His view was that our personal data is already out there in the world and it will just be a matter of time before we all get breached. He was, in a sense, correct. Up to 70 million individuals recently had personally identifiable information stolen in the recent Target data breach.

In July 2012, I wrote about the near-total transition in Western Europe to the chip-based EMV payment system [EMV is an acronym for Europay, MasterCard and Visa, an international standard for inter-operation of integrated circuit cards]. Replacing the existing magnetic stripe card data swipe system still in use in the United States is a security imperative. Too much private data sits without protection in that stripe. As of 2011, 75 percent of cards in Europe were already chipped, and penetration in Canada exceeded 50 percent. I have started to observe some EMV chip-capable payment terminals in retail outlets in the New York City metropolitan area, but not yet been able to make a payment in the U.S. via chip-and-PIN as opposed to swipe the stripe.

Many reports state that one of the factors leading to the Target breach were known insecurities of the magnetic stripe system, combined with a RAM-based point-of-sale terminal virus. Perhaps this is the case, although I wonder as well whether the upstream flow of the data was adequately protected. Certainly, at least some of the data was resident in other company databases. Why then, in light of known vulnerabilities, has the payments industry has about the same eagerness for the upgrade that the nation had for the switch over to metric measurements. Why do I perceive a lack of will?

I have several personal accounts with a major bank that offers EMV chip-and-PIN cards to its customers. One card has the chip because I requested it last year. However, I recently signed up for a promotion with that same bank for another card with a different sponsor. I received the new card in the mail and immediately noticed that there was no EMV chip. This new card is definitely meant for travel, offering a no-foreign-transaction fee benefit. How does this make sense?

Using the U.S.-issued chip-and-PIN card in Europe offered its own surprise. The European terminals seem to have a lax security procedure. Over the course of a recent trip to two different countries, my chip-and-PIN card was accepted without the terminal requesting that I enter the PIN. This too, makes no sense.

Then again, we live in a world where large corporations and government entities store our private data on unencrypted laptops that walk out the door. The common theme here is that in many cases, our profession knows the right solution, or at least a better solution. We must be more effective in the implementation. The public is becoming desensitized into believing that breaches are inevitable and that we must live with them.

This is not the message that we security practitioners want to send.

Dan Srebnick is an executive information security strategist based in the New York City area. He is owner of Technical Merits LLC.

Time for a charge card overhaul

We’ve all been breached, but there are steps we can take to evolve the system, says security strategist Dan Srebnick.

A CIO for whom I once worked used to try to convince me that the battle for private data is already lost. His view was that our personal data is already out there in the world and it will just be a matter of time before we all get breached. He was, in a sense, correct. Up to 70 million individuals recently had personally identifiable information stolen in the recent Target data breach.

In July 2012, I wrote about the near-total transition in Western Europe to the chip-based EMV payment system [EMV is an acronym for Europay, MasterCard and Visa, an international standard for inter-operation of integrated circuit cards]. Replacing the existing magnetic stripe card data swipe system still in use in the United States is a security imperative. Too much private data sits without protection in that stripe. As of 2011, 75 percent of cards in Europe were already chipped, and penetration in Canada exceeded 50 percent. I have started to observe some EMV chip-capable payment terminals in retail outlets in the New York City metropolitan area, but not yet been able to make a payment in the U.S. via chip-and-PIN as opposed to swipe the stripe.

Many reports state that one of the factors leading to the Target breach were known insecurities of the magnetic stripe system, combined with a RAM-based point-of-sale terminal virus. Perhaps this is the case, although I wonder as well whether the upstream flow of the data was adequately protected. Certainly, at least some of the data was resident in other company databases. Why then, in light of known vulnerabilities, has the payments industry has about the same eagerness for the upgrade that the nation had for the switch over to metric measurements. Why do I perceive a lack of will?

I have several personal accounts with a major bank that offers EMV chip-and-PIN cards to its customers. One card has the chip because I requested it last year. However, I recently signed up for a promotion with that same bank for another card with a different sponsor. I received the new card in the mail and immediately noticed that there was no EMV chip. This new card is definitely meant for travel, offering a no-foreign-transaction fee benefit. How does this make sense?

Using the U.S.-issued chip-and-PIN card in Europe offered its own surprise. The European terminals seem to have a lax security procedure. Over the course of a recent trip to two different countries, my chip-and-PIN card was accepted without the terminal requesting that I enter the PIN. This too, makes no sense.

Then again, we live in a world where large corporations and government entities store our private data on unencrypted laptops that walk out the door. The common theme here is that in many cases, our profession knows the right solution, or at least a better solution. We must be more effective in the implementation. The public is becoming desensitized into believing that breaches are inevitable and that we must live with them.

This is not the message that we security practitioners want to send.

Dan Srebnick is an executive information security strategist based in the New York City area. He is owner of Technical Merits LLC.
INTRODUCING
CONTINUOUS MONITORING
FOR THE PERIMETER
A New Paradigm for Security

LEARN MORE AT QUALYS.COM/CONTINUOUS

The QualysGuard Cloud Platform and integrated suite of solutions helps businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

© 2014 Qualys, Inc. All rights reserved.