MAKING THE GRADE

Kathleen Styles is heading up a U.S. Dept. of Education effort to improve student privacy

Perfecting PIPEDA
Canadian’s privacy law is 10 years old this year, and the government is overhauling it

Cutting the red tape
Concerns ran the gamut at the SC Magazine Government Security Roundtable
REGULARS

4 Editorial The art of this war is changing

8 Threat report Gang members who placed skimming devices on ATM machines were arraigned

10 Threat stats The number of phishing attacks increased by seven percent

12 Update DigiNotar operated with a lack of basic security, resulting in the issuing of counterfeit certificates

13 Debate Operation Shady RAT, a cyberespionage offensive chronicled by McAfee, is a boondoggle

14 Two minutes on… The flawed certificate authority system

15 Skills in demand Subject matter experts are a hot property

16 From the CISO's desk Taking stock of PCI five years on, by Eduardo Perez, Visa

18 Opinion Cloud management practices, by Michael Ginsberg, CEO, Echoworx

20 Letters From the online mailbox

50 Last word Cloud: A risk/reward proposition, by Siobhan Byron, president of Forsythe Technology Canada

FEATURES

22 Making the grade Kathleen Styles is heading up a U.S. Department of Education effort to improve student privacy.

27 Keeping up the guard Mega-payment breaches may be quieting, but protecting cardholder data remains a challenge.

C1 Perfecting PIPEDA Canada’s privacy law is 10 years old this year, and the government is overhauling it. Do the changes go far enough?

30 Beyond theory Mobile malware, often distributed through applications, is increasing in scope and sophistication.

34 Cutting the red tape As federal and state agencies are forced to do more with less, concerns continue to mount, we learned during an SC Magazine roundtable.

PRODUCT REVIEWS

37 Product section It’s all about the data, says Peter Stephenson, our technology editor. And here are tools and strategies to mitigate the threat of company asset theft.

38 Group Test 1: Encryption In the past, encryption tools often slowed down operations and were difficult to implement, but we’ve come a long way.

45 Group Test 2: Data leakage prevention Insiders and outsiders alike are motivated to remove sensitive data from its protected home on the enterprise network, but there are defenses available to thwart them.

Our solutions are the convergence of security and compliance.

As a recognized global leader in data security and compliance solutions, we’re helping small and large organizations worldwide protect sensitive data in all forms, in all environments. Trustwave’s on-demand technology is delivered via our revolutionary TrustKeeper® customer portal to simplify the monumental challenge of achieving security and compliance goals. Our integrated solutions leverage the research and expertise of our elite security team, Trustwave SpiderLabs®, to deliver unprecedented intelligence to your fingertips.

To see Trustwave’s full suite of security and compliance solutions, visit www.trustwave.com/meet.

Kathleen Styles, U.S. Dept. of Education P22

Cryptzone P41

Fidelis Security Systems P48

Security, meet Compliance.
Editorial

The art of this war is changing

Just this week, I was talking to one of our editorial advisory board members, who said that lately he found himself jumping on airplanes more than working in the home office. Apparently, seemingly endless trips to his company’s various locations in the Asia-Pacific region are major priorities for him and his team to ensure that IT security operations are buttoned up across all their offices.

To be more specific, because the global threat landscape is changing at a clip many of us in this industry have never witnessed before, his international firm is fine-tuning its security and risk management plans and controls. Beyond just enlisting tried-and-true risk management best practices, he and his bosses want to see the organization continue to rely on people, processes and technologies to establish more adaptive controls and systems to strengthen overall network resiliency.

This means that relying on purchased tools isn’t going to cut it. The way he sees it, IT security plans and policies, processes, technological deployments and user training now have to stand up to any number of attack scenarios.

Similar thoughts were voiced by quite a few information security leaders with whom I’ve spoken recently. Being prepared, yet nimble, is key to any well-designed mission. The idea of understanding the context of what’s happening to the business now, why and how it’s happening and, then, divining what could happen in the future is not a new philosophy with which to underpin one’s IT security blueprint.

Being adaptive to and aware of particular situations is an age-old concept that even Sun Tzu hit upon in his *The Art of War*. It’s a philosophy that is intertwined throughout this still well-referenced tome, but there are specific quotes that more clearly showcase the idea, such as: “By altering his arrangement and changing his plans, the skillful general keeps the enemy without definite knowledge.”

Armed with this knowledge, we at *SC Magazine* are looking forward to our SC Congress New York conference and expo on Nov. 16 in Manhattan. During the event, industry leaders will share their expertise on how to deal with today’s fast-evolving threats and what sorts of adaptations can be made to security plans to ensure preparedness for sophisticated attacks against your infrastructures.

Sun Tzu also said, “Whoever is the first in the field and awaits the coming of the enemy will be fresh for the fight… the clever combatant imposes his will on the enemy.” SC Congress New York can definitely help here. Hope to see you there!

Ilenna Armstrong is editor-in-chief of *SC Magazine*.

Being prepared, yet nimble, is key to a well-designed mission.”
WHAT IS SCWC 24/7?
SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

ON DEMAND
Data security
Many leading CSOs at various conferences this year touted the need for organizations to have their security controls follow and protect their most important data assets, rather than the network. So, just how is this best achieved and what policies, plans and technologies can help? Also, how are data breach notification laws helping to drive the evolution of this philosophy among organizations of all sizes?

Mobile security
To safeguard handheld devices used by business executives is a constant trial—one that rarely is satisfactorily remedied. To safeguard handheld devices used by business executives is a constant trial—one that rarely is satisfactorily remedied. But companies must find a way to manage and protect these endpoints. We offer some solutions.

For MORE INFO
For information on SCWC 24/7 events, please visit natasha.mulla@haymarketmedia.com.

SC WORLD CONGRESS
Oct. 23
www.scmagazineus.com/scwc247
NATASHA MULLA, NATIONAL ACCOUNT MANAGER - EVENT SALES
(646) 638-6017 natasha.mulla@haymarketmedia.com

WHO’S WHO AT SC MAGAZINE
EDITOR-IN-CHIEF Ilvana Armstrong
ilvana.armstrong@haymarketmedia.com
EXECUTIVE DIRECTOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
SENIOR REPORTER Angela Mozarciak
angela.mozarciak@haymarketmedia.com
TECHNOLOGY EDITOR Peter Steffenson
peter.steffenson@haymarketmedia.com
SC LAB MANAGER Mike Stephenson
mike.stephenson@haymarketmedia.com
DIRECTOR OF SC LAB OPERATIONS John Albian
john.albian@haymarketmedia.com
SC LAB EDITORIAL ASSISTANT Judy Traub
judy.traub@haymarketmedia.com
PROGRAM DIRECTOR, SC CONGRESS Eric Green
eric.green@haymarketmedia.com
CONTRIBUTORS
Stephen Lawton, Dale Raskin, Jim Romeo
DESIGN AND PRODUCTION
Art Director Brian Jackson
brian.jackson@haymarketmedia.com
VP of Production & Manufacturing Louis Morin
louis.morin@haymarketmedia.com
Senior Print and Digital Controller Kris Klar
kris.klar@haymarketmedia.com
EVENTS
SENIOR EVENTS MANAGER Natasha Mulla
natasha.mulla@haymarketmedia.com
SENIOR EVENTS COORDINATOR Anthony Curry
anthony.curry@haymarketmedia.com
EVENTS ASSISTANT Maggie Keller
maggie.keller@haymarketmedia.com
U.S. SALES
ADVERTISING DIRECTOR David Shifman
(646) 638-6028 david.shifman@haymarketmedia.com
WEST COAST BUSINESS MANAGER Matt McGinley
(646) 638-6017 matt.mcginley@haymarketmedia.com
NATIONAL ACCOUNT MANAGER - EVENT SALES Mike Yuce
(646) 638-6020 mike.yuce@haymarketmedia.com
UK ADVERTISEMENT DIRECTOR Mark Gordon
44 208 267 4672 mark.gordon@haymarketmedia.com
LICENSE & REPRINTS ACCOUNT EXECUTIVE Malika Toure
(646) 638-6104 malika.toure@haymarketmedia.com
EMAIL LIST RENTAL
EMAIL, SENIOR ACCOUNT MANAGER Frank Coppola, Edith Roman Associates
(845) 731-3832 frank.coppola@promediction.com
CIRCULATION
GROUP CIRCULATION MANAGER Sherry Dore
(646) 638-6003 sherry.dore@haymarketmedia.com
SUBSCRIPTION INQUIRIES
CUSTOMER SERVICE: (800) 558-1703
EMAIL: Haymarket@caribouwest.com
WEB: www.scmagazineus.com
MANAGEMENT
CEO OF HAYMARKET MEDIA Les Mariscal
EXECUTIVE VICE PRESIDENT Tony Keefe

At WGU we respect your time and intelligence, because what you know is more important than time in a classroom. WGU’s ONLINE competency-based approach puts you in control of your academic destiny... and your own security.

Master of Science
Information Security and Assurance
- Incorporates (and includes in the tuition!) 6 security and networking certifications. (Your time to completion will be shorter if you already hold any of these certifications.)
- Certified by the National Security Agency’s IACE program.
- Meets CNSS National Training Standards.
- Scholarships Available.

ONLINE. ACCELERATED. AFFORDABLE. ACCREDITED.

“WGU respected the knowledge and experience I already had, making it possible for me to accelerate my program. The curriculum is rigorous and relevant.”

Western Governors University
TOLL-FREE AT: 1.866.225.5948
OR VISIT OUR WEBSITE AT: www.wgu.edu/scm
Threat Report
Cybercriminal activity across the globe, plus a roundup of security-related news

The Netherlands was the top producer of zombie IP addresses during the past month. Of the countries making up the EMEA, the Netherlands was the top producing country. For the other regions, the top producers were Brazil in South America, the United States in North America and India in the Asia-Pacific region.

Source: Symantec

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

MEDIUM-LEVEL ACTIVITIES
LOW-LEVEL ACTIVITIES
HIGH-LEVEL ACTIVITIES

IDAHO — The state attorney general issued a consumer alert warning of widespread phishing scams targeting residents. Multiple individuals reported receiving phone calls and text messages claiming to come from their banks. The text falsely claimed the recipient’s card was compromised and asked for personal data to reactivate it.

MANTECA, CALIF. — Two accused members of an Armenian gang that steals money by placing skimming devices on cash machines were arraigned here. They face numerous felony counts after being caught on surveillance video attaching the devices to an ATM.

MILWAUKEE — The confidential information of 75,000 University of Wisconsin-Milwaukee students and employees is at risk after a server was discovered to be infected with malware. School officials do not believe any data was stolen and said the attackers may have instead been aiming to steal research information.

NEW HAVEN, CONN. — A Google search could have yielded the personal information of 43,000 students, faculty, staff and alumni affiliated with Yale University in 1999. The data was stored on a file-transfer protocol (FTP) server, which became searchable last September when Google began indexing such servers.

SAUDI ARABIA — A company contracted to fill cash machines in Riyadh may be responsible for some users receiving less money than they expected. Workers may be cheating customers by placing lower-denomination bills in the slots for higher-denomination currency.

SYRIA — Pro-revolution citizens are being targeted in a new scam in which a fake Facebook page seeks to steal their login credentials. The link to the bogus page spread through Twitter and was disguised as a link to a “fascinating video clip.” The regime’s militias are believed to be behind the attack.

PAKISTAN — The nation will begin enforcing a ban on virtual private networks (VPN). The Pakistan Telecommunications Authority delivered a memo to internet service providers, asking them to block encrypted VPN connections — unless permission is obtained — out of concern terrorists are trying to hide their communications.

CZECH REPUBLIC — The central European nation issued its cybersecurity strategy through 2015. The 10-page document focuses on three themes: education and training, partnerships with technology vendors and the private sector, and global collaboration. The strategy’s main goal is to protect the nation’s critical infrastructure.

HONG KONG — The news website belonging to the country’s holding company for the Hong Kong stock exchange sustained a distributed denial-of-service attack, leading to a temporary stoppage of trading on seven listed companies. The firms had just released price-sensitive information on the site. Authorities are unsure of the hackers’ motivation.

MILWAUKEE — The confidential information of 75,000 University of Wisconsin-Milwaukee students and employees is at risk after a server was discovered to be infected with malware. School officials do not believe any data was stolen and said the attackers may have instead been aiming to steal research information.

NEW HAVEN, CONN. — A Google search could have yielded the personal information of 43,000 students, faculty, staff and alumni affiliated with Yale University in 1999. The data was stored on a file-transfer protocol (FTP) server, which became searchable last September when Google began indexing such servers.

SAUDI ARABIA — A company contracted to fill cash machines in Riyadh may be responsible for some users receiving less money than they expected. Workers may be cheating customers by placing lower-denomination bills in the slots for higher-denomination currency.

SYRIA — Pro-revolution citizens are being targeted in a new scam in which a fake Facebook page seeks to steal their login credentials. The link to the bogus page spread through Twitter and was disguised as a link to a “fascinating video clip.” The regime’s militias are believed to be behind the attack.

PAKISTAN — The nation will begin enforcing a ban on virtual private networks (VPN). The Pakistan Telecommunications Authority delivered a memo to internet service providers, asking them to block encrypted VPN connections — unless permission is obtained — out of concern terrorists are trying to hide their communications.
There were 840,322 malware attacks in the United States last month.

### Top 10 malicious programs

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Trojan.JS.Popupper.aw</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Hoax.HTML.BroUpdate.af</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Trojan.HTML.Iframe.dl</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Trojan.JS.Redirector.qb</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Trojan.JS.Redirector.py</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Adware.Win32.FunWeb.jp</td>
<td>-4</td>
</tr>
<tr>
<td>7</td>
<td>Trojan-Downloader.JS.Expact.au</td>
<td>73</td>
</tr>
<tr>
<td>8</td>
<td>Hoax.Win32.Screensaver.b</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>Exploit.Java.CVE-2010-4452.a</td>
<td>28</td>
</tr>
<tr>
<td>10</td>
<td>Hoax.HTML.FraudLoad.a</td>
<td>-2</td>
</tr>
</tbody>
</table>

Source: Kaspersky Lab

Kaspersky Lab’s analysts detected 35 malicious programs targeting the Bitcoin digital currency system. Realizing that their potential earnings largely depend on the number of computers they have access to, the cybercriminals have moved from stealing Bitcoin wallets to using Twitter and P2P network-based botnets.

### Malware Vertical encounter rate

<table>
<thead>
<tr>
<th>Malware</th>
<th>Vertical encounter rate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>0000 Food &amp; beverage</strong></td>
<td>200%</td>
</tr>
<tr>
<td><strong>135% Education</strong></td>
<td></td>
</tr>
<tr>
<td><strong>130% Retail &amp; wholesale</strong></td>
<td></td>
</tr>
<tr>
<td><strong>125% IT &amp; telecom</strong></td>
<td></td>
</tr>
<tr>
<td><strong>90% Banking &amp; finance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>90% Government</strong></td>
<td></td>
</tr>
<tr>
<td><strong>70% Health care</strong></td>
<td></td>
</tr>
</tbody>
</table>

Source: Cisco ScanSafe

### Phishing

A seven percent increase

### Top breaches of the month

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lincoln Financial Group (New York)</td>
<td>A programming error caused PII of current and former retirement plan enrollees to be accessible to unauthorized plan administrators.</td>
<td>91,763</td>
</tr>
<tr>
<td>Univ. of Wisconsin (Milwaukee)</td>
<td>University technology staff learned that unauthorized individuals installed viruses on a campus server.</td>
<td>79,000</td>
</tr>
<tr>
<td>Yale University (New Haven, Conn.)</td>
<td>A computer file containing data of former faculty, staff and students was accidentally made accessible online.</td>
<td>43,000</td>
</tr>
</tbody>
</table>

Source: RSA Anti-Fraud Command Center

### Zombie IPs Global distribution

```
Zombie IPs Global distribution

Top countries: Brazil 8.4%, India 13.1%, Other Asia 18.8%, Other Europe 13.1%, Russia 6.0%
```

### Spam rate Compared to global email

```
Spam rate Compared to global email

08/08/11 08/09/11 08/10/11 08/11/11 08/12/11 08/13/11

Top 5 attacks used by U.S. hackers
1. Botty bot 31.28%
2. Zeus trojan 2.96%
3. Sinowal trojan 2.30%
4. TDSS Downloader trojan 1.97%
5. Downloader trojan 1.54%

Top 5 attacks used by foreign hackers
1. Botty bot 31.28%
2. Zeus trojan 2.96%
3. Sinowal trojan 2.30%
4. TDSS Downloader trojan 1.97%
5. Downloader trojan 1.54%

Top 5 attacks used by foreign hackers
1. Botty bot 31.28%
2. Zeus trojan 2.96%
3. Sinowal trojan 2.30%
4. TDSS Downloader trojan 1.97%
5. Downloader trojan 1.54%

Top 10 spyware threats
1. Backdoor.Win32.Cycbot.cfg (v): trojan 1.35%
2. Backdoor.Win32.Cycbot.cfg (v): backdoor 0.30%
3. Yontoo (v): adware (general) 1.47%
4. Fraud Tool.Win32.FakeRean: rogue AV 1.35%
5. Trojan.Win32.Adware: adware (general) 1.32%
6. INF.Autorun (v): trojan 1.29%
7. Trojan.Win32.Jpgiframe (v): trojan 1.05%
8. Pinball Corporation (v): adware (general) 1.04%
9. Trojan.JS.Redirector.cd (v): adware (general) 1.00%
10. TDSS Dowloader trojan 0.97%

The majority of these threats propagate through stealth installations or social engineering. (v) is a detection that has come directly from VIPRE.
```

### Malware Vertical encounter rate

```
200% Food & beverage
135% Education
130% Retail & wholesale
125% IT & telecom
90% Banking & finance
90% Government
70% Health care
```
Update

NEWS BRIEFS

The government has launched a consumer IT security awareness campaign in a bid to help Canadians protect themselves. The campaign, running October as Cybersecurity Awareness Month, features ad promos and an associated website. The website is designed to provide Canadians with a single portal for security information.

Get Cyber Safe is part of the cybersecurity strategy launched by the government, but has taken a while to set up after being unveiled a year ago. The website covers basic consumer awareness tips, such as regularly updating passwords and anti-virus software, using a secure wireless network, and learning how to recognize online scams.

Parliament reintroduced controversial copyright measures in a new bill that will legally enable companies to stop Canadians from copying digital products. Bill C-11, reintroduced at the end of September, resurrects many of the measures originally found in Bill C-32, which died on the ballot after the previous Parliament ended prematurely. C-11 maintains legal protections for digital locks. If a manufacturer chooses to impose its own copying policies by encoding a product using digital rights management technology, Canadians are legally forbidden to circumvent it.

The bill will go a long way toward placating powerful trading partners, such as the United States, which has kept Canada on the priority watch list in its “Special 301” report since 2009. The report focuses on trade barriers to U.S. interests, arising from intellectual property laws in partner countries. The U.S. government’s big sticking point is Canada’s failure to implement World Intellec-
tual Property Organization (WIPO) copyright policy in law.

Michael Geist. Canada research chair in internet and e-commerce law at the University of Ottawa, said that the bill is designed in part to appease the U.S. Canada also took other measures to mollify trading partners at the end of September, signing the Anti-Counterfeiting Trade Agreement (ACTA), a jointly developed international standard for anti-counterfeiting measures. However, signing is just the first step. As with the WIPO copyright treaty, Canada still has to ratify ACTA.

Canada isn’t the haven for pirates that the U.S. thinks it is, according to a report from the Business Software Alliance. The BSA showed that Canadians are relatively unlikely to pirate software. The research showed that seven percent of Canadians are active pirates, while one in five tend to acquire products illegally.

PRO

Social gap

A recent survey conducted by Websense revealed that IT pros consider themselves ill-equipped for dealing with social media at work. Seventy percent of Canadian respondents to the survey said that employees’ use of social media in the workplace presents a serious security threat to the organization. However, 31 percent of them said that they had the necessary controls in place to mitigate the threat.

CON

There’s the take-home message here that [they] are too big to fail.

~ Christopher Soghoian, privacy researcher, on the lack of enforcement action against certificate authorities that issue counterfeit SSL credentials

THE QUOTE

THE MAGAZINE POLL

What is most valued in a security professional?

- 45.66\% Work experience
- 46.56\% Certification (CISP, etc.)
- 4.58\% Education
- 1.53\% All of the above

THE STATS

68k

hold the CISP certification in 134 countries (as of 7/10)

$93k

median salary for CCNP-Cisco Certified Network Professional

Source: (ISC)²/Global Knowledge

FOR

Debate Operation Shady RAT, a cyberespionage offensive chronicled by McAfee, is a botnet. Arguments as to terminology have always caused heated debate in the anti-virus industry. Alternative/varied meanings can be attached to any term. There isn’t even a single definition of the word “virus.” Yet, analysis of the activities of the malicious programs in Shady RAT allows one to conclude categorically that this, in fact, is a botnet — due to the following: mass distribution of emails containing malicious files; after executing the malicious file contained in an email, the victim’s computer gets infected with a trojan horse loader; the trojan interacts with a remote server via the internet, sending it information and receiving from it automatic commands, for example, to download other malicious programs; the number of computers infected by the trojan at any point in time is more than one; and given access to the control center, a hacker is able to execute any command on an infected computer. Thus, what we have here is a botnet: a network of infected computers interacting with a remote control center.

AGAINST

The Shady RAT advanced persistent threat (APT) is a cyber adversary displaying advanced logistical and operational capabilities for long-term intrusion campaigns. Its goal is to maintain access to victim networks and exfiltrate intellectual property data and information that is advantageous. Botnets are a tool designed for an organization to control hundreds to millions of infected hosts with identical commands. The larger the botnet, the more effective it will be. To achieve a larger size, botnets are created through indiscriminate victim targeting, making them decidedly visible. The APT infrastructure is designed for discrete manipulation that allows the APT to achieve precise goals in each victim it compromises. The Shady RAT report reveals the APT specifically targeted key organizations worldwide. Its objective for each victim is unique. The danger in simplifying the APT as a botnet is that it leads us to ignore the threat that the adversary is much larger, more organized, and better equipped than we assume.

THE MONTH

Morto worm

What is it?

Morto scans the LAN for systems running RDP. Once RDP is found, the worm attempts a dictionary attack on the adminis-
trator account. Upon successful login, the remote hard drive is mounted, and Morto copies itself to the remote PC. Using the Regedit command, the DLL previously copied over is loaded into memory.

How does it work?

Morto scans the LAN for systems running RDP. Once RDP is found, the worm attempts a dictionary attack on the adminis-
trator account. Upon successful login, the remote hard drive is mounted, and Morto copies itself to the remote PC. Using the Regedit command, the DLL previously copied over is loaded into memory.

Should I be worried?

This should be a wake-up call to IT administrators worldwide because the worm exploited weak configurations. Morto was packaged with only 36 guessable passwords, such as “123,” “Admin” and “password.”

How can I prevent it?

Don’t forget about the local administrator ac-
count on your computers. Enhance the same password policies apply to local accounts as they do the domain-level accounts. Disable RDP services if not needed and keep all systems protected with anti-malware software.
The flawed CA system

N
ever mind malware or phishing attacks, the foundational assurance of the internet is in doubt these days, following attacks against certificate authorities (CA) Comodo and DigiNotar.

CAs, or companies that sell the digital SSL certiﬁcates used by websites to validate their identity to visitors, play a pivotal role in what is trust-ed online, said Roel Schouwenburg, senior researcher at Kaspersky Lab.

“When we look at the CA infrastructure, it really is a tangled web of trust,” he said. For starters, when the CA system was invented, the internet was a fraction of its current size, and only a few sites required secure communications.

Fast forward to today, and there are some 650 trusted CAs – a number experts believe is too high. They operate with various levels of security, yet browsers trust them all about the same.

This can lead to bad things happening. In March, Comodo revealed that hackers gained access to its system and fabricated nine certiﬁcates for some top-tier sites. Experts believe the Iranian government carried out the Comodo, and more recent DigiNotar, attacks to spy on private communications.

Critic Moxie Marlinespike, founder of PGP and CTO of Whisper Systems, said the existing CA protocol lacks the ability for users to easily revise which companies they trust.

“Someone made the decision to trust Comodo and we are locked into trusting them forever,” Marlinespike said. Comodo, one of the world’s top ﬁve CAs, certiﬁes somewhere between a quarter and a ﬁfth of the internet. If browser companies revoked trust in Comodo, a large portion of the internet would “break,” Marlinespike said.

Experts agree that the current system is badly broken, but warn there will be no easy ﬁx. Schouwenburg suggested that browser makers perform additional checks on the certiﬁcates provided for domains that are currently being targeted in spying operations.

Marlinespike, meanwhile, released a free add-on for the Firefox web browser called Convergence, which essentially inverts the current CA system, giving more power to users. With the tool, users can take their pick of so-called “trust notaries” to authorize their communications, and then revise their choices at any time.

There are about 30,000 active users of Convergence, but Marlinespike hopes it will become more widespread.

“If the four major browser vendors shipped it with the browser, that would be it, problem solved, end of the CA system in one fell swoop,” he said. – Angela Moscaritolo

531
Number of fake SSL certiﬁcates hackers were able to issue through DigiNotar.
Taking stock of PCI five years on

Eduardo Perez

From the CSO’s desk

Last month marked the five-year anniversary of the PCI Security Standards Council. Looking back now, it is amazing to see how far we have come as a result of the ongoing participation of security professionals like you. An integral part of the PCI community, you have helped steer the process, driving PCI awareness and adoption levels that have led to the overall growth and improvement of payment card security we see today.

At the time of our launch, PCI adoption rates were at levels that matched lack of awareness in the market. Our stakeholders told us, and we recognized the challenge with the multiple ways that merchants had to tackle data security and report their compliance to each of the card brands. We listened and knew there had to be a change in order to increase adoption of PCI standards and improve payment card security.

This required a forum for those using the PCI standards to input their experience and feedback in the development of the guidelines. We had to find an avenue for listening and working with those on the front lines – this would be the driver for change.

To that end, you and the rest of our community have responded in force, pushing the evolution of the PCI rules and playing an instrumental role in producing critical supplemental guidance on topics of great interest and importance to the market – including EMV, point-to-point encryption, wireless, skimming prevention, tokenization – that underscore our commitment to provide what stakeholders ask for.

At Visa, we are encouraged by the collective efforts, we are seeing fewer large-scale card data breaches in the marketplace. And when breaches do occur, entities that have applied the PCI standards are in a better position to mitigate the impact of the compromise.

To drive security forward in the midst of a rapidly evolving payments system, we will have to continue to focus on and listen to where the market is going and what you are telling us.

This means that the standard, our very core, needs to continue to evolve. And the way we do that continues to be through feedback from the community.

This community must continue to be the engine that propels us forward. With the ongoing involvement and input from you and your peers that has brought us this far, together as champions of PCI, we will ensure that in a changing payments environment, the security of cardholder data remains paramount.

Consequently...

As a result, U.S. data breaches in 2004-05 were possible through basic attacks, like SQL injection. But the lack of initial buy-in led to similar breaches in subsequent years.

Consequently...

Visa level-one PCI compliance was tracking at only 12 percent in March 2006, and PCI efforts were considered primarily a U.S. concern, after the recent migration to EMV in Europe.

Reaching out...

The council knew it couldn’t do it alone. We needed our stakeholders’ expertise to succeed. So we established a strong community of more than 600 participating organizations.

Future efforts...

You’ve told us you want more guidance on mobile payments and further exploration of P2PE, cloud, virtual payment cards, and new payment formats and other technologies.

You’ve told us you want more guidance on mobile payments and further exploration of P2PE, cloud, virtual payment cards, and new payment formats and other technologies.
Bring Android to work, safely

Employees’ use of personal devices – the consumerization of IT – is commonplace in the United States. In a recent survey from Citrix, 44 percent of CIOs said they have a formal, bring-your-own (BYO) device policy. In two years, 94 percent of the respondents will have one. Not all smartphones, however, are created equal: The popular Android holds a number of threats for the enterprise network, from malware to unauthorized transmission of personal data to SMS scams. We expect more news of Android’s security weaknesses in the coming months, because the platform’s openness and marketplace processes makes it enticing for criminals.

Securing Android – or any mobile device – will go beyond standard protection methods. The mobile phone’s connection points – user, charging device and external network – are what make it vulnerable. These vectors don’t exist in the PC world. Current threats for Android range from malware that steals device data – including messages, emails and call contents – to text messages that charge premium rates to trojans that access the network via the mobile connection point. Only recently, Android trojans that record and transfer voice calls have been seen. With Android, the CIO needs a laser focus on permissions, device security and connection points to prevent these threats.

Mobile device network access and permissions should specify what each individual mobile user can access and do on the network. If malware is able to access the network, these controls will make it tough to reach data. The organization must also ensure it has enhanced security for each smartphone, beyond what is on the device. Finally, the IT department should increase the scans of inbound and outbound device connections to spot unusual patterns. These additional steps will give the CIO a consistent level of usage policy enforcement and control, which, in turn, will allow more security across the mobile infrastructure and the internal fixed network systems.

Cloud management practices

Single sign-on and encryption policies are putting credential management – and in particular public key infrastructure (PKI) – under closer scrutiny these days. The spotlight has become more intense as we witness the meteoric rise in mobile devices for business use, as well as the growing reliance on the cloud for application development and delivery. Developers, for one, are facing a growing need to expand authentication processes to enable secure sign-on and encryption from any device. Authenticating access to cloud-based applications is also putting an increasing strain on development requirements.

Recent breaches have shown that password protection is simply not enough, as organizations deal with increasingly stringent legislative demands for authentication. Even so-called encryption features in mobile devices are proving to be tantamount to locking a door and leaving the key under the mat for others to break in. Historically, deployment of PKI entails a high total cost of ownership, as vendor-provided PKI solutions typically require extensive management and in-house IT support.

Rather than investing in a full-blown and costly PKI infrastructure, however, developers can now turn to third-party platforms to meet their credential management needs, either in the cloud or at the endpoint (i.e., the mobile device). By “plugging into” a full PKI infrastructure that operates the digital certificates for them, developers can eliminate the cost impediment associated with credential management and apply the needed security measures across multiple applications.

When selecting a third-party vendor for data encryption and credential management, the orcus is on IT managers to ensure that the vendor is leveraging a PKI-based technology and working with a provider that also can protect sensitive information on endpoint devices and in the cloud. With the right third-party resources, businesses will ultimately reap the full benefit of credential management at a much lower cost.
Got something to say?

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

In response to an August Opinion column, Affiliate programs: legitimate business or fueling cybercrime?, by Bradley Aronis, VP technical strategy, M86 Security:

I am the affiliate manager for a large brand. We find that just the mention of affiliate marketing can leave a bad taste in people’s mouths. There are many affiliate programs that just promote junk, don’t stand behind their product, and rarely pay out when they are supposed to. It makes my job much more difficult, but when I do get someone to sign up, and they start seeing real dollars, they are true believers in affiliate marketing.

Nathan O’Leary

In response to the Debate in the September issue, Security awareness training is a worthwhile investment (Amrit Williams, CSO at Quantivo, argues that educating the workforce is not enough to protect corporate resources):

Pardon me, Amrit, but that seems to be a very narrow and uninformed take on awareness training. We all know a layered defense is required and that if your company is in the sights of an APT team, you will eventually go down. But having an informed workforce is probably one of the easiest and most cost-effective steps you can take to reduce help desk nuisance calls, i.e., a Windows alert told me I had new viruses on my system and I had to click to remove them, what do I do now? If your philosophy was accurate, we wouldn’t need to have driver training for new drivers, because as we all know, everyone follows the rules, all the time. But if you don’t know the danger exists, many will proceed and break those rules.

Rick Swimmer

Amrit Williams responds: I disagree. I believe that no matter what you tell people, someone somewhere is opening a malware-laden email because he really does believe that someone somewhere does love him. You highlight the general theme of most arguments for security awareness training… awareness training empowers all employees to make better decisions. Sure, but only when you have implemented all the proper controls and you are wanting to add yet another layer, but never, ever is awareness training a substitute for real controls.

Jeff Sherwood

In response to an August news story, PCI Council revokes company’s QSA status:

So long as PCI allows QSAs to perform the validation and implement the solutions, one should expect the issue to continue. What are the chances a QSA is going to find an issue with solutions they recommended and implemented in subsequent validations? Zero percent. At my initial QSA training, the instructor told the class that nine out of every 10 dollars QSA firms earn will be from the implementation of solutions. Hence, everyone gives away the validation in hopes of making the consulting bucks. PCI can never be taken seriously so long as there are no independence requirements, and QSAs are engaged to review the results of their own work.

QAToo

In response to a July story, UCLA Health System fined over celebrity patient snooping:

Nice article. Hospitals in general need to do a better job of making employees aware of the HIPAA and HITECH requirements like these. I have found that employees do not completely understand the HIPAA regulations nor the implications of not following them. Just displaying the medical record of a patient without a valid business purpose is a privacy breach. My advice to UCLA Health System, first and foremost, is to provide education to all employees. They can expect that auditors will ensure access to patient information is being logged and that someone is reviewing the log, especially for celebrity patients. It will be interesting to see the practice changes UCLA Health Systems and other hospitals put into place.

Kerry Shackelford, www.coalitionsystems.com
After the lull of summer, the chatter of some 55 million students has, once again, enlivened classrooms at more than 100,000 public schools across the country.

Schools maintain great volumes and varieties of sensitive student information— not just names, addresses and Social Security numbers— but also intimate details of a student’s life, such as health data, teacher and counselor notes, discipline records and, of course, grades. The U.S. Department of Education (DoE), the agency charged with establishing and enforcing federal education policies, in April announced a series of initiatives aimed at safeguarding student privacy. As part of this effort the agency hired its first-ever chief privacy officer (CPO), Kathleen Styles.

Styles, now just six months on the job, is heading up a new division called Privacy Information and Records Management Services, dedicated to advancing the acceptable collection, use and disclosure of information within the department. In her role, Styles is working with states and districts to implement privacy precautions, such as minimizing the collection of personal information. Also, she serves as a senior adviser to U.S. Secretary of Education Arne Duncan on the department’s privacy, confidentiality and data security policies.

Styles says the agency’s increased focus on privacy is necessary to deal with a recent “explosion of information about students” in federal, state and local school systems— thanks, in part, to the digitization of student data. Digital records can ultimately be even more secure than those in paper form, she says, but the move to computerize data comes with an entirely new set of privacy challenges that must be managed.

Also contributing to increased privacy demands within the education sector is the establishment of Statewide Longitudinal Data Systems (SLDS). Such systems, which are grant-funded and currently in place in 41 states and the

Kathleen Styles is heading up a U.S. Department of Education effort to improve student privacy. Angela Moscaritolo reports.

MAKING THE GRADE
District of Columbia, serve as statewide repositories of student performance and demographic data that can be used to track student progress over time and analyze the effectiveness of school programs.

“The challenge is how to use that information to improve education and increase accountability, while still preserving privacy protections for our children,” Styles says.

Like the Education Department, many organizations today have a CPO in place to manage data governance programs, and a core team working on privacy and data protection issues, says Trevor Hughes, president and chief executive officer of the nonprofit International Association of Privacy Professionals (IAPP). Too, privacy is often “extending throughout the enterprise,” Hughes says, with the help of so-called privacy liaisons within various departments, including IT, product development, marketing and HR, who manage some aspect of privacy as part of their overall job responsibilities.

Many experts agree that the alliance between the privacy and security teams is particularly important. The two disciplines are actually “two sides of the same coin,” as they share the common goal of protecting data from being used inappropriately, Hughes says. However, there often are nuanced differences between the two professions. While the stated goal of an information security professional is to protect the confidentiality, availability and integrity of enterprise data, privacy professionals aim to ensure data is used in compliance with the law and, perhaps most importantly, consumer expectations.

The field of privacy, says Styles, combines the practical aspect of security with the exercise of answering theoretical questions about the appropriate uses of data. “I find it to be fascinating,” Styles says. “It’s a field I enjoy greatly.”

Across the federal government, all agencies have privacy programs, though they exist in various levels of maturity, Styles says. For instance, not all agencies have a CPO, let alone one with executive-level authority, such as Styles has. At some other agencies, privacy exists within the legal or IT departments, instead of being a standalone office.

“An emerging best practice is that privacy is separate,” Styles says.

The rise of a profession

Looking back, there have been individuals working on issues related to privacy for decades, says IAPP’s Hughes. In the early 1970s, however, there weren’t many pros specifically focused on privacy, besides a handful of lawyers working in government. At the time, much of this work revolved around the creation of the Privacy Act of 1974, which governs the collection, maintenance, use and dissemination of personally identifiable information maintained by federal agencies.

Within the private sector, the profession began to take hold during the dot-com boom, Hughes says. “Not until the 90s did we see corporate America recognizing the need for specialists in the field of privacy,” he says.

At the end of the decade, there were still fewer than 150 privacy profession- als in the United States, Hughes says. By 2002, when Hughes came on board as executive director of the IAPP, the organization had around 500 members. Today, its base has grown to more than 9,000 across 70 countries.

There is no time like the present to pay attention to privacy.

“There has been a story of very significant growth year after year, with so many factors feeding into that growth and helping to build the profession,” Hughes says.

An influx of privacy and data security regulations applying to individual business sectors and states have been largely responsible, experts say.

Also driving the profession is the near-light-speed pace of technological innovation. As a result, new privacy concerns crop up almost daily and are garnering more and more attention from both consumers and policymakers. The rise of social media, online behavioral advertising, mobile devices and cloud computing, for example, have all raised questions about the collection, storage and use of personal data.

Still, the majority of privacy professionals are employed within large organizations, according to the IAPP’s 2010 Salary Survey. The poll of nearly 1,000 members found that 64 percent of respondents work at organizations with 5,000 or more employees.

While large companies in the United States are focusing on privacy due to brand concerns and strong enforcement of state and federal regulations, many small organizations are still struggling with such demands, says Andy Serwin, chair of the privacy practice at Foley and Lardner, a Milwaukee-based law firm, and executive director of The Larees Institute, a technology and information governance think tank.

Some small businesses don’t have a handle on the privacy laws with which they must comply, he says. Others simply do not have sufficient resources necessary to build out a privacy program within their organization.

Ad evolution

Perhaps there is no better person to discuss the evolution of the privacy profession than Jennifer Barrett Glasgow. That’s because she is widely considered to be the first-ever CPO and on the front lines today of an ongoing debate over internet privacy issues.

Two decades ago, Glasgow was tapped to create a privacy program at the marketing services firm Acxiom. At the time, Acxiom had just acquired a data company called InfoBase, which maintained a repository of customer intelligence that was gathered from public records and surveys for marketing purposes. Now in the market to sell data, company leaders quickly realized they had to learn how to do so appropriately, while also generating revenue.

“It was in 1991 that I was asked to look at this thing called privacy and what it meant to the company,” Glasgow recalls. “I started out thinking it would be a 12- to 18-month project to figure out what we should be doing. And here I am 20 years later, though it’s a very different scope and scale.”

Many of the regulations with which the company must currently comply didn’t exist even five years ago, she says. For a global firm, navigating the changing regulatory landscape requires a dedicated team of personnel and constant monitoring.

These days, the organization has a global privacy team of about 15 employees, organized geographically by region, focusing on the Americas, Europe, Asia-Pacific and Northern Africa. The group establishes policies based on regulations, recommendations and industry best practices. It also helps to roll out the policies across its individual lines of business, which are ultimately responsible for maintaining compliance.

The privacy department also functions as an internal auditor, conducting periodic compliance reviews. Glasgow explains.

As the company considers acquiring new products, the team conducts impact assessments to ensure compliance with company policy can be achieved.

Besides the growth in federal and state regulations, one of the changes impacting Acxiom’s privacy program is the surge of so-called consumer data collection.

Glasgow says.

When browsing the web for products or services, a cookie, or small data file, may be placed on a user’s computer to allow advertising firms to silently track the URLs that user visits, as well as the date, time and duration of each visit. This data collection helps advertisers increase the effectiveness of their campaigns by serving consumers ads based on their preferences.

But, it has sparked an intense privacy debate that is currently playing out in Congress. “A ‘do-not-track’ bill, introduced in the U.S. Senate in May, would offer web users the option to prevent advertising and marketing companies from collecting information about their web-browsing activities.

The Do-Not-Track Online Act of 2011, introduced by Sen. Jay Rockefeller, D.W.Va., is widely supported by a number of U.S. privacy groups, including the American Civil Liberties Union and Electronic Frontier Foundation. Members of the online advertising community, however, argue that such a law would harm innovation and say the industry self-regulation of such advertising has been effective to date.

Ultimately, advertising firms, like all companies that collect sensitive information, are obligated to protect consumer privacy. “As we consider privacy issues in any new products and services they offer, Glasgow says. One of the questions privacy professionals must ask themselves is how much data shared on their networks is too much.
Back to the books

One of the greatest challenges facing those in the field today is that current laws do not always adequately address or clearly respond to today’s privacy questions, says IAPP’s Hughes. Many of the existing laws were created before the advent of today’s latest technologies and business models.

Those in the education sector are currently dealing with this reality head on. As part of its commitment to better safeguard student privacy, the DoE has proposed several clarifications to the Family Educational Rights and Privacy Act (FERPA), a federal law enacted in 1974 to protect the privacy of student education records. Currently, FERPA applies to schools that enroll students in K-12 and higher education. There has been confusion, though, about whether agencies and service providers that do not enroll students, but have received permission to work with pupil data as part of research projects, should have to comply with the law. The newly proposed changes would extend the law to all entities with access to sensitive student data. Additionally, under the DoE’s proposal, high school administrators would be able to share student achievement information to track how their graduates perform in college. States would also be able to enter into research agreements on behalf of their school districts to measure the success of programs.

The department says the changes will give states the flexibility to share data for research purposes and also increase accountability for those with access to student information. Critics of the proposed changes argue that they could actually hinder privacy by making it easier for states to collect and share information about students. The National Association of Independent Colleges and Universities, for example, has opposed the plan, noting that it would “substantially increase the number of entities allowed to access personally identifiable student information without the student’s or parent’s consent.”

The DoE is currently reviewing the 274 public comments it received during the 45-day period the proposed regulations were open for feedback, Styles says. The responses have been “all over the map,” she adds. Some commentators support the changes and say they strike the right balance by allowing for effective use of data while protecting privacy. Others, meanwhile, say the changes would erode privacy.

A final version of the law is due out by the end of the year, Styles says. She hopes it will provide more clarity and guidance to schools. As part of her role, Styles says she aims to bolster and standardize data management practices within the agency and provide guidance to help state and local school systems improve their own privacy postures. For now, a number of privacy questions remain unanswered, though, such as what kind of impact the FERPA changes will have within the education sector and whether regulations to reign in behavioral advertising will ultimately materialize. Only time will tell, but one thing is certain—the privacy profession is burgeoning in the United States. “I applaud organizations that are embracing the idea of CPOs and privacy professionals,” says IAPP’s Hughes. “There is no time like the present to pay attention to privacy.”

MICROSOFT: Privacy by Design

Privacy, like security, must be considered during the development of new products and services—not after the fact, says Brenda Lynch, CPO of Microsoft. The approach, dubbed Privacy by Design (PbD), recently has risen to popularity within the privacy community, but is actually an idea Microsoft embraced when it started its privacy program more than a decade ago, he says.

PbD was used, for instance, in the development of Microsoft’s new, controller-free gaming and entertainment console, Kinect for Xbox 360. The system, which lets users control video games with their own voice and body movements, posed some unique privacy challenges due to its use of facial and body recognition technology to identify players.

“The outcome is that we delivered it in a way that biometric information is only used on the device and never shared back to a server, and not stored in a way that can personally identify anyone,” Lynch says.

The Redmond, Wash.-based computing giant has more than 40 full-time privacy professionals and another 400 individuals who oversee privacy policies as part of their role, Lynch says.

Companies should work to manage data responsibly as part of a comprehensive privacy policy, Lynch says. It also is vital to be transparent about privacy practices and provide customers with a choice about how their data is used. Failing to do so could not only tarnish a company’s reputation, but also hinder its bottom line, he says.

“If we aren’t responsible custodians of information, it’s going to have a significant impact on our business,” Lynch says. – Angela Moscaritolo
There is reason to believe Russo’s hunch might be correct. According to Visa, 97 percent of the largest U.S. merchants, the 377 retailers that process greater than six million transactions per year, have validated compliance with the Payment Card Industry Data Security Standard (PCI DSS). Ninety-six of the 881 businesses that process between one and six million transactions also have attested to the rules.

“The days of somebody being able to do a real quick SQL injection and gain loads of data for most level-one merchants, I think those days are over,” says Jeff Hall, a PCI security assessor, boatloads of data for most level-one and six million transactions also have Standard (PCI DSS). Ninety-six of the year, have validated compliance with the to Visa, 97 percent of the largest U.S. hunch might be correct. According

According to a Verizon release.

prosecutions of high-profile hackers,” against these more vulnerable targets, targets for many hackers, who favor

possible reasons for this trend, includ-
ging the fact that small- to medium-sized businesses represent prime attack targets for many hackers, who favor

The report also indicates there are several possible reasons for this trend, includ-
ing the fact that small- to medium-sized businesses represent prime attack targets for many hackers, who favor

Mobile Payments: Empower merchants

While a push by Visa to spread adoption of chip technology could lead to increased levels of security and fewer compliance headaches for merchants, the world’s leading card brand isn’t being entirely selfless. Visa hopes its newly announced Technology Innovation Program (TIP) will give a shot in the arm to mobile payments, consid-
ered its next-generation business model.

Top three challenges to obtain PCI compliance

| Network segmentation to “wall off” your customers’ credit card data | 27% |
| Auditing system and data access | 15% |
| Patch management | 19% |
| Securing your decentralized stores and/or locations | 16% |
| Wireless networking security | 9% |
| Encryption of data in motion | 7% |
| Encryption of data at rest | 7% |

Or when it specifically comes to steal-
ing credit card numbers, the attackers may be finding it harder to get to the giant stacks. Much of the criticism dealt

over the mobile web and also payments made with a mobile device at a point-of-
sale terminal, which is derived from the $240 billion. Much of the value, which includes both purchases conducted

For one, an international standard for EMV already exists. But more significant, Visa offered a serious boost in August when it announced an incentive plan for merchants to migrate their terminals to accept EMV, contactless EMV payments.

Under Visa’s Technology Innovation Program (TIP), which takes effect Oct.

to “wall off” your customers’ credit card data | 23% |
| Auditing system and data access | 20% |
| Patch management | 20% |
| Securing your decentralized stores and/or locations | 15% |
| Wireless networking security | 16% |
| Encryption of data in motion | 11% |
| Encryption of data at rest | 11% |

most adoption is EMV, commonly referred to as chip-and-PIN.

EMV technology effectively replaces the need for a magnetic stripe because a microchip is embedded into the card, corresponds to a PIN, and is virtually impossible to clone. The U.K. has had great success with EMV, and this year, the U.K. Cards Association reported that credit card fraud fell 17 percent to $92 million, the lowest level in a decade.

Of course, criminals won’t stand idly by as security improves. Instead, the fraud will migrate to another channel, such as card-not-present transactions conducted over the web, which EMV can’t protect against, say experts.

And given the challenges crooks are running up against with measures such as tokenization and point-to-point encryption, they also are scurrying to find new and effective ways to steal the card numbers in the first place. One area of growing concern is skimming. According to the Verizon report, physical attacks in which credit card devices, such as ATMs and point-of-sale terminals, are manipulated to capture the card number as the card is swiped doubled again in 2010, after also dou-
bling the previous year.

“Now the endpoints become the tar-
gain to another channel and, in some cases, such as this, according to experts, not only raise concerns of on-premise termi-
nal manipulation, but also the possibility that tampering might occur somewhere along the supply chain.

Russo points to the PCI Council’s Payment Application Data Security Standard (PA-DSS) and PIN-Entry Device (PED) benchmarks, which provide best practices to protect against skimming. The council also maintains a list of trusted hardware and software providers.

In the end, no defense is unbreak-
able. Russo insists. That’s why organiza-
tions must continue to follow all of the guidelines the council dispenses. While organizations are getting a better handle on technologies like encryption, they’re still falling short in other areas, includ-
ing patch management and network segmentation, according to Gartner. In fact, Visa says, most merchant breaches reported in 2010 involved card data outside of the payment network envi-
ronment. Such a scenario adds weight to Russo’s message.

“There are no silver bullets,” he says.

“The more layers you could put on, the better off you’re going to be.”

The craft-store chain Michaels was a victim of arguably the most notable retail breach this year, not because of a vulnerable wireless connection or flawed website, but because thieves were able to implant skimming devices on terminals in 80 stores across 20 states. Incidents such as this, as such as experts, not only raise concerns of on-premise terminal manipulation, but also the possibility that tampering might occur somewhere along the supply chain.

The PCI Council’s Payment Application Data Security Standard (PA-DSS) and PIN-Entry Device (PED) benchmarks, which provide best practices to protect against skimming. The council also maintains a list of trusted hardware and software providers.

In the end, no defense is unbreak-
able. Russo insists. That’s why organiza-
tions must continue to follow all of the guidelines the council dispenses. While organizations are getting a better handle on technologies like encryption, they’re still falling short in other areas, includ-
ing patch management and network segmentation, according to Gartner. In fact, Visa says, most merchant breaches reported in 2010 involved card data outside of the payment network environment. Such a scenario adds weight to Russo’s message.

“There are no silver bullets,” he says.

“The more layers you could put on, the better off you’re going to be.”

Sensing that more retailers will adopt such initiatives, the Payment Card Industry Security Standards Council offered an update in June on which types of mobile payment apps meet its requirements. Further guidance is expected.

But, PSC’s Bates predicts the card brands will be challenged to change user behavior. “Having just lost my iPad, I’m not sure I want my credit cards on it,” he says. “For a 60-year-old like me, there is nothing wrong with plastic.” – Dan Kaplan
C
anian privacy law is undergoing an overhaul. The Personal Informa-
tion Protection and Electronic Doc-
uments Act (PIPEDA) is to be amended by bill C-12, a piece of legislation which received its first reading on Sept. 29.
Among the new provisions is a clause requiring companies to notify customers if they sustain a serious data breach. But will the bill be enforceable?
Under the new rules, private organiza-
tions that are compromised must report it to the provincial privacy commis-
sioner if it is reasonable to believe that the information’s release could cause significant harm to individuals. The commissioner then decides whether the breach is serious enough to warrant wider public notification.
According to the proposed legisla-
tion, the parameters affecting whether a breach is more widely reported include the sensitivity of the information that leaked, and the number of individu-
als whose personal information was involved. The third parameter is the extent to which the breach indicates a systemic problem.
It must be reported to the privacy commissioner “as soon as feasible” after the organization discovers the incident, according to the legislation.
This is the first time that any such breach notification laws have existed in Canada at a federal level. Such sweep-
ing laws do not exist in the United States, outside of specific sectors, such as health. However, south of the border, there are state laws that have effectively made breach notification an effective policy at a national level. “The United States was the model, and it’s the U.S. that developed this,” says Michael Geist, Canada research chair of internet and e-commerce law at the University of Ottawa.
But is mandatory breach notification a good thing for Canadians? “You’re seeing more and more breaches come to the forefront,” says Michael Power, a Toronto-based lawyer specializing in privacy and security. Companies aren’t very good at taking care of security on their own, he says. This requirement only tells you that organizations have published a privacy policy, have someone
who says he hopes that the Cana-
adian legislation will handle breach notification more effectively than the U.S. In many cases, the U.S. requires organizations to notify people about any breach, including minor ones that don’t financially hurt anyone, he says.
In Alberta, the only province to have a formal breach notification requirement, the model is more in line with PIPEDA’s new system. There is a two-part test in which the privacy commissioner is con-
tacted first. The breach is then assessed for “significant harm.”
According to the proposed legisla-
tion, the parameters affecting whether a breach is more widely reported include the sensitivity of the information that leaked, and the number of individu-
als whose personal information was involved. The third parameter is the extent to which the breach indicates a systemic problem.
It must be reported to the privacy commissioner “as soon as feasible” after the organization discovers the incident, according to the legislation.
This is the first time that any such breach notification laws have existed in Canada at a federal level. Such sweep-
ing laws do not exist in the United States, outside of specific sectors, such as health. However, south of the border, there are state laws that have effectively made breach notification an effective policy at a national level. “The United States was the model, and it’s the U.S. that developed this,” says Michael Geist, Canada research chair of internet and e-commerce law at the University of Ottawa.
But is mandatory breach notification a good thing for Canadians? “You’re seeing more and more breaches come to the forefront,” says Michael Power, a Toronto-based lawyer specializing in privacy and security. Companies aren’t very good at taking care of security on their own, he says. This requirement only tells you that organizations have published a privacy policy, have someone

Related to the federal sector (Privacy Act)

2,022

Related to the private sector (PIPEDA)

2,393

Other (issues redirected to another jurisdiction or not covered by privacy legislation)

4,793

Inquiries received by the privacy commissioner in 2010

Source: Office of the Federal/Ontario and Canadian Privacy Commissioners

that developed this,” says Michael Geist, Canada research chair of internet and e-commerce law at the University of Ottawa.
But is mandatory breach notification a good thing for Canadians? “You’re seeing more and more breaches come to the forefront,” says Michael Power, a Toronto-based lawyer specializing in privacy and security. Companies aren’t very good at taking care of security on their own, he says. This requirement only tells you that organizations have published a privacy policy, have someone

However, Alberta’s approach to evaluating harm makes it almost U.S.-like in its assessment of breaches, Power says. “If an email address is exposed in a data breach, it takes the view that this is a risk of significant harm, and that you have to notify,” he says.
Could the federal government be equally sensitive?, Powers asks. “They

set the bar very low in Alberta. As to how it will be set at a federal level, it remains to be seen.”

Unless PIPEDA has teeth, the question of how low or high the bar is set may be moot. One complaint about the legislation is that it isn’t powerful enough because the capability to enforce it doesn’t exist.

“You don’t have any order-making power, so the privacy commissioner can only make findings and recommenda-
tions,” says Power, calling it a deficiency in the current statute. “If there is a systematic problem in an organization that has a number of privacy issues, then you could argue that she has no power to fine.”

Cases have been bought against orga-
nizations under PIPEDA, but they are private cases where an organization has been sued by an individual, rather than a privacy commissioner.

Last month, Nicole Landry sued the Royal Bank of Canada after it faxed information about her finances to her husband’s lawyer during their divorce.
The court called the incident a serious violation of PIPEDA, but only awarded her $4,900 in damages. She had asked for $10,000.

This is only the second time that dam-
ages have been awarded under PIPEDA. The first was in 2010, when the federal court awarded $5,000 to a banking client after it was found that their credit profile contained someone else’s details.

Not everyone has the power or money to bring a private case. Some ask why can’t the privacy commissioner do it for them? France and Germany have the power to make rulings and fine people.

The Federal Trade Commission in the U.S. can penalize companies for breaches. The decade-old PIPEDA law is reviewed every five years. The last review was in 2005, and the next was delayed by the recent, unexpected Canadian elec-

tions. Geist expects the next review will slip to 2012.

“The commissioner is on the record saying that she will push for an enforce-
ment agenda,” says Geist. “And the gov-
ernment has talked about enforcement in other areas.”

Could the regulators step in where the privacy commissioners are not allowed? In the U.K., for example, it was left to the Financial Services Authority to sue Nationwide, a bank whose employee lost a laptop contain-
ing the personal details of thousands of customers. That cost the bank £980,000 ($1.58 million Canadian).

In Canada, the regulators are a lot less active. Power hasn’t seen a financial regulator step in and impose a penalty for a privacy violation. They see it as the privacy commissioner’s jurisdiction.

More than breach notifications, the thing that has critics riled about the PIPEDA amendments are a clause allow-
ing businesses to disclose information without the knowledge or consent of the individual involved. This is permitted in some very broad cases, such as “perform-
ing police services,” and “preventing, detect-
ing, or suppressing fraud.”

Organizations such as OpenMedia, a digital rights advocacy group, are con-
cerned that this will make the Canadian law more like the controversial USA Paren-
t Act, a legislative response fol-
lowing the attacks of 9/11, which make

it easier for law enforcement agencies to search personal communications transmitted via a wire, email or other records. The group is also concerned that the provision will serve as a precur-
or to lawful access legislation. The government attempted to pass this legislation, which allows authorities to monitor Canadian internet users’ habits, as bill C-52 in the last parliament. But, it was dropped from the recently tabled omnibus crime bill.

Faith in PIPEDA won’t be helped by the fact that it doesn’t apply to the government. Public sector organizations are governed by the Privacy Act, which is a far older piece of Canadian legisla-
tion determining how the government should treat people’s privacy. There is no provision in this legislation for breach notification, and no likelihood that it will be updated anytime soon, meaning that the government is taking a “do what we say, not what we do” approach to the whole issue.

“Every privacy commissioner since the 80s called for a modernization of the law,” says Geist. “They tried everything from reports through to a top 10 list of low-hanging fruits of ready and relatively painless changes.”

As of this year, then, it appears that PIPEDA is moving in the direction of less privacy, rather than more. It enables more private information about Canadi-
an citizens to be collected and disclosed, and doesn’t include the capability for the privacy commissioner to penalise companies for mishandling information. There is a privacy breach notification clause, but without teeth, how hard can the privacy commissioner bite?

Canadian is overflowing its 10-year-old privacy law. Do the changes go far enough? Danny Bradbury investigates.
Mobile malware, often distributed through applications, is increasing in scope and sophistication. Is your business ready? Dan Kaplan reports.

Sometimes, the forecasters guess correctly. That appears to be the case with the myriad statements entering 2010 and 2011 that forecasted a precipitous rise in malware targeting mobile devices.

According to a McAfee report released in February, the number of new mobile malware variants totaled 55,000 last year, a rather large spike of 46 percent compared to 2009. Clearly, the threat landscape has come a long way since 2004, when the first-ever malware for the mobile phone, known as Cabir, was sent to a number of antivirus firms for inspection. The worm, written for Symbian feature phones, was merely an innocuous proof-of-concept – it was designed to display the word “Caribe” on the phone’s display and spread to other devices using Bluetooth signals – but its arrival certainly proved prescient.

A couple of years later, in 2006, Kaspersky Lab identified what it called the first piece of mobile malware designed to steal money – a virus that targets devices running Java. Dubbed RedBrowser, the virus sent text messages to premium-rate numbers without the user even realizing it.

Fast forward to 2011 and it appears the tipping point is near. According to Nielsen, the number of smartphones in the United States, such as the iPhone, BlackBerry and Android, is expected this year to overtake the number of feature phones. This steady ascension, from handhelds that provide few capabilities beyond calling and texting to phones with functionality that resembles a traditional computer, has of course piqued the interest of the malware community. After years of test runs that largely affected mobile phone users overseas, cybercriminals are now rolling up their sleeves and readying their wares to resemble what malware victims are used to seeing on their desktop or laptop computer.

“Smartphones have all the components you would expect of a traditional PC,” says Andy Chou, co-founder and chief scientist of Coverity, a software integrity firm based in San Francisco. “They are capable and complex. They have operating systems and applications that run on top of them.”

Hackers traditionally have written most of their malware for Symbian and Windows Mobile devices because they are the oldest and most researched. But that all seems to be changing.

According to a Juniper report released in May, malware samples targeting Google Android devices jumped 400 percent between June 2010 and January 2011. This should come as no surprise, though. After all, market share usually dictates malware targets.

A series of surveys conducted by Nielsen between January and March found that 31 percent of consumers planning to purchase a new smartphone now prefer Android, compared to 30 percent who would choose an iPhone and 11 percent who would opt for a BlackBerry. Twenty percent are unsure what they would buy next.

Within enterprises, while BlackBerry is considered the “gold standard” for enterprise-security functionality because of its management and encryption capabilities, many workers prefer the bells and whistles that the Android and iPhone provide.

Most experts agree that what makes the Android platform a particularly ripe attack vector compared to other mobile operating systems is its ever-expanding application marketplace. According to Lookout Mobile Security, the number of apps available in the Android Market climbed 127 percent from August 2010 to February 2011, while Apple’s App Store grew 44 percent.

The latest figures show that the Android Market contains close to 300,000 applications for download. The problem is, in some cases, these applications are nefarious in nature, customized to install malware on the phone or gain access to sensitive information.

“It is the main delivery mechanism to get on the phone right now,” says Chris Wysopal, co-founder and CTO of Veracode, an application security firm. “Android has gone with the more open model, and they allow developers to sign their own apps and put them up for download in the marketplace.”
While security vendors admit that the lion’s share of malware currently is being written for the more lucrative PC environment, that hasn’t stopped authors from fashionable their code to penetrate the mobile landscape. And chances are, they’d be effective, considering 85 percent of smartphone users do not use anti-virus, according to Juniper, citing an informal poll conducted by the SANS Institute.

Rogue applications are growing in sophistication. In August 2010, according to Juniper, the first Android trojan appeared in the form of an application that mimics a media player and allows the attacker to eavesdrop in public Wi-Fi networks and steal a token that could be used to access private data.

**Market watch**

So far, Android has been the mecca of malicious applications. Some experts blame its open model. Apple – the other main app provider – has avoided similar problems, except on “jailbroken” devices.

“When an Apple developer uploads an app, it goes through an approval process,” Wysopal says. “The app gets signed with a key issued by Apple. When the app goes to execute on the iPhone, the signature is checked. Unless the key is issued by Apple, that key won’t run at all. You know only good, known apps are able to run on the device.”

That is not to say one model is better than the other, Mahaffey says. Many developers and consumers prefer Google’s community-based approach where users flag things as malicious and apply ratings.

“We’re always balancing security and user experience,” he says. “Apple’s App Store is designed to be a safe place where you don’t have to worry about security, but Android is saying, ‘Hey, we want this to be a safe community place.’ One isn’t necessarily better than the other. They’re just different.

**MOBILE STRATEGY: Tips for businesses**

**Use anti-malware solutions and firewalls to protect against malicious applications.**

**Implement SSL VPN clients to protect data in transit.**

**Leverage centralized tracking, wiping and backup for lost/stolen devices.**

**Deploy centralized administration to enforce and report on security policies.**

**Control applications that employees may wish to install.**

**Monitor device activity for data leakage and inappropriate use.**

Source: Juniper Networks

Additionally, end users must worry about another class of applications: legitimate ones that may have been built without security in mind, Mahaffey says. For example, last July, Citigroup was forced to release an update to its iPhone banking application after it was discovered that the previous version, unknown to users, saved confidential account information in a hidden file on their devices.

Even apps that come standard on the phone can sometimes be vulnerable. German researchers in May disclosed that Android’s calendar and contact apps contain a flaw that could allow an attacker to eavesdrop in public Wi-Fi networks and steal a token that could be used to access private data.

**Businesses, however, should be concerned about malicious apps making their way onto employee-owned devices, Wysopal says. As a result, they should consider a mobile device management solution, as well as ensure that all enterprise-level mobile apps, such as for document-sharing, meet security specifications prior to purchasing them.**

Of course, today’s smartphones are complex, and therefore apps can’t be blamed for all that goes wrong. After all, in some cases, malicious apps must take advantage of an underlying platform vulnerability in order to be successful.

“[Apps are] the most visible concern,” says Covington’s Chou. “But in terms of the volume of the software on these phones, there’s still a humongous amount that is below that level that you don’t get to see and interact with visually.”

For example, lower on the stack are drivers for Bluetooth and 4G connectivity, as well as the library layer, which is responsible for web browser rendering, Chou says. These components can be leveraged to spread malware by, for example, tricking a victim into opening a corrupted PDF file.

Still, Chou believes that from an architecture and software control standpoint, mobile platforms have learned many lessons from their predecessors. Even applications, while the preferred vehicle to spread attacks, are tightly restricted at best or, at worst, require the user to approve permission requests.

“The original version of the PC wasn’t really designed with security in mind,” Chou says. “Software that is now being put into phones, [many developers] are definitely aware of the core, fundamental problems.”

And there may be one other saving grace for the mobile world that will stave off hackers, in the near term at least: operating system heterogeneity. Criminals have less incentive to research something when there is no clear-cut market share bellwether.

“There is no operating system leader like Windows [is on the PC],” says Denis Maskennikov, a senior malware analyst with Kaspersky Lab. “Diversity helps with different security issues.”

This story originally appeared in our special “Spotlight on Mobile” issue.

---

**MOBILE STRATEGY: Tips for businesses**

**Use anti-malware solutions and firewalls to protect against malicious applications.**

**Implement SSL VPN clients to protect data in transit.**

**Leverage centralized tracking, wiping and backup for lost/stolen devices.**

**Deploy centralized administration to enforce and report on security policies.**

**Control applications that employees may wish to install.**

**Monitor device activity for data leakage and inappropriate use.**

Source: Juniper Networks

Additionally, end users must worry about another class of applications: legitimate ones that may have been built without security in mind, Mahaffey says. For example, last July, Citigroup was forced to release an update to its iPhone banking application after it was discovered that the previous version, unknown to users, saved confidential account information in a hidden file on their devices.

Even apps that come standard on the phone can sometimes be vulnerable. German researchers in May disclosed that Android’s calendar and contact apps contain a flaw that could allow an attacker to eavesdrop in public Wi-Fi networks and steal a token that could be used to access private data.

**Businesses, however, should be concerned about malicious apps making their way onto employee-owned devices, Wysopal says. As a result, they should consider a mobile device management solution, as well as ensure that all enterprise-level mobile apps, such as for document-sharing, meet security specifications prior to purchasing them.**

Of course, today’s smartphones are complex, and therefore apps can’t be blamed for all that goes wrong. After all, in some cases, malicious apps must take advantage of an underlying platform vulnerability in order to be successful.

“[Apps are] the most visible concern,” says Covington’s Chou. “But in terms of the volume of the software on these phones, there’s still a humongous amount that is below that level that you don’t get to see and interact with visually.”

For example, lower on the stack are drivers for Bluetooth and 4G connectivity, as well as the library layer, which is responsible for web browser rendering, Chou says. These components can be leveraged to spread malware by, for example, tricking a victim into opening a corrupted PDF file.

Still, Chou believes that from an architecture and software control standpoint, mobile platforms have learned many lessons from their predecessors. Even applications, while the preferred vehicle to spread attacks, are tightly restricted at best or, at worst, require the user to approve permission requests.

“The original version of the PC wasn’t really designed with security in mind,” Chou says. “Software that is now being put into phones, [many developers] are definitely aware of the core, fundamental problems.”

And there may be one other saving grace for the mobile world that will stave off hackers, in the near term at least: operating system heterogeneity. Criminals have less incentive to research something when there is no clear-cut market share bellwether.

“There is no operating system leader like Windows [is on the PC],” says Denis Maskennikov, a senior malware analyst with Kaspersky Lab. “Diversity helps with different security issues.”

This story originally appeared in our special “Spotlight on Mobile” issue.
CUTTING THE RED TAPE

As federal and state agencies are forced to do more with less, concerns continue to mount, Illena Armstrong learned during an SC Magazine roundtable.

To find a generally accurate barometer to gauge the typical pace of government, just turn to personal experience.

As an example, recall a recent jaunt to the Department of Motor Vehicles to renew a driver’s license or, perhaps more fitting given still bleak economic forecasts, a visit to the state Unemployment Insurance Agency to verify eligibility for extended benefits. The lines to talk to an agent undoubtedly were long, the conversation with the government representative likely patience-trying, the follow-up paperwork tedious, and the desired end result long in coming.

Similar types of impediments experienced by the average Joe or Jane can grow weary of wrangling for needed funds and resources. “It’s a mixed bag,” says Bob Maley, founder and principal at consultancy Strategic CISO and former CISO of the state of Pennsylvania, agrees, pointing out that many IT security pros have trouble keeping on top of operating system and security updates.

One of the top concerns for technology leaders gathered at an SC Magazine roundtable was the increased use of newer technologies in the enterprise, such as mobile devices, cloud services and social media.

According to experts, who were interviewed in just the last month.

As a host of challenges often thwarts even the most stalwart pro with support.

Part of the reason for this is the time it takes to get projects finished, he adds. Approval processes to acquire funding, to choose vendors and more are extremely time-consuming.

“They have to believe it’s the state of bureaucracy rather than the private sector,” he says. “They’ve got to believe it’s the state of bureaucracy that slows things.”

These hardships and many others voiced at an SC Magazine Government Security Roundtable sponsored by ArcSight, an HP Company, and held late last year, still hold true for many in this space, according to experts, who were interviewed in just the last month.

“Getting end-users to ‘work smarter’ is a constant priority,” says Eric Avakian, CTO of ArcSight’s public sector division, said during the Roundtable.

Many attendees of last year’s Roundtable – including ease of use, deployments, such as those mentioned at the Roundtable – including ease of use, mission enhancement, cost and, yes, security – they make great strides in hindering the attacks targeting these, he adds.

Many IT security pros likely welcome such advice even more today than during last year’s SC Roundtable given the spike in high-profile attacks against government agencies and critical infrastructure companies over the last several months. Although traditional forms of cybersecurity focusing on data theft for profit gain still reign, government-sponsored strikes and hacktivist attacks have spiked.

For example, the group LulzSec took responsibility for hitting websites belonging to the Central Intelligence Agency, the U.S. Senate and a slew of others. Too, various federal agencies and defense contractors, such as Lockheed Martin, have experienced system breaches likely spear-headed by foreign intelligence groups.

Perhaps unsurprisingly, vectors of attack discussed more than any others at SC’s Roundtable included cloud services, mobile networks and social networking. Indeed, these areas still pose vexation for many.

Part of the predicament, says Kris Rowley, CISO for the state of Vermont, is that there are so many types of devices that many IT security pros have trouble keeping on top of operating system and security updates for them.

Eric Avakian, the current CISO for the state of Pennsylvania, agrees, pointing out that mobile device policies are key to locking down critical data.

But older attack methods are still in use. IT security leaders must remember that even some of the newest attacks still rely on more traditional means of entry, such as social engineering, Prescott Winter, CTO of ArcSight’s public sector division, said during the Roundtable.

contact.roc.houar@haymarketmedia. com for a full version of this story.
After basketball, he plans on joining his hacktivist pals online.

Attend SC Congress New York on Nov. 16 to help your IT security program overcome these fast-evolving threats. When you attend, you’ll get everything you’ve come to expect from an SC Magazine event:

- A timely program of educational sessions and keynotes
- Thought-leading industry speakers
- Practical, current and hard-hitting best practices to better your security programs
- An exhibitor hall filled with top solution and service providers
- A bevy of networking opportunities to learn from and lessons to share with your peers

Get as focused on foiling his attacks as he is determined to break into your corporate network. SC Congress New York has your back.

It’s all about the data

There is only one reason that we bother with security of our information systems: the data. If we didn’t care about who sees, damages or alters our data, we wouldn’t need to waste millions of dollars on the tools of our trade. We could just hook up the networks and go out for a cold adult beverage, congratulate each other on a job well done, and update our résumés.

Sadly, that is not the case. The information is the crown jewel, your organization’s most important asset. We need to protect it or we put the organization at risk. So, although we still may want those adult beverages, it’s usually because of the rigors required to ensure that the information is protected. That is what this month’s Group Tests are about: the data.

Reviewer Mike Lipinski will first guide us through encryption products. Encryption is the mainstay of information protection and, in fact, I have heard experts seriously suggest that it really is all that we need. Imagine a world with no firewalls, no intrusion prevention systems, none of those other tools we use routinely. All one has is encryption. I’m not sure that we are ready for that yet, but there is no doubt that encryption is probably the most critical piece in our information assurance arsenal.

I fielded the other set of reviews. This is an interesting group because we picked the three top products based on our collective experience in the SC Labs. Each of those got a more complete review – a full page instead of just half a page. For some time we have been exploring ways to increase the depth of our reviews, and this just might be the ticket. Let me know what you think. You can email me at pstephen@norwich.edu.

We hope you enjoy this month’s reviews. These are two of the most important groups of the year, and it was a pleasure to bring them to you.

—Peter Stephevon, technology editor
Encryption

In the past, encryption tools often slowed down operations and were difficult to implement, but they’ve come a long way, says Michael Lipinski.

P

rotecting information against today’s sophisticated, real-time threats in today’s mobile environment is a challenge that keeps a lot of IT security professionals up at night. What is our defense against a breach that exposes a user’s file system? How do we protect sensitive data that walks out of the enterprise every day on laptops, mobile devices and removable media? We could say that we’ve established policies to prevent that from happening. That is a viable mitigation tactic. But, we continue to read about organizations with said policies losing a notebook, drive or tape with sensitive data on it. So, in the end, policies are only as good as the enforcement capabilities. Even within the enterprise, on systems that don’t leave the fortress, there is risk of exposure.

This month we focus on encryption technologies. Although, historically, these technologies were hard to use and impacted the performance of systems, they have always been a reasonably priced option for adding a layer of protection. Encryption technology isn’t new. With the risk of exposure increasing, should protection of the information where it resides become a required part of our defense-in-depth practice? I have to admit, encrypting files and media does have overhead, both in performance and time. But, I was hopeful to see some vast improvements in this technology as we reviewed this set.

We were looking for the performance impact on the local system. We were interested in what management tools were available to assist with deploying and managing this technology in a large enterprise. Another focus was the ability to securely back up keys or recover encrypted files or partitions. We tested the products in our virtual environment. We set up both 64-bit and 32-bit servers for hosting the applications and database components. If the applications supported 64-bit operating systems, we tested in that environment. Our desktop environment consisted of Windows 7 notebooks with various removable media components for testing those capabilities. Some of the solutions came with a complete installation package that ran through the deployment of the application and all the dependencies. Others were much more tedious to deploy and required a lot of manual configuration.

The solutions reviewed fell into two groups: user-centric or enterprise-centric. The difference was in how they were managed and deployed. The user-centric applications installed and were managed locally with some capabilities to back up configurations and keys. The enterprise-centric solutions provided a centralized console for setting up policy; provided software deployment tools; offered disaster recovery components, like centralized key storage, key backup and recovery options for systems under administrative control; and may have been LDAP/AD integrated.

Although we did not evaluate other endpoint protections under this review, we should note that several of these solutions were part of a larger suite of product offerings and integrated with a common management platform. All of the solutions did what they advertised. Yet, there were vast differences in how they would perform and how one could manage them in an enterprise environment.

Price, features and performance all varied, so the best option one has is to evaluate several of these when trying to choose a solution for the enterprise. Some of the offerings deployed quickly and were ready to use with little overhead. Others required some serious time and technical abilities to get up and working. In the end, there are some very good choices available. Price points are reasonable, and there are solutions that provide protection with little overhead. Consider adding encryption for data at rest as a last line of defense.

We also would like to take a minute to thank Kevin O’Connor for his help this month in the SC Lab, assisting with the product testing. Kevin stepped in and handled most of the physical deployments and testing so that I could keep my vacation plans, a date in North Carolina with Hurricane Irene.

Specifications for encryption tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Centrally managed</th>
<th>Key recovery</th>
<th>AD/LDAP integration</th>
<th>Removable media protection</th>
<th>Secure individual files</th>
<th>Whole disk encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point Full Disk Encryption vE80.20</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Credent Enterprise Server v7.1.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Cryptzone Secure efile and Secure eUSB v4.8.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Data Encryption Systems DESlock® Pro v4.1.1.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Safend Data Protection Suite v3.4SP4</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Sophos SafeGuard Enterprise v5.6</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Symantec PGP Whole Disk Encryption v10.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Trustwave Encryption v4.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>WinMagic SecureDoc Full Disc Encryption v5.2SR2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Files remain encrypted post LDAP/AD login: ● Encryption for transmitting files: ● Centralized policy management: ● Logging of information copied to removable media: ● Reporting: ●
### Check Point Full Disk Encryption

**Check Point Full Disk Encryption v80.20**

- **Vendor**: Check Point Software Technologies
- **Price**: $125/user at 1,000 users
- **Contact**: www.checkpoint.com

Check Point Full Disk Encryption provides a licensing structure that includes the Any-ID feature, which allows a single license to cover any number of endpoints. It is available in desktop and mobile versions, and it supports Active Directory (AD) for centralized management. The solution also offers a directory-based user authentication method, ensuring secure access to encrypted systems.

### Credant Technologies

**Credant Technologies Credent Enterprise Server v7.1.2**

- **Vendor**: Credant Technologies
- **Price**: $62/user at 1,000 users
- **Contact**: www.credant.com

Credant Technologies is a full-disk encryption solution that offers real-time encryption for all data on the hard drive. It supports both Windows and Linux operating systems, and it provides a centralized management console for easy deployment and management.

### Secured eFile, Secured eUSB v4.8.3, Secured eCollaboration

- **Vendor**: Cryptzone
- **Price**: $41/sec for 331; Secured eUSB: $33; Secured eCollaboration: $33
- **Contact**: www.cryptzone.com

Cryptzone offers a comprehensive suite of data protection solutions, including full-disk encryption, eCollaboration, and eUSB encryption. The platform provides a single console for managing all encryption policies and is compatible with various operating systems.

### Data Encryption Systems DESlock+ Pro v4.1.12

- **Vendor**: Data Encryption Systems
- **Price**: $53/user at 1,000 users
- **Contact**: www.des.co.uk

DESlock+ Pro is a full-disk encryption solution that supports both Windows and Linux operating systems. It provides a centralized management console for easy deployment and management.
Safend Data Protection Suite v3.4SP4

Safend Data Protection Suite (DPS) v3.4SP4 protects against data leakage by providing centrally managed desktop and laptop hard disk encryption. DPS is a hard disk encryption solution that leverages the security of full-disk encryption and the flexibility of file-based encryption to protect sensitive data. By encrypting data files — but not OS or executable files — multiple users’ data can be protected and segregated. User logout or standby instantly removes encryption keys for that user and protects against cold boot attacks. DPS is completely transparent — it does not require users to activate the encryption/decompression process or select or recover keys. Administrators can fix machines and install software without access to encrypted data. Internal hard disk encryption’s effectiveness is multiplied by using removable media encryption running on the same agent and enabled with a server license.

Server prep necessitated us installing Net 3.5 and IIS. Every-thing else installed for us with the Data Protection Suite Manage-ment Server implementation. The install offers a choice between using MS SQL or the embedded database, a nice deployment feature. Once up and running, user management is done through Active Directory (AD) integration. One has to open Windows Management Instrumentation (WMI) ports on the Windows Firewall for the management system to poll devices, but this allows one to not only manage them but also detect hardware.

Admins can install the user agents manually or via a group policy object (GPO). There was also a MAC client available, which we did not test. Security is set via policies and applied to AD groups, users or machines. One has full control over fixed and removable media encryption, including port and device control.

SC MAGAZINE RATING
Features ★★★★★
Case of use ★★★★★
Documentation ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★
Strengths Full control over fixed, removable media, and system ports and devices. Easy to use and deploy.
Weaknesses Sharing of encrypted data on non-client devices can be confusing, but not to clarity.
Vendor Safend
Price $25+ per seat
Contact www.safend.com

Sophos SafeGuard Enterprise v5.6

Sophos SafeGuard Enterprise v5.6 uses FIPS 140-2 validated cryptographic deployed and managed from an easy-to-use console.

The tool encrypts data transparently — users do not need to decide which data is to be disguised. Encryption and decryption is performed in the background. The operating system is encrypted at up to 256-bit AES behind a secure pre-boot (power on authenticati-on) environment to the entire hard drive. Access through the pre-boot environment is single sign-on, taking the user straight to the installed operating system. If the user forgets their password, they can answer predefined questions through a challenge-response interface to enable access without a call to the help desk. Each encrypted client has a small agent installed to collect and apply policies, and the compliance status of each machine can be easily seen in the management console.

The installation is very intuitive. First, one installs SafeGuard Policy Editor. A wizard guides the admin through everything needed, including loading SQL Express, Net, IIS and any of the required security updates. One is guided through creating the default policy. The policy is then published into a configuration package and installed on the endpoints. We were very impressed with the load and setup process.

Capabilities can be extremely granular, though that level of capability usually comes with some complexity. The policy configuration can get complicated based on one’s requirements, but in the end, after interacting with the user interface for a bit, we had no problem working through anything we desired to configure. One can import users from a directory. One feature for administrators we particularly liked: Service accounts enable members of the IT team to logon to endpoint computers for post-installation tasks without activating the Power-on Authentication.

This is a feature rich, powerful solution at a reasonable price point.

SC MAGAZINE RATING
Features ★★★★★
Case of use ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★
Strengths Strong and very granular policy management, easy to use and deploy.
Weaknesses None worth noting.
Vendor Sophos
Price $574 (for 1,000 seats with perpetual license)
Contact www.sophos.com

PGP Whole Disk Encryption from Symantec v10.3

PGP Whole Disk Encryption from Symantec encrypts all the contents on the disk on a block-by-block basis. The complete disk is encrypted (including white space) to offer total data security. The only way to access an encrypted disk is with the authorized user’s passphrase and the pre-boot authentication.

PGP Universal Server is a console that manages the applications, and provides email, disk and network file encryption. Management from the PGP Universal Server allows ease of deployment, management and reporting from one central location. PGP Desktop was deployed on our endpoints and is available for both Window-s and Mac operating systems. The solution includes whole disk encryption; PGP NetShare, to share files among PGP users; PGP Virtual Disk, allowing users to employ part of a drive and an encrypted virtual disk; and PGP Zip, for creating compressed and encrypted packages.

The deployment requires a dedicated server and, as part of the process, wipes out any data on the server. PGP Universal Server is a customized Linux installation and cannot be installed on a Windows server. Every PGP Universal Server requires a dedicated system. PGP Desktop makes it easy to create and manage key pairs. With the Universal Server, a recovery token is stored (and tracked whenever accessed) to allow for forensic analysis of the disk or if the user forgets a passphrase. With the integration of Intel Anti-Thief technology, a stolen or misplaced laptop can be remotely disabled. This includes both the platform and the data residing on the disk. Client software can be delivered through a distribution platform directly or from the management console. Users can back up features for keys and reconstruct capabilities in the event a passphrase is forgotten. One has to use the Universal Server to set up policy and enforce encryption of removable media. This option works for USB devices.

SC MAGAZINE RATING
Features ★★★★★
Case of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★
Strengths Good enterprise whole disk and email encryption solution.
Weaknesses Complex management console. Very pricey solution.
Vendor Symantec
Price starts at $18 for 100 users, volume discounts available
Contact www.symantec.com

INFORMATION ASSURANCE

Every year, data breaches cost companies millions of dollars. That’s why it is important to know how to manage risks like cyber attacks, accidental damage and more. Take charge of your career with a master’s degree from the University of Maryland University College (UMUC). Our nationally recognized information assurance program can help you save your company critical dollars and increase the value of your work.

• Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and DHS
• MS in information technology with specialization in information assurance recognized as a Professional Science Master’s by the Council of Graduate Schools
• Program offered entirely online
• Interact free from monthly payment plan available, plus financial aid for those who qualify
800-888-UMUC • umuc.edu/data

Enroll now.
Trustwave Encryption v4.3

WinMagic SecureDoc Full Disc Encryption v5.2SR2

For performance, ease of use and features we select Trustwave DLP as our Best Buy.

Data leakage prevention (DLP)

Plenty of insiders and outsiders are motivated to remove sensitive data from its protected home on the enterprise network, but there are defenses, says Peter Stephenson.

This area is so important that we have broken our usual mold this month, and rather than presenting six to a dozen product to chew on, we have identified just three that we think are the best of breed. Then, we looked more deeply than we usually have room to do and expanded our coverage to a full page for each product. This gave us the space to take a more comprehensive look at these three offerings, and what we found was very interesting. My early sense was that this category is still new enough that we would see massive differences in approach, capability and the way the vendors view data leakage prevention. That didn’t happen. In fact, although the product we chose for Best Buy had some unique approaches to DLP, they all are quite similar and first-rate.

This time, we had the luxury of looking at how these products are set up in a structured, step-by-step manner, and we really got the chance to do some testing that we don’t normally have time to do when we have products to look at. For example, besides setting the test bed, we were able to create a full suite of policies instead of trying the policy manager once and then moving on to the next tests. As a result, we found some near, but hidden, capabilities that were part of this month’s products.

DLP no longer is an option; it’s a necessity. It is now common wisdom that you should consider your network infected. The only questions are, with what is it infected and when will the infection try to exfiltrate data? Even if you are not infected it is likely that you have users who will attempt to take data off of the network.

We reviewed a particular situation where an employee left the organization and came back later as a contractor in another area of the company. The person took all of the mail that was in his company email account and forwarded it to his personal Gmail account. He then planned to save all of the messages to a CD or thumb drive to return to the organization and ensure that the email was preserved.

The problem was that the emails were full of credit card numbers. These numbers hit the public mail server. As it happened, the organization was, at that moment, testing a DLP product and saw the exfiltration, caught it and stopped it. Fortunately, for sure, but one can’t depend on that kind of luck unless DLP is actually deployed. And that is what this set of reviews is about. Here are three superb products to consider. You will, naturally, pick the one that fits your application best but, no matter what that actually means in your context, don’t balk at cost, deployment and more. This is important not just for security, but also for privacy, liability and regulatory compliance. Just do it!
Specifications for data leakage prevention tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Code Green Networks TrueDLP v8.0</th>
<th>Fidelis Security Systems XPS v6.4.1</th>
<th>Trustwave DLP v9.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-configured policies</td>
<td>☐</td>
<td>☑</td>
<td>☐</td>
</tr>
<tr>
<td>Editable policies</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>Create custom policies</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Case management/ticketing</td>
<td>☑</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>Blacklisting</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Hardware appliance</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Software/virtual appliance</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

**Verdict**

This is a first-rate product with solid performance and a comprehensive feature set.

**Strengths**

- Easy to configure and use.
- User-friendly interface.
- Effective data leakage prevention.

**Weaknesses**

- Limited support options.
- Expensive pricing.

**SC MAGAZINE RATING**

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

**SC MAGAZINE RATING**

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

**OVERALL RATING**

★★★★★

**Features**

- Pre-configured policies
- Editable policies
- Create custom policies
- Case management/ticketing
- Blacklisting
- Whitelisting
- Hardware appliance
- Software/virtual appliance

**Summary**

The Code Green data leakage prevention tool comes as a purpose-built appliance. It is easy to configure, with a straightforward, benefits significantly from the quick start. Within an hour, we had the appliance online and ready to configure with our exchange servers. The documentation is solid and well-illustrated. Overall, we found that ease of use at this stage could have been improved a bit, but even without network installation wizards, which have become standard practice for most appliances, we hit no show-stoppers. It has excellent configuration menus once the appliance is linked into the network.

It is important, however, that one understands the network and email system thoroughly because it is easy to misconfigure either the appliance or one’s exchange server. Once the appliance was integrated into the network, we began general configuration. The first step addressed the network details, and there is a menu that assists with that.

The appliance performs several functions. The obvious one is watching email leaving the enterprise and stopping messages that violate a policy. Another, and extremely important, is discovering the locations of sensitive data on servers or other computers. This is the inspection service, and enabling it is optional. Once we had the appliance configured, the next step was applying policies. Again, there is an excellent menu for this, and the out-of-the-box policies provided cover a lot of territory. Each policy can be modified. There is a range of workflow options — from “do nothing” through notification to logging. Additionally, one can block the transaction, force it to be encrypted or reroute it.

Besides using policies outside the box or modifying them, one can create new ones. Before writing a new policy, one must register the data that it will affect. The admin sees several classifications of codes, specific patterns file types that can be filtered, and other types of structured data, such as credit card numbers, driver’s licenses, and more. The list is quite complete. Finally, one can include data that the device discovers if that function is turned on.

Essentially, the policy piece of the Code Green device falls under three categories: registered data, discovered data and protected data. Each of these has policies that the administrator can edit and configure to meet specific requirements. The landing page of the menu exudes simplicity. The dashboard contains a good summary of event activity, data usage incidents, discovery incidents and a health monitor that tells the status of the device itself. Each of these major categories allows for appropriate drill-down — logs for recent activity and other details for the rest. The data usage incidents also are tracked graphically as a histogram.

Incidents may be tracked and managed in much the same manner as a help desk incident system. For example, events can be assigned to individual administrators or groups for remediation. There are several preconfigured reports, and one can create custom reports quite easily. Reports can be scheduled and exported as PDF or CSV files. Creating a report is a straightforward, step-by-step process. This is an example of an excellent wizard. In fact, the only configuration or editing function on the Code Green device that are not supported by first-class wizards are those required to initially integrate the device into the network.

We used the standard policies that came with the device, and it catches attempts to defeat it exactly as we anticipated. The device is transparent to users unless it bounces a message. If that happens, the administrator can configure the process of notification. Usually, by default, the message from an Exchange Server goes to the sender. We also had examples of bounced messages where the Exchange Server was not properly configured with the appliance.

Pricing on this device can range widely depending on which version is purchased. Regardless, we find that it is an excellent value. Support requires a contract to access most of the assistance portal, but this is reasonably complete. Varying levels of phone support are available. Access to the assistance portal, in general, requires that the product be registered. Overall, we found the company’s support website to be clean and useful.

We liked this product with its clear, web-based user interface and its intuitive policy configuration and management. There are more than enough choices for that to give the appliance the flexibility and feature set needed in a superior DLP product.
Fidelis XPS

The Fidelis suite is a lot more complicated than some other DLP offerings. It is composed of a combination of appliances that perform different prevention tasks. The configuration we tested consisted of the Command Post, a Direct 1000 Sensor and a Mail Sensor. Each module has specific tasks to perform.

The Command Post is the management system. It controls the other modules, analyzes their data and provides the administrator interface. The Direct 1000 module, a separate appliance, manages email. The Mail Sensor, also a separate appliance, connects the network cables and mousing over a cluster triggers a pop-up with all of the information. This allows tracing a particular type of alert to its source and noting its destination.

The second display type of dashboard is the Information Flow Map. Like the radar display, this is unique. It shows how information flows on the network so it can be traced based on sensors. There are multiple ways to analyze nodes that show up on this display, and one can create rules that are unique to a particularly troublesome endpoint that is generating lots of alerts. Reporting is comprehensive, and there are choices of how reports are created. While reports are built from alerts, they may be put into a PDF, emailed or shown as a trendline. There are a few standard reports the user can customize.

We find that the number of out-of-the-box reports could have been greater. Emails can be quarantined and managed based on criteria in any of the policies. How the system performs depends a bit on how one configures it and its component appliances. However, the offerings, overall are extremely versatile – although it does require a significant understanding of one’s enterprise and what the goals are. It is not, as is typical for this type of tool, simple to set up and deploy. Its documentation and wizards considerably help, however.

Support is obtained only through logging in. There is no publicly available support, which, given the complexity of the system, we find odd. The starting price is reasonable enough, and the products are available as either hardware or virtual appliances. Depending on the configuration, however, the system could get quite pricey.

Once in the network, the admin can move on to the web user interface. Where other DLP devices – as well as many other types of policy-driven tools – talk in terms of policies, the Trustwave product refers to these as “categories.” Policies, in Trustwave-speak, are the actions that one can take when a category is violated.

There are more than 70 out-of-the-box categories ready to go as, or one can edit them easily into new categories. Likewise, it is quite straightforward to create new categories. Categories are adjustable as well. That means that one can set the sensitivity and regulate, to some degree, such things as false positives. The types of characteristics that can be edited in a category include content, protocol, IP address range(s) and email. The whole create/edit process is simple point-and-click. Violations of categories can be sent to either a Trustwave or Arcsight SIEM for further processing and correlation. The DLP monitors all ports and protocols by default, so if a violation occurs on a non-standard port – will be identified. There are, therefore, few false positives that surface when identifying numbers with a special calculation because the tools verifies the calculation, not just the format. Another useful feature is the capability to understand foreign languages. Trustwave has linguists on its team, so if a language other than English or Spanish is required, the company likely has the support needed. We were especially impressed by the neat arrangement of the dashboard. Drill-downs are intuitive, and there is a lot of summation in the information. Reporting is comprehensive and covers most regulatory requirements. Graphics are clear and appropriate, and there are 30 to 40 premade reports available out of the box. However, creating new reports is simple, so the richness of functionality is a big plus. Because the product provides sound correlation capabilities, violations can be grouped and timelines established. Thus, Trustwave DLP becomes a first-rate investigative tool.

Vendor: Fidelis Security Systems
Price: $25,000
Contact: www.fidelissecurity.com

Trustwave DLP

Occasionally we see a product that anticipates all of our questions and offers the right answers and solutions to all of the challenges that we had ready to throw at it. It doesn’t happen often, but it certainly happened in this case. The Trustwave DLP is, hands down, the best thought-out DLP product we have seen.

This tool is available either as a hardware or software appliance. The hardware version has a nice twist on the installation challenges we have seen from appliances in the past: forcing the administrator to install into the network from the command line. With this product, one tells Trustwave about the IP addressing, and the appliance comes configured. Once racked up, the admin connects the network cables and powers it up. The appliance does the rest. This was typical of the thoughtfulness we observed in the design and implementation of the solution.

Once in the network, the admin can move on to the web user interface. Where other DLP devices – as well as many other types of policy-driven tools – talk in terms of policies, the Trustwave product refers to these as “categories.” Policies, in Trustwave-speak, are the actions that one can take when a category is violated.

There are more than 70 out-of-the-box categories ready to go as, or one can edit them easily into new categories. Likewise, it is quite straightforward to create new categories. Categories are adjustable as well. That means that one can set the sensitivity and regulate, to some degree, such things as false positives. The types of characteristics that can be edited in a category include content, protocol, IP address range(s) and email. The whole create/edit process is simple point-and-click. Violations of categories can be sent to either a Trustwave or Arcsight SIEM for further processing and correlation. The DLP monitors all ports and protocols by default, so if a violation occurs on a non-standard port – will be identified. There are, therefore, few false positives that surface when identifying numbers with a special calculation because the tools verifies the calculation, not just the format. Another useful feature is the capability to understand foreign languages. Trustwave has linguists on its team, so if a language other than English or Spanish is required, the company likely has the support needed. We were especially impressed by the neat arrangement of the dashboard. Drill-downs are intuitive, and there is a lot of summation in the information. Reporting is comprehensive and covers most regulatory requirements. Graphics are clear and appropriate, and there are 30 to 40 premade reports available out of the box. However, creating new reports is simple, so the richness of functionality is a big plus. Because the product provides sound correlation capabilities, violations can be grouped and timelines established. Thus, Trustwave DLP becomes a first-rate investigative tool.

Vendor: Trustwave
Price: $10,000
Contact: www.trustwave.com

SC MAGAZINE RATING
Features ✽✽✽✽✽
Performance ✽✽✽✽✽
Ease of use ✽✽✽✽✽
Documentation ✽✽✽✽✽
Support ✽✽✽✽✽
Value for money ✽✽✽✽✽
OVERALL RATING ✽✽✽✽✽

Features

Performance
Ease of use
Documentation
Support
Value for money

Strengt

This product knocked us out with its ease of use, solid performanc...
Cloud: A risk/reward proposition

Still, the benefits are pretty impressive. The cloud provides enterprises with the elasticity and flexibility to access IT services they need during peak periods, without investing heavily in hardware that is only needed sporadically or seasonally. As quicker and more effective and efficient applications arrive in the enterprise, cloud providers are often better equipped to handle that transition. Providers also can achieve better economics of scale across their customer base, while keeping pace with the latest technology innovations.

Yet, the cloud has its dark side. In today’s environment of hacker attacks, phishing expeditions and downright nasty malware, risk management is at the forefront of any enterprise cloud computing implementation. The idea of an enterprise’s data being outside of its complete control may be a difficult concept for decision-makers to overcome.

That’s why smart companies assess what level of risk is acceptable to their businesses, and then determine which cloud approach is best — public, private or hybrid.

For some companies, a public cloud strategy may be the best idea, enabling them to get out of the IT bits and bytes business altogether and have a third-party vendor handle all of their infrastructure needs. Other companies, concerned with regulatory issues such as Sarbanes-Oxley and HIPAA in the United States and the Data Protection Act in Canada — may opt for a private cloud approach.

However, many may prefer a hybrid course. This places fewer mission-critical applications in a public cloud, as those that offer a competitive advantage or require higher security needs can be placed in a private cloud environment — all with a common “cloud management umbrella” so the customer has greater visibility and monitoring capabilities. It may also include keeping some legacy applications running where they are.

Companies also must address the unique needs of their data-centric security models. As part of defining optimal workload placement, they must examine the individual elements that comprise information within the enterprise. Doing so enables them to address the key security, visibility and compliance issues an enterprise should consider during cloud migration. It is also critical to classify the types of data that should be placed in the cloud, as well as how to structure the assets’ lifecycle management process to maximize the benefits of the cloud.

The cloud is not going away — even with the concerns about security, visibility and compliance. Yet, the ISACA survey found the percentage of respondents whose organizations now use the cloud has spiked from 16 percent in 2010 to 26 percent in 2011. The trend to increase use of some form of a cloud delivery model is expected to accelerate into 2012 and beyond.

Cloud computing obviously will continue to grow as enterprises look to gain cost, flexibility and efficiency advantages. The companies which are best able to balance the risks with the benefits are the ones which will be able to leverage their IT resources as a competitive advantage in today’s downturned economy.

Siobhan Byron is president of Forrester Technology Canada, an IT infrastructure integrator.

Companies must address the unique needs of their data-centric security models.”
Our business is to secure your business.

ESET NOD32 Antivirus 4
Fast, Effective, Proactive, Antivirus and Antispyware

Our award-winning ESET NOD32 Antivirus is the faster, smarter, easier-to-manage defense against Internet threats and the only anti-malware solution with ICSA certification for both Windows and Mac OS. With a unified management console that scales to support small and large business networks, ESET NOD32 delivers advanced proactive protection for all your Windows, Mac and Linux endpoints.

Call or visit us online: 866-343-3738  www.eset.com