Online account fraud remains prevalent, but all banks can strive to prevent it, says Rudy Wolfs of ING Direct P18

Jumping new hurdles
Security concerns in Canada are getting attention as new technologies and advanced threats emerge PC1

Life after Stuxnet
A cyberattack on nuclear facilities upped the ante for those in charge of critical infrastructure P29
REGULARS
4 Editorial Are you ready for action?
8 Threat report A cyberattack targeting Canada ministries has been traced back to China
10 Threat stats Considerable growth in use of Cascading Style Sheets to spread malware
12 Update A massive email hack has hit customers of Canadian retailers and service providers
13 Debate Congress should pass a law that prohibits the tracking of a consumer’s online behavior
14 Two minutes on... Vendors and cyber offense
15 Skills in demand Pros needed who understand the impact of cloud technology on security
16 Opinion Protecting data on copiers, by Larry Kovnat, Xerox
17 From the CISO’s desk No silver bullet for PCI compliance, says Eduardo Perez, chairman, PCI Security Standards Council
32 Letters From the online mailbag
49 Calendar A guide to upcoming courses, shows and IT security events
50 Last word Are you prepared for a breach? by Richard Blumberg and Gary Kibel

FEATURES
18 Digital stick-up Online account fraud remains prevalent, but all banks can strive to prevent it, says Rudy Wolfs of ING Direct.
24 The envelope, please The winners of the prestigious 2011 SC Awards U.S. were announced on Feb. 15 in San Francisco.
26 Scaled down, armored up For many small and midsize businesses, neglecting safeguards is a thing of the past.
29 Life after Stuxnet The cyberattack on Iran’s nuclear facilities has upped the ante for those in charge of critical infrastructure.

PRODUCT REVIEWS
33 Products section UTMs and anti-malware gateways often are our key protection at the perimeter
34 Group Test 1: Anti-malware gateways A strong solution can stop email and web-based threats before ever making it inside the environment
40 Group Test 2: UTM The ability to distribute protection across a large enterprise is critical
48 First Look: IronKey This tool provides an assured, secure online account connection for commercial banking customers

HACKERS ARE DISGUISED
...and their intrusions can seriously damage a company’s reputation and bottom line. Look at the cyberactivist group Anonymous, which masterminded recent DDoS attacks on PayPal, MasterCard and Visa, and published on the internet tens of thousands of HBGary Federal’s internal email messages, defaced its website and hijacked the Twitter account of its CEO.

Attend SC Congress Canada to discover the motivation and objective of different types of hackers – whether it’s revenge, intellectual property or financial data – so you can defend against them. Hear real-world practitioners discuss what can be learned from recent high-profile attacks and other pressing topics.

Whether you work for the government, a financial institution, the health care industry or anywhere else where your and your customers’ data is critical to business, SC Congress Canada is the place to find answers, talk with experts and discover ideas that will address your security challenges.

Are you ready for some action?

W e’ve all heard the calls countless times for the federal government and private industry to work together more closely to improve information security across both sectors. Too often, these entreaties – some of which have been well thought out and supported by numerous groups and industry luminaries – either have been completely ignored or only half-heartedly taken up to any great effect. So, yet another appeal recently made by industry groups should come as no surprise.

The Business Software Alliance, the Center for Democracy & Technology, the Internet Security Alliance, TechAmerica and the U.S. Chamber of Commerce released their plea for stronger IT security planning in the form of a white paper. Having been in the works for six months, the paper offers up a slew of recommendations to strengthen cybersecurity across the board. It touches on everything from creating and implementing a “National Cybersecurity Research and Development Plan” and establishing policies that would help “boost the number” of IT-related college grads to establishing processes that engage the international community to collaborate and develop standards on “issues of global concern.”

It is a considerable and even inspiring inventory of recommendations. Mighty ambitious, too, considering that while it provides some meat on a few of the suggestions’ bones, the to-do list offers scant real details about execution. These, undoubtedly, will be left to the collaboration involving other important partners as implied in the paper.

But, exactly how will they work together? And when? Hasn’t that been the problem all along? Despite the lip service given to this nebulous partnership concept over the years, what really has seen the light of day?

Other groups have released similar suggestions, too, and, yes, such dialogue among various organizations is great to see. But, don’t we seem to have an awful lot of recommendations already floating around? When are we going to see something actually happen as a result of them? Sans real collaboration with the U.S. executive office and maybe Congress or some other agencies, we’ll continue discussing theory after theory of how we can strengthen cybersecurity together with still little to show for it.

And, as internet-borne bombs are lobbed at both public and private entities, more talk is exactly what we could do without.

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

THIS MONTH

SC WORLD CONGRESS
24 7

SC WORLD CONGRESS eSymposium
April 26: Cyberespionage
The threat of critical information shows that attackers – state-sponsored or not – are entailing whatever weaknesses exist in systems they can siphon off corporate and government data, often going unnoticed for months. Experts share background on the types of attacks to watch out for and what to do to thwart them.

UPCOMING
May 26: Cyberwarfare: What’s it mean to you.
The U.S. Department of Defense recently noted in its annual report to Congress that China was focusing on ‘eliciting’ information for ‘strategic or military utility.’ How can private companies work with the government to help diminish the effect of attacks and what can they do internally to bolster their own piece of the country’s critical infrastructure? We examine the trends and look at solutions.

June 16: Auditing & compliance
What are some of the issues to be mindful of to ensure you get through audits successfully, what types of technologies can support these efforts, and what can information security officers do to better work with their auditors to ensure their plans and practices are unreviewed?

FOR MORE INFO
For information on SCWC 24/7 events, please contact Natasha Mulla at Natasha.mulla@haymarketmedia.com. For sponsorship opportunities, please contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit, www.scmagazineus.com/scwc247.

World’s who at SC Magazine

WHO’S WHO AT SC MAGAZINE

EDITOR

EDITOR IN-CHIEF Ilana Armstrong
ilana.armstrong@haymarketmedia.com

EXECUTIVE EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com

MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

REPORTER Angela Moscaritolo
angela.moscaritolo@haymarketmedia.com

TECHNOLOGY EDITOR Peter Stophonos
peter.stophonos@haymarketmedia.com

DIRECTOR OF SC LAB OPERATIONS John Atilan
john.atilan@haymarketmedia.com

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

PROGRAM DIRECTOR, SC WORLD CONGRESS
Eric Green arn.green@haymarketmedia.com

CONTRIBUTORS
Deb Raeford, Beth Schultz, Stephen Lawton

DESIGN AND PRODUCTION

ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com

VP OF PRODUCTION & MANUFACTURING
Louise Marrin
louise.marrin@haymarketmedia.com

SENIOR PRINT AND DIGITAL CONTROLLER
Krissi Vartanian
krisi.vartanian@haymarketmedia.com

SEVEN

SENIOR EVENTS MANAGER Natasha Mulla
natasha.mulla@haymarketmedia.com

EVENTS COORDINATOR Anthony Curry
anthony.curry@haymarketmedia.com

Kris Lovejoy, vice president of IT risk, office of the CEO, IBM

Tim Mathew, board member, Cloud Security Alliance

Stephen Northcutt, president, SANS Technology Institute

Randy Sanovic, former general director, information security, General Motors

Howard Schmidt, cybersecurity coordinator, White House; president and chief executive officer, Information Security Forum

Justin Somaini, chief information security officer, Symantec; former director of information security, VeriSign

Craig Spiezle, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft

W. Lord Tipton, executive director, (ISC)²; former CIO, U.S. Department of the Interior

Amit Yoran, chief executive officer, Neustar; former director, Department of Homeland Security’s National Cyber Security Division

Seeings is believing...
Find out why this award-winning technology is so highly rated by reviewers and loved by customers.

Real-Time Log Analysis for Proactive Network Defense

Logs have to be analyzed. Regulations such as PCI, HIPAA, NERC CIP, SOX and GLBA require it, but let’s face it - traditional log analysis is reactive. You have a choice: You can pick a product that is forensically focused: gathering logs, storing them in a database and offering search and reporting, or you can choose TriGeo SIM.

TriGeo SIM is the ONLY log analysis solution that combines real-time log analysis with active response for true Proactive Network Defense.

Real-time, in-memory analysis is the key. TriGeo’s enterprise-wide view of the network makes it possible to capture, correlate and actively respond to network attacks and insider threats - at network speed.

For proactive network defense, there is only one choice.
Threat Report
Cybercriminal activity across the globe, plus a roundup of security-related news

Netherlands top producer of zombie IP addresses
During the past month, the EMEA region (Europe, Middle East, Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, 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

Source: Symantec

DataBank

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

MINNEAPOLIS – A Texas man who pleaded guilty to stealing $275,000 from a Minnesota e-commerce company also admitted to hacking into networks at NASA. Jeremy Parker, 26, was not officially charged with the NASA intrusion, but the activity will be factored into his sentencing.

LOS ANGELES – Disney employees filed a class-action lawsuit claiming employee identification cards are encoded with Social Security numbers, which violates California law and puts workers at risk of ID theft. A Disneyland spokeswoman said the company is working to improve the safety of the cards.

EL PASO, TEXAS – The El Paso Independent School District website was defaced with a vulgar, animated image and a message reading “Owned by TheSlayer.” Following the intrusion, the site was offline for 12 hours while staff removed the message.

NEW YORK – The Health and Hospitals Corp. (HHC), the city’s municipal hospital system, has begun notifying 1.7 million individuals their personal information was breached. The data was stolen from the truck of HHC’s record management services vendor.

OTTAWA, CANADA – A cyberattack targeting Canada’s treasury board and finance department was traced back to IP addresses in China. The hackers, who tried to access classified government information, used spear phishing to infect computers.

POLAND – Customers of the bank ING were targeted by a new version of the Zeus trojan. Attackers steal an infected user’s cell phone number when they enter it at the bank site. The attackers then send that number an SMS message that directs users to install a malicious mobile app that hijacks all future SMS messages, including one-time passcodes used to access online accounts.

RUSSIA – Evgeny Anikin was sentenced to five years in prison after admitting his role in the hack of RBS WorldPay, based in Atlanta in the United States. He was part of a gang that compromised prepaid payroll accounts, create bogus cards and withdraw more than $9 million in less than 12 hours from 2,100 cash machines worldwide.

FRANCE – The French Ministry confirmed that its systems in December sustained a massive attack by hackers, possibly from China, wishing to steal documents related to the G20 economic summit. The intruders spied on some 150 computers and may have gained access through socially engineered emails.

SRI LANKA – Though the physical conflict between the island’s military and the insurgent Liberation Tigers of Tamil Eelam (LTTE) ended in 2009 after 30 years, a cyberwar continues. LTTE supporters continue to bombard the Army website, and a commander warned of attacks going after sensitive data.

AUSTRALIA – The government-hosted security systems of the Australian Capital Territory (ACT) fought off nearly 650,000 cyberattacks in 2009-10. Jon Stanhope, chief minister and minister for territory and municipal services, credited a layered defense with protecting 98 ACT-hosted websites.
A new method for spreading malware using Cascading Style Sheets (CSS) that contain partial data for script downloaders, a new method for spreading malware that makes it much harder for many anti-virus solutions to detect malicious scripts. This method is currently being used in the majority of drive-by download attacks and allows cybercriminals to install exploits to users’ machines without them being detected. Source: Kaspersky Lab

### Top 10 malicious programs You’re Kido

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Change</th>
<th>Previous month’s rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Net-Worm.Win32.Kido.ir</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Virus.Win32.Sality.za</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>HackTool.Win32.Kiser.zw</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>Net-Worm.Win32.Kido.js</td>
<td>-1</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Virus.Win32.Sality.bh</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Hoax.Win32.Screensaver.b</td>
<td>-2</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>AdWare.Win32.HotBar.dh</td>
<td>-2</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>Virus.Win32.Win32</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>Trojan.JS.Agent.bhr</td>
<td>-3</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>HackTool.Win32.Kiser.js</td>
<td>1</td>
<td>11</td>
</tr>
</tbody>
</table>

February saw considerable growth in the use of Cascading Style Sheets (CSS) that contain partial data for script downloaders, a new method for spreading malware that makes it much harder for many anti-virus solutions to detect malicious scripts. This method is currently being used in the majority of drive-by download attacks and allows cybercriminals to install exploits to users’ machines without them being detected. Source: Kaspersky Lab

### Top 10 spyware threats Win32 still tops

<table>
<thead>
<tr>
<th>Threat name</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan.Win32.Generic!BT</td>
<td>22.97%</td>
</tr>
<tr>
<td>Trojan-Spy.Win32.Zbot.gen</td>
<td>3.46%</td>
</tr>
<tr>
<td>Trojan.Win32.Generic.pak!cobra</td>
<td>2.89%</td>
</tr>
<tr>
<td>Zugo LTD (v)</td>
<td>2.52%</td>
</tr>
<tr>
<td>Fraudtool.Win32.Securityshield.exe (v)</td>
<td>2%</td>
</tr>
<tr>
<td>Trojan.Win32.Generic!SB.0</td>
<td>1.72%</td>
</tr>
<tr>
<td>INF.Autorun (v)</td>
<td>1.66%</td>
</tr>
<tr>
<td>Worm.Win32.Downad.Gen (v)</td>
<td>1.48%</td>
</tr>
<tr>
<td>Pinball Corporation (v)</td>
<td>1.19%</td>
</tr>
<tr>
<td>Exploit.PDF-JS.Gen (v)</td>
<td>0.83%</td>
</tr>
</tbody>
</table>

The majority of these threats reported last month propagate through stealth installations or social engineering. Source: Source: Fortinet Threatscape Report

### Top breaches of the month Data loss

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacoby Medical Center (New York)</td>
<td>Backup tapes</td>
<td>1.7 million</td>
</tr>
<tr>
<td>Cambridge Who’s Who Publishing (Uniondale, N.Y.)</td>
<td>Data tapes with customer information were misplaced during the shipping process.</td>
<td>400,000</td>
</tr>
<tr>
<td>Broken Arrow Med. Center (Broken Arrow, Okla.)</td>
<td>A computer with patient information not used since May 2004 was stolen from a secured information systems room.</td>
<td>84,000</td>
</tr>
</tbody>
</table>

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

515,002,269 (as of March 11)

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

Phishing attacks worldwide increased 11 percent through February. The numbers represent the first time in nearly a year where the count of phishing attacks broke the 18,000 mark. The most popular method with phishers is the use of hacked websites to host attacks. When their ploys are shut down, phishers lose nothing since they paid nothing to host the attacks in the first place.

Received spam Top five spam regions

<table>
<thead>
<tr>
<th>Country</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>12.59%</td>
</tr>
<tr>
<td>Japan</td>
<td>9.14%</td>
</tr>
<tr>
<td>France</td>
<td>5.45%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>3.53%</td>
</tr>
<tr>
<td>Italy</td>
<td>3.21%</td>
</tr>
</tbody>
</table>

The rate indicates the accumulated emails lagged as spam. Source: Source: Fortinet Threatscape Report

### Spam rate Compared to global email

<table>
<thead>
<tr>
<th>1/21/11</th>
<th>1/28/11</th>
<th>2/18/11</th>
<th>2/4/11</th>
<th>2/11/11</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>30%</td>
<td>40%</td>
<td>50%</td>
<td>60%</td>
</tr>
</tbody>
</table>

The rate indicates the accumulated emails tagged as spam. Source: Source: Fortinet Threatscape Report

### Zombie IPs Global distribution

<table>
<thead>
<tr>
<th>Country</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>14.7%</td>
</tr>
<tr>
<td>Brazil</td>
<td>9.7%</td>
</tr>
<tr>
<td>Other Europe</td>
<td>13.6%</td>
</tr>
<tr>
<td>Other Asia</td>
<td>21.4%</td>
</tr>
<tr>
<td>Russia Federation</td>
<td>8.6%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>2.6%</td>
</tr>
<tr>
<td>Italy</td>
<td>2.6%</td>
</tr>
<tr>
<td>China</td>
<td>3.7%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>4%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>6.4%</td>
</tr>
</tbody>
</table>

The biggest increases in month-over-month zombie activity occurred in “other” Asian and South American nations, while the largest decreases occurred in Brazil and Russia. Source: Commtouch Software Online Labs

### Phishing All-time high

Phishing attacks worldwide increased 11 percent through February. The numbers represent the first time in nearly a year where the count of phishing attacks broke the 18,000 mark. The most popular method with phishers is the use of hacked websites to host attacks. When their ploys are shut down, phishers lose nothing since they paid nothing to host the attacks in the first place.
The massive email hack that compromised records at email marketing services provider Epsilon hit customers of Canadian retailers and service providers. Customers of Tivo, Best Buy and the Air Miles rewards program were informed that their email addresses had been compromised. Dallas-based Epsilon, a permissions-based marketing company that sends 40 billion emails each year, revealed in April that someone had gained access to its internal systems. It later updated the statement, adding that only two percent of the email addresses it holds had been compromised.

For the second time in three years, legislation to bring Canada’s copyright law into the digital age has fallen victim to parliamentary paralysis. In March, the controversial Bill C-32 died when Prime Minister Stephen Harper’s government was defeated in a parliamentary confidence motion. Along with the bill died federal Industry Minister Tony Clement’s attempt to make individual Canadians liable for fines up to $5,000 for breaking the digital laws that protect music, movies or software. The legislation had drawn fire from organizations like the Canadian Association of University Teachers (CAUT), which argued that imposing fines on access to digital material online would “lock down vast amounts of material, effectively preventing its use for research, education and innovation.”

Health Canada inadvertently sent the private information of two individuals to a Toronto resident last month in a security gaffe. Thirty-three-year-old Kyle Andrews, a user of medical marijuana, had contacted the government department asking for guidelines on the suggested use of the drug. Health Canada sent him the Marijuana Medical Access Regulations in the envelope. They contained private information on other Canadian residents who also used cannabis for medical reasons.

Along with other critical infrastructures, Canada’s telecommunications networks are vulnerable to homegrown terrorists and radical Islamist ideologues. That was the conclusion of the Special Senate Committee on Anti-terrorism, in its third report.

Shamed by Sen. Hugh Segal, the committee cited the Chinese-based cyberattacks against the Department of Finance and Treasury Board of Canada Secretariat, uncovered earlier this year, to point out that response to earlier threats has been “too slow and [hampered by a] lack of resources.”

The second annual SC Congress Canada will be held at the Metro Toronto Convention Centre on June 14 and 15. Confirmed speakers for the gathering of security pros, include Ann Cavoukian, information and privacy commissioner of Ontario; Rafal Rohozinski, senior fellow at the Munk School of Global Affairs; and Bobby Singh, director of information security at Rogers Communications. For more information, visit www.sccongresscanada.com.

What is your view of HBGary Federal?

FOR

AGAINST

Debate Congress should pass a law that prohibits the tracking of a consumer’s online behavior.

Ever heard of Bightsy, Lotame or 33Across? Odds are they’ve heard of you — and your browsing history. Web tracking is as pervasive as it is unpopular. Many ad networks, data aggregators and analytics providers recognize users should have privacy choices. The question is: What should those user privacy choices look like? Here’s a minimal set of criteria: A choice mechanism should enable a user to opt out of data collection, apply to all trackers and be user-friendly. And here’s how industry-proposed solutions stack up: Users can only opt out of tracking-targeted advertising, not tracking itself. The most comprehensive opt-out mechanism covers a small proportion of trackers. And to discover that mechanism, users must navigate a counterintuitive website. It should come as no surprise that trackers can’t develop a meaningful choice mechanism. Web tracking cuts across numerous industries, each packed with firms that have different business models, incentives and cultures. Congress and the FTC must step in to protect user privacy.

How does it work? Anonymous boldly took direct action against corporations and persons deemed a threat to their cause. This public demonstration has resulted in an even stronger resolve and willingness to perform criminal acts in the support of their ideals. Any person, organization, company or government may be targeted. Now the group is recruiting exploit and skills to support their hacking activities.

How can I prevent it? In many ways the Anonymous movement is a digital manifestation of mob mentality. The “success” that Anonymous has enjoyed will only feed the allure recently created. We can expect hacktivist movements will continue to gain momentum and further support. We must act now to educate our employees and our leaders of this powerful threat.

Do not hallucinate.
As the fallout continues from the compromise of HBGary Federal and the subsequent publishing of tens of thousands of its emails by hacker group Anonymous, some in the security industry are embarrassed over revelations that the malware forensic firm was engaged in shady, potentially illegal activities.

The saga has brought to light a potentially uncomfortable reality: that legitimate security companies, presumably created to protect innocent users from the dangers of the internet, may be using their firepower to win big contracts and attack others, even their peers.

Of particular concern is the discovery that HBGary Federal and two other security firms were in negotiations with a major law firm, believed to represent Bank of America, to launch an offensive against the whistleblower site WikiLeaks and its supporters.

Late last year, WikiLeaks founder Julian Assange hinted that his organization is sitting on a treasure trove of documents that point to corruption at a major U.S. bank (purportedly Bank of America) and a leaked PowerPoint deck seems to suggest that HBGary Federal, Palantir Technologies and Berico Technologies were hired to hack WikiLeaks’ central server and spread false documents as a way to discredit the whistleblower site.

The stolen emails also disclosed a proposal on behalf of the U.S. Chamber of Commerce to undermine its left-leaning adversaries. “From a government-policy standpoint, heads should roll on that one, if it’s true,” said Jeremiah Grossman, founder and CTO of web application security firm WhiteHat Security. “Our government contracting with people to target citizens? That should not be allowed.”

Since this plot has been unearried, many in the vendor community have attempted to distance themselves from HBGary Federal and its sister company HBGary, said Chenxi Wang, principal analyst at Forrester Research. “People are worried about what security companies are doing behind closed doors,” Wang said.

Grossman, who founded WhiteHat Security in 2001, said he doesn’t think the industry suffers from a systemic problem. “I couldn’t name another company that engages in that – a coordinated effort to hack another entity,” he said. “Not to say it’s not happening, but we don’t know of it.”

Wang, however, said she has heard vendors express concern over the threat of attacks from competitors. “I would tend to think that these kind of offensive tactics are employed more often than we know,” she said. – Angela Moscaritolo

### Vendors and cyber offense

**Ron Woerner**, director of cybersecurity studies, College of Information Technology, Bellevue University

**How do you describe your job to average people?**

Not only do I help protect my organization (a university), but I also teach students about the security profession. There are so many aspects to information security that it’s a challenge to determine what’s critical for them to know in order to succeed. It’s quite similar to security awareness training where there’s only a finite amount of time and attention you need to make the most of it.

**Why did you get into IT security?**

Like many, I fell into security. As a military intelligence officer, I learned about data classification and safeguarding sensitive information. As a UNIX systems administrator, I learned how to apply controls to protect the systems and its data. As a junior security analyst, I learned the importance of policies and awareness. The variety of activities required of a security professional is what keeps me interested. That and the many great people I’ve gotten to know in the security field.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.

**What was one of your biggest challenges?**

Security is often a constant battle, not only against the “bad guys” but also with management who may not “get” security as well as end-users who bypass controls for their own convenience.

**What keeps you up at night?**

After 20 years, [computer science professor Eugene Spafford] Spafford’s Law of Security is alive and well. “If you have responsibility for security, but no authority to make changes, then you’re just there to take the blame when something goes wrong.”

**For what would you use a magic IT security wand?**

It would be used to influence those who take undue risks without understanding the consequences. All security pros need the ability to lead those around them to develop and implement controls to assure protection. The technology is easy compared to having this ability. The support of other security pros is what keeps me jacked.
Overcoming new threats

Businesses today need a holistic approach to security that focuses on moving from threat detection to prevention. To overcome the next generation of threat vectors, organizations should consider preventing the proliferation of new threat vectors that impact enterprise security from the gateway to the endpoint. However, as companies combat traditional security threats, businesses also face a new generation of vectors with the proliferation of Web 2.0 applications, mobile computing and custom attacks that are dramatically increasing security complexity for enterprises.

Therefore, it is vital to integrate more user awareness. Employees are essential to helping organizations mitigate risks in the enterprise. Businesses will benefit from implementing technologies that combine stronger security and more user awareness.

Another necessity is securing the virtual environment. Virtualization, like every new technology, can present new risks to companies. Improper implementation of security for virtual environments can adversely affect an organization, exposing it to new threats. Therefore, implementing the proper architecture in a virtual environment can protect against both internal and external threats.

Organizations are using an average of nine different vendors to secure their infrastructure, often creating greater management complexity: Trying to piece together too many disparate point products can leave systems vulnerable. Before adding another point product to the environment, consider which solutions can evolve as the business grows and new threats arise.

Organizations of all sizes have different security needs and priorities, and are looking for flexible solutions that enable them to create their own portfolios. It is important to help enterprises build an extensible infrastructure that provides security against the wide array of attack methods – and can evolve with an organization’s future needs. This ultimately provides organizations with protection for the next generation of threat vectors, before they impact the business.

Protecting data on copiers

Recent news reports on copier security have brought to the forefront how information stored on a copier’s hard drive may be accessible to would-be identity thieves and others. While this vulnerability is eye-opening to many, this concern has been important to manufacturers for quite some time. Just as you would install a virus scan on your laptop or PC, you need data safeguards for multifunction printers (MFPs).

What features and tools will help to protect the information flowing through MFPs? IT administrators and users should work with their vendor to make sure their security features are enabled – for example, Image Overwrite electronically “shreds” information stored on the hard disk(s) of MFPs as part of routine job processing. Network authentication and authorization allows admins to restrict access by verifying network usernames and passwords in network directories prior to use. Encryption is also built into many MFPs to make sure data stored within a device is protected. MFPs even have features that protect information from hard copy theft. With secure print, jobs are safely stored at the MFP until the owner enters a personal number to release them.

When purchasing a new MFP, choose a vendor that offers options for removal of the hard drive before the MFP is disposed of or turned in after a lease. Additionally, it is important to keep in mind that with new threats developing on a daily basis, there will always be a need to update the software that runs your copiers. Responsible MFP manufacturers make new patches available for their customers to easily download, through a website or even RSS feed, so machines can easily be updated with the latest protection.

MFPs are valuable tools that streamline business processes and share information. By taking advantage of the available options, users can reap these benefits while IT administrators ensure their company’s information is secure.

Opinion

Eduardo Perez, chairman, PCI Security Standards Council

In 2010, the PCI Security Standards Council released new versions of the three standards we manage: the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA DSS). We also kicked off our new three-year lifecycle for the future development of these standards. All around the world, organizations are moving toward the adoption of the updated standards so that they can begin 2012 with a solid footing against the newest iterations. As evidence of the maturity of these security standards, the vast majority of the enhancements were focused on providing further clarification on the application of existing requirements.

As we enter this critical implementation phase of our security journey, there are a few items I’d like you to keep in mind:

Technology is just a part of the solution. We live in an exciting time of innovation and continually evolving technologies. For the payment security world, cardholder this means increasing focus on the promise of technologies (like encryption and tokenization) designed to help reduce the card data environment (CDE) within an organization and help control where the data resides.

The council recognizes the potential of these technologies for simplifying the process of PCI DSS compliance for organizations and understands the market appetite for information on how to take advantage of them.

It is important to remember, however, that there is no silver bullet when it comes to security. Addressing and developing both people and processes, in addition to technology, is critical to a security strategy that is not just successful but maintainable.

People and processes continue to be the key to implementing a strong security strategy.

No silver bullet for PCI compliance

Technology can only go so far to protect you, but having these other two elements in place will go a long way in helping you stay secure.

Regardless of the type of technologies you have put in place, you can’t ignore one critical aspect of this process: If you don’t need the data – don’t store it.

Consider the benefits of two processes highlighted in the recent changes to the DSS 2.0 – scoping and logging. The clarifications around scoping reinforce the need for a process that identifies and documents all locations and flows of cardholder data to ensure accurate scoping of the CDE. This process helps you better understand where the data resides, allowing you to protect that segment more effectively.

We hope you will support the PCI Security Standards Council by sharing feedback about your company’s implementation journey. Visit the website at www.pcisecuritystandards.org.

Photo by Bob Adler

From the CSO’s desk

Photo by Scott Adler

You need data safeguards for multifunction printers.”

You need data safeguards for multifunction printers.”

“ Don’t need it, toss it

PCI compliant technologies can store and properly protect certain data, such as the primary account number (PAN), but if you don’t have a business use for this data – get rid of it.

Facilitating the process

The council provides education for all stakeholders across the payment chain. We have expanded that arm to facilitate the process of compliance and securing payment card data.

Call for input

Participate in the process by offering feedback. Join us in training sessions to become better educated on the standards and get in touch with us along the way with comments.

Visit the website

The revamped council website – with a centralized documents library – makes it simpler to find what you’re looking for and is presented in a language you can easily understand.
Online account fraud remains prevalent, but all banks can strive to prevent it, says Rudy Wolfs of ING Direct. Dan Kaplan reports.

Assume the desktop is compromised and deliver a multilayered approach that not only protects against one type of attack but also protects against the next type of attack that criminals can come up with,” Wolfs adds.

Target: Small business

Most of today’s sophisticated banking trojans employ a “man-in-the-browser” method, which renders traditional security controls offered by financial institutions, such as SSL and multifactor authentication, practically useless.

“None of the old controls work,” says Avivah Litan, vice president and distinguished analyst at Gartner. “It looks like a legitimate user inside the browser application. It’s not piercing through the outside. It’s on the inside.”

Some of the latest iterations of Zeus, which recently merged code bases with SpyEye, are so advanced that they may send shivers down the spine of even the most hardened cybercrime fighter. One new variant targeting U.S. customers, security firm Trusteer recently revealed, actually has the ability to keep online account sessions open after customers believe they have logged off.

And Zeus isn’t the only kid on the block. In March, Symantec researchers...
warned of the Tatanarg trojan, which can modify HTML in the browser and, in an apparent slight to competing malware writers, is coded to find and eradicative variants of the Zeus trojan that may be running on an infected machine. Litan says customers belonging to banks of all sizes are being targeted by this style of attack.

But because commercial account takeover typically affects small and midsize businesses because they have fewer controls in place, much of the stolen money is being drained from community banks, experts say. It makes sense, too, considering many mom-and-pop organizations prefer to do businesses with financial institutions of similar sizes.

Dave Jevans, chairman of IronKey, a Sunnyvale-Calif. maker of financial malware protection products, says smaller banks are capable of defending their borders against attack, but they often fall short at defending against threats targeting the end-user.

“The real problem is what we see meaningful losses is at the smaller financial institutions,” Jevans says. “They don’t have the security infrastructure and teams that the big banks have. They often outsource a lot of their IT and online banking activities. They don’t have a lot of direct control and they haven’t invested in a lot of the security technology that the big guys have.”

But Carey Whaley, vice president of payments and technology policy at the Independent Community Bankers of America, says a recent survey his trade association conducted of some 800 community banks revealed that just five percent suffered a monetary loss due to corporate account takeover.

“It’s a handful of banks right now,” Whaley says. “It’s not an epidemic. (But) is it on our community banks’ radar screens? Absolutely. Are they battening down the hatches? Absolutely.”

Pending FFIEC guidelines

But just what type of security controls must banks offer? When the FFIEC, in 2005, released its report, Authentication in an Internet Banking Environment, phishing was the scourge of the internet. The federal guidance, among promulgating other risk-based measures, mandated that banks adopt multifactor authentication.

“The real problem, as with any problem, commercial account takeover has become the No. 1 fraud concern of banks,” Litan says. Not surprisingly, then, the next iteration of FFIEC guidance, due out soon, lays out expectations that seek to trigger reforms to today’s most pressing concerns. A draft of the guidance briefly was posted in December on the National Credit Union Administration website.

“Since virtually every authentication technique can be compromised, financial institutions should not rely on any one authentication method or security technique in authorizing high-risk transactions, but rather institute a system of layered security,” according to the leaked version of the guidance.

Among other measures, the guidance requires banks to have a comprehensive security program that detects and responds to suspicious activity, something credit card companies already widely practice.

But Litan says some of the other proposed requirements, including device identification and challenge questions, are not effective against advanced malware.

“They’re recommending things that have been beaten already,” Litan says. “But in their defense, some of the banks want more specificity. They don’t want the FFIEC to give broad principles.”

Nowadays, while phishing is the problem, commercial account takeover now involves the fraudulent use of accounts to steal money. Small and midsize banks of any size are pretty significant,” Silver Tail’s Litan says. “It’s random questions and there’s also trick questions in there. There are questions we expect people to say ‘none of the above.’ There is enough variety and randomness to it to reduce the impact of a long-term malware attack.”

Additional protection measures include providing customers, at no cost, with a separate, read-only operating system that locks down the browser once users connect to their bank site. In addition, FFIEC Direct leverages transaction monitoring technology from Silver Tail Systems to study the behavior of users’ banking sessions.

“If one of our customers gets compromised, it’s not good for them,” Bradfute says. “We are in the trenches with our customers. I’ve literally gone to customers’ homes and answered questions. We try to take very good care of them. Our success depends on their success. It’s a very symbiotic relationship.”

James Polk Stone, a three-branched institution nestled among the sprawling dairy farms of eastern New Mexico, recognizes that the stealthy malware that makes crooks control of victims’ PCs enters at the user location — not the bank. Thus, educating customers on running anti-virus and firewalls and considering tactics such as using a dedicated, non-Windows machine for online banking, is instrumental to their safety.

“Frankly, we scared the living hell out of them,” Bradfute admits, adding that each meeting had perfect attendance.

And even though only about 50 of the bank’s 1,110 commercial customers use ACH transactions for functions like direct deposits, Bradfute and his team have created a custom-built program that parses payroll files, seeking out anomalies that could signal unauthorized transfers.

In addition, the bank is considering providing its customers with portable media that they could load each time they want to access the online banking portal. The media, such as a CD or USB stick, would create a separate, read-only operating system that would not be at risk to malware. Once the media is removed, any memory is wiped, and the user can return to the normal operating system.

While none of its customers have been targeted by ACH fraud, Bradfute “guarantees it’s coming.” He can only hope the bank’s internal controls and user education will stop it.

“The bad guys only have to be right once,” he says. “We have to be right all the time.”

— Dan Kaplan

CASE STUDY: Symbiotic relationship

Last fall, Richard Bradfute, CEO of the James Polk Stone Community Bank, made the three-hour trip to two of his bank branches to meet with commercial account holders. The meetings were called to address the continued risk of Automated Clearing House (ACH) and wire fraud, perpetrated by criminals who take control of commercial bank accounts to steal money. Small and midsize organizations across the country have been the primary target and have suffered massive losses to the tune of hundreds of millions of dollars over the past several years.

Richard Bradfute, CEO of the James Polk Stone Community Bank, a three-branched institution nestled among the sprawling dairy farms of eastern New Mexico

“Stealing money looks different than not stealing money,” Silver Tail’s Mather says. Wolfe says all banks — no matter their size — should be running the latest and greatest to detect and stop today’s most innovative fraudsters. Size is not an excuse.

“Today the technology available to banks of any size is pretty significant,” Wolfe says. “The costs are not preventive. The size of your bank shouldn’t have any relevance to the sophistication and quality of security. That said, the more you see, the more you learn.”

But Whaley of the Independent Community Bankers Association would prefer to see the FFIEC take a risk-based approach. “If you have two business customers and right relationships with them, do you need the same security if you have thousands or millions of customers?” he asks.

Precedent could be coming

Since the wave of corporate account takeovers began pillaging SMBs, a number have fought back in the form of lawsuits against their banks, contending that the financial institutions were the ones who should have spotted and stopped the fraud. Therefore, they say, the banks should be liable for the losses.

The technology available to banks of any size is significant.” — Rudy Wolfs, CIO, ING Direct

“Today the technology available to banks of any size is pretty significant,” Wolfe says. “The costs are not preventive. The size of your bank shouldn’t have any relevance to the sophistication and quality of security. That said, the more you see, the more you learn.”

But Whaley of the Independent Community Bankers Association would prefer to see the FFIEC take a risk-based approach. “If you have two business customers and right relationships with them, do you need the same security if you have thousands or millions of customers?” he asks.

Precedent could be coming

Since the wave of corporate account takeovers began pillaging SMBs, a number have fought back in the form of lawsuits against their banks, contending that the financial institutions were the ones who should have spotted and stopped the fraud. Therefore, they say, the banks should be liable for the losses.
ARE YOU Rolling the Dice WHEN IT COMES TO Hiring Your IT Security Personnel?

Know What You’re Getting with GIAC Certified Professionals.

Hiring new personnel is never easy. In information security, finding a person with relevant and applicable hands-on technical skills can be a gamble. The volume of candidates and resumes can be overwhelming. Fortunately, there are key indicators, such as industry certifications like those granted by the Global Information Assurance Certification (GIAC) program, that can aid in identifying superior talent. No organization wants to make headlines because of a data breach or other incident that reveals a failure to properly secure its systems and data. Having GIAC certified professionals on your security team improves your chances of mitigating a cyber attack, aids in maintaining the integrity of your systems, and minimizes the impact when an attack occurs.

GIAC Certifications enable you to get the right people in the right job positions to secure your organization’s information.

The GIAC Certification Program:
- Validates real-world competency
- Offers job-specific, skills-based certifications aligned with critical infosec job duties
- Assures professionals have practical hands-on skills
- Is highly respected among both industry leaders and technical practitioners

According to the 2010 Verizon Business Data Breach Investigations Report:
- 61% of data breaches were discovered by a third party
- GIAC Certified Intrusion Analysts detect incidents before your customers do
- 86% of victims had evidence of the breach in their log files
- GIAC Certified Incident Handlers know how to identify and respond to potential breaches
- 96% of breaches were avoidable through simple or intermediate controls
- GIAC Security Essentials Certification establishes a baseline for best practice security program structure and controls

In one highly publicized case, Experi-Metal Inc. (EMI), a Sterling Heights, Mich.-based metal supply company, sued Dallas-based Comerica Bank in December 2009, accusing the institution of failing to detect 35 wire transfers that occurred over the course of several hours on Jan. 22, 2009. Through a slick phishing scam, attackers gained access to the banking credentials of EMI to wire nearly $600,000 to money mule accounts. The lawsuit accuses the bank of lacking the controls to detect the fraud – EMI rarely transferred money from its account – in addition to grooming its customers to expect emails from the bank that ask it to click on links and enter credentials. The case brings to the first of its kind to go to trial, and both sides were awaiting a verdict as of press time.

“The concept of [what is] reasonable security has not really been ruled upon in court,” says Dave Navetta, partner at the InfoLawGroup, a Denver-based security, privacy and technology firm. “It could set a precedent of some sorts. [One] can make arguments that both sides were responsible. It’s a difficult decision to make for a judge.”

Comerica has the deep coffers to fight this tooth and nail, believing the fault is on EMI and therefore the metal supplier is not entitled to monetary relief. But while a precedent may be set if a judge rules in favor of EMI, many small banks already reimburse their customers for their losses, Whaley says.

“In most cases, community banks choose to absorb the loss,” he says. “High-profile litigation with customers is not good for business, causes reputation risk, and most community banks see this as a last resort where forensic evidence shows that relaxed procedures on the business side led to the loss.”

Some commercial customers may find further help in a proposal introduced in Congress in September by Sen. Chuck Schumer, D-N.Y. The bill, which has been referred to committee, would amend Regulation E of the existing Electronic Fund Transfer Act to extend fraud liability protection to local governments and school districts. Current law only offers this protection to consumers.

A shared burden
Still, many experts say that the obligation to practice security rests on both the bank and the customer. Even though ING Direct operates with the assumption that its customers’ machines already are infected, it believes they should still play a pivotal role in the chain.

“Part of it is a two-way partnership with customers and banks,” Wolfs says. “Ultimately, security does rely on the customer to take appropriate precautions and works with the bank and their business processes. Just like an automotive company delivers cars, if people drive around without their seatbelts or park everywhere without locking their door, there’s going to be problems.”

Part of the new FFIEC guidance speaks to consumer awareness, according to the leaked draft. Among the expectations are that banks will offer their customers an explanation of protections required for electronic funds transfers and information on when they may contact them to request banking credentials. Michael Jackson, associate director of the FDIC Division of Supervision and Consumer Protection, says his office has been instrumental in promoting discussions around the problem of commercial account takeovers. That includes collaborating with banks, small business trade associations, the FBI and the Financial Services Information Sharing and Analysis Center.

“The biggest thing is to get the information out,” he says. “These incidents originate outside of the banking arena, outside of the space that has always been guarded in the past.”

A separate challenge for banks is that a majority of them use service providers to host their online banking portals. In many cases, these outsourcing firms provide only minimal security and the bank is responsible for the rest.

“I think the banking software companies need to offer a lot of security standard with their package,” Whaley says.

ING Direct has the luxury of size and home-grown applications, but security has been a priority since it was founded in 2001 – not surprising, considering the bank has never operated outside of the internet era.

“Anybody can stop any project on a security concern at any point,” Wolfs says. “You’ve got a trump card in our operation if you feel there are concerns about security.”
Managing threats

A decade or two ago, the image of the traditional, once monopolistic telecommunications company as stodgy protector of its proprietary, legacy networks might have been apt. Ma Bell gathered her matronly skirts about her and dared anyone to threaten her brood. Today, when even what should be the most secure Canadian government departments are reduced to sending their employees to the nearest Starbucks to charge their devices, the dilemma is that Canadian organizations large and small are already maxed out. It is, he says, a classic glass-half-full scenario.

It is very hard for a corporate IT group in a big company to keep up with all the threats,” he says. “For a small- or mid-sized company, it is virtually impossible. So companies need to find service providers who can give them consulting services where the security is guaranteed. The service provider can focus on the security issues, and the business can focus on what it does well.”

Bell has a growing business in both professional services consulting on security issues and in managed services, where the company relieves its customers of concerns related to software vendor selection and network monitoring. While Cameron says that large customers — primarily financial institutions and the federal government — make up the biggest component of its managed services, Bell is taking what it learns at the top end and cascading that knowledge down to smaller customers.

“Like other carriers, Bell is holding its cards close about its plans for v6. We’ve been working internationally with the carrier community.”

Bell’s enterprise division (BCE), believes the move to IPv6 — the successor to IPv4 — represents a huge cost-saving for a well-financed one. Fourth on Cameron’s list of security trends is something he says is not even on most organizations’ horizons: IPv6.

“The transition to v6 will require reconfiguration of all of the security infrastructure,” he says. He says that the transition and migration will introduce some new vulnerabilities that won’t occur once v6 is fully deployed. Like other carriers, Bell is holding its cards close about its plans for v6. “We’re very focused on it,” says Cameron. “Obviously, we’re the biggest consumer of IP in Canada. We have to make some decisions before we start to reveal our strategy, but we’ve got teams on it and we’re doing our own planning. We’ve been working internationally with the carrier community.”

He concedes there is a lot of uncertainty. After all, that is one of the reasons Bell has found a new revenue stream in taking a load off customers whose IT resources are already maxed out. It is, he says, a classic glass-half-full scenario.

“The good news is that new technologies provide tremendous potential to improve technology and decrease costs,” he says. “But, in using them, we all have to be very aware of some of the security challenges they pose.”

His best piece of advice for organizations juggling security issues is “Have a strategy. That’s more important than all the other components individually. Make a plan and keep it updated. Everything on the security front evolves, and you have to keep pace.”

That is a lesson that Bell Canada itself seems to have learned in the post-monopoly environment. ■

Security concerns in Canada are getting attention as new technologies and advanced malware emerge, reports James Hale.
The winners of the prestigious 2011 SC Awards U.S. were announced on Feb. 15 in San Francisco.

More vibrant than ever, the sixth year of the SC Awards U.S. was held on Feb. 15 in San Francisco. The gala event honors those companies and individuals whose products and services have most strongly contributed to the vitality of the IT security industry.

“I attend because I believe it’s the pre-eminent award ceremony in our industry,” said Dov Yoran, co-founder of MetroSITE Group. He likens the event to the Oscars. “I also find the attendance consists of the who’s-who in the information security industry.”

Visit our website to see a full list of winners, as well as to view photos and video clips from the evening.

Preparations are already underway for the 2012 SC Awards U.S. For more information, contact Natasha Mulla at (646) 638-6108 or natasha.mulla@haymarketmedia.com.

1. Lindsey Jones, media relations, Entrust; Karen Kiffney, sr. product marketing manager, RSA; Paul Stump, senior manager, product marketing, RSA; Jennifer Binet, territory account manager, Entrust; RSA was winner of Best Multifactor Product

2. Winn Schwartau, president and founder of The Security Awareness Co.; Jackie Baumann, director of PR at M.A.D. Partners; and Richard Marshall, director of global cybersecurity management at the Department of Homeland Security

3. Maurice Hampton, information security and privacy services leader, Clark Schaefer Consulting, and on SC Awards judge

4. Ilene Armbruster, editor-in-chief of SC Magazine; Neal D’Averil, founder and executive director of Identity Theft Council; winner of the Editor’s Choice Award; and host/comedian Ron Pounson

5. Chris Porter, CEO of The Training Camp and Col. Mike Converyon, leader of the U.S. Air Force’s Information Warfare Group

6. Sophos team, winner of Best Email Security

7. Bob Smith, co-founder and CTO, and Daniel Ashby, CEO, M.A.D. Partners, winner of Rookie Security Company of the Year

8. (ISC)2 team: Jayda Shriver, marketing program manager; Judy Livers, senior market development manager; and Pamela Diersen, senior product development manager; (ISC)2 was winner of Best Professional Training Program

9. Qualys team, winner of Best Security Company and two other awards

10. The crowd listens in anticipation as an award is announced
For many small and midsize businesses, neglecting IT security is a thing of the past, reports Angela Moscaritolo.

For the four-person IT staff at Arc Greater Twin Cities, information security is just one element of the job, but the nonprofit would be nothing without it.

“Our only real currency in the world is our reputation, and if you are breached, your reputation goes down the tank and that’s your business,” says Paul Harder, director of technology at Saint Paul, Minn.-area Arc, which provides support services to individuals with intellectual and developmental disabilities. “Our primary concern is the protection of data.”

And a lot of sensitive data there is. For starters, there’s credit card information.

As a not-for-profit with about 430 employees, much of the organization’s income comes from its retail business—a line of thrift stores and donation centers—called Arc’s Value Village—where shoppers can buy anything from a pair of vintage high heels to a solid brass beer stein. And then there’s an ever-growing trove of personal data—including medical diagnoses, prescription information and financial records for many of the 6,300 individuals Arc serves.

From an information security perspective, Arc is no different than any other business. Organizations of all types and sizes must be on high alert for malware and phishing attacks and counter additional data leakage threats posed by social media, mobile devices and malicious insiders.

For small and midsize businesses (SMBs)—organizations with fewer than 500 employees—many of those challenges are compounded by tight budgets, thin workforces and a lack of in-house information security expertise.

But despite the daunting challenges they face, SMBs are beginning to outgrow their old reputation of neglecting IT security. While these entities in the past often failed to implement the most basic safeguards, they are now becoming focused on protecting sensitive data, according to a global SMB information protection survey released last June by Symantec.

The survey of 2,152 SMB executives and IT decision-makers in 28 countries found that 74 percent of respondents are “somewhat or extremely” concerned about losing electronic information.

Industry rules and regulations, such as those applying to health care, financial services and power companies, have forced many SMBs to build up their security ecosystems, says Michelle Dickman, CEO of TriGeo, a security solutions provider that caters to the small and midsize sector. In the retail vertical, the Payment Card Industry Data Security Standard (PCI DSS), which applies to any merchant that processes, stores or transmits credit card information, has prompted some SMBs to address security.

Even so, PCI DSS compliance rates among SMBs remain low, according to a survey released in January by the National Retail Federation, a trade association representing 1.6 million U.S. companies. In the survey of 651 SMBs, just 49 percent of respondents said they had completed a PCI DSS self-assessment, even though 74 percent were aware of the requirements.

Moreover, those outside the regulated industries—such as manufacturing firms—have been even slower to embrace security, Dickman says.

“These folks say, ‘My management won’t cough up money until we have a reason—a breach or regulation requiring it,’” says Dickman.

Gaining upper-level support for security often proves difficult for those in regulated industries as well. Dickman says IT professionals know that PCI DSS and other rules mandate only a minimum level of security, but their bosses often choose to allocate funds for the least expensive product that ensures compliance. While this trend has held steady for years, it is, to the delight of security advocates, beginning to wane as some higher-ups realize the importance of going above and beyond what is required.

Frequent headlines trumpeting the fact that cybercrooks are draining small-business bank accounts are certainly increasing awareness that the bad guys are targeting everyone, regardless of size, Dickman says.

Back in Minnesota, Arc Greater Twin Cities is an example of one of those entities going above and beyond what is mandated. After coming on board in 1999 to head up the IT department, Harder says his team first built up the network infrastructure and then started looking at ways to protect it.

“This might have been the right or the wrong way, but it was the only way we could go because of the financial constraints we were under,” he says.

Fast forward to today, and Arc still has a tight budget. To remain in good standing as a partner of the United Way, no less than 70 percent of a nonprofit’s budget must go toward the people it serves, leaving just 30 percent for all administrave needs. But that hasn’t prevented the organization from becoming PCI DSS compliant, Harder says.

Finding the funding to accomplish all of their security initiatives, including PCI, is difficult, Harder says. The organization can only take on one major security project a year, so planning is imperative. Plus, Harder calls himself a “ruthless negotiator” with vendors and often stresses that because Arc is a charity, donations could have tax advantages for them.

“A dedicated organization with a dedicated professional technologist can do wonders with little money,” he says. “The most difficult part for any nonprofit is to sell the concepts to their leadership.”

To overcome that challenge, Harder says to “educate, educate, educate.” Also, because Arc maintains some extremely sensitive personal health information—such as medical diagnosis and prescription data—the organization has adopted protections mandated by the Health Insurance Portability and Accountability Act (HIPAA), a set of guidelines for working with patient health data. HIPAA typically applies to health care organizations, including counselors, therapists and other providers that transmit electronic billing information to health insurance companies.

Frequent headlines trumpeting the fact that cybercrooks are draining small-business bank accounts are certainly increasing awareness that the bad guys are targeting everyone, regardless of size, Dickman says.

Back in Minnesota, Arc Greater Twin Cities is an example of one of those entities going above and beyond what is mandated. After coming on board in 1999 to head up the IT department, Harder says his team first built up the network infrastructure and then started looking at ways to protect it.

“This might have been the right or the wrong way, but it was the only way we could go because of the financial constraints we were under,” he says. 

Fast forward to today, and Arc still has a tight budget. To remain in good standing as a partner of the United Way, no less than 70 percent of a nonprofit’s budget must go toward the people it serves, leaving just 30 percent for all administrative needs. But that hasn’t prevented the organization from becoming PCI DSS compliant, Harder says.

Finding the funding to accomplish all of their security initiatives, including PCI, is difficult, Harder says. The organization can only take on one major security project a year, so planning is imperative. Plus, Harder calls himself a “ruthless negotiator” with vendors and often stresses that because Arc is a charity, donations could have tax advantages for them.

“A dedicated organization with a dedicated professional technologist can do wonders with little money,” he says. “The most difficult part for any nonprofit is to sell the concepts to their leadership.”

To overcome that challenge, Harder says to “educate, educate, educate.” Also, because Arc maintains some extremely sensitive personal health information—such as medical diagnosis and prescription data—the organization has adopted protections mandated by the Health Insurance Portability and Accountability Act (HIPAA), a set of guidelines for working with patient health data. HIPAA typically applies to health care organizations, including counselors, therapists and other providers that transmit electronic billing information to health insurance companies.

SMB defense
a technique called “port scanning” to address. Cybercriminals often employ monitoring, Harder noticed a huge amount While walking past the data center intelligence it provided to stop an attack. The SIEM solution provides real-time visibility and allows the IT team to easily find and analyze log data generated by the various security products running on an organization’s network. In Arc’s case, the SIEM solution provides real-time visibility and allows the IT team to easily investigate suspicious behavior and policy violations.

In fact, soon after deploying the SIEM, Harder was able to use intelligence it provided to stop an attack. While walking past the data center where the SIEM console was up on a monitor, Harder noticed a huge amount of port scans coming from a single IP address. Cybercriminals often employ a technique called “port scanning” to discover weak access points that will provide an entryway into a computer.

Researching the attacking IP address, Harder discovered it belonged to a legitimate company in Oregon. One of that company’s machines had been compromised and was being used to probe computers at Arc. Harder called the company, and within five minutes after the phone call, the port scans stopped. Another time, Harder caught a malicious insider attempting to copy Social Security numbers to a flash drive, he says. Arc employees are allowed to use external memory devices, but company policy prohibits personal information from being taken offline.

The SIEM product detected the insertion of the USB memory device and alerted Arc’s IT team that the device was plugged in. A separate endpoint security product allowed the team to see what type of data was loaded on the device. Needless to say, the perpetrator didn’t even make it out the door before being caught.

“People use USB devices all the time on our network,” he says “If someone’s just listening to music, we don’t discourage that, but we always take a look to see if there is any data flow.”

From malicious insiders to external cyberthieves, SMBs today are facing many of the same threats as their enterprise counterparts. The good news, though, is that many understand the importance of protecting sensitive information and so IT security endeavors are becoming a top priority.

And, with the economy showing signs of improvement, SMB IT budgets are expected to grow this year, according to a survey, released in February by research firm Gartner."
Critical infrastructure

this time, but security does need to be re-evaluated, he says.

Certainly with the arrival of Aurora, Stuxnet and WikiLeaks, it has been an “off-the-hook” year, says Rowney, who is also director of the breach response team at Symantec. “How fast things have progressed.”

Others agree. Stuxnet was definitely a game-changer in terms of what it could do, says David Kennedy, director of information security at Diebold, a security integrator that provides protection and detection solutions. “What it showed was that our current ways of thinking about security are flawed.”

The fact that the intrusion happened from the inside points out that hackers are bypassing traditional defenses, he says. “Stuxnet should have been detected.”

He says that the anamolous traffic on the system should have alerted somebody. “We can’t treat the internal environment as a safe haven anymore,” Kennedy says. “Internal users are untrusted now. We need to look at critical infrastructure and put controls around it.”

But others say it will take more than technology to safeguard systems. Following Stuxnet, executives should place emphasis on policies and procedures, says Amichai Shulman, CTO at Imperva, a Redwood Shores, Calif.-based data security vendor. Stuxnet was successful because the code was distributed using USB sticks or key foils, probably giveaways at some event, he says. These were then inserted carelessly in protected networks which unleashed the bug.

Shulman advises that rather than focusing efforts on protecting the control systems in SCADA networks, as he has seen in some government entities, it would be better to beef up security management systems, using the same tools and techniques used to protect web-facing applications. IT professionals should consider everything outside of the SCADA network to be hostile. To protect the power grid, he says it is essential to isolate the SCADA management network away from other functions, such as HR, finance and transportation.

But, this might not be enough as the SCADA systems in Iran were protected well by most standards, says Charlie Miller, principal analyst of software security at Independent Security Evaluators, a security consulting firm. They ran on an isolated (non-internet-connected) network that consisted of fully patched Windows computers running up-to-date anti-virus. “This is really all you could hope for in these critical infrastructures,” Miller says.

Ahead of the curve
Still, the complexity of infrastructure systems invites any number of exploits that, experts say, can only be thwarted by staying on top of the latest threat intelligence. Attackers are constantly changing and adapting, so the best defense is one that is dynamic and flexible, says Don Jackson, director of threat intelligence at Dell SecureWorks. His recommendation is that those responsible for building and managing critical infrastructure systems employ the services of objective security professionals to continuously refine threat models by incorporating data from the latest incidents and intelligence on emerging threats.

“Assessments need to take into account new information learned about the financial resourcefulness, technical sophistication, determination and the impact of threat agents, such as those behind Stuxnet,” Jackson says. “Those assessments inform funding and policy regarding critical infrastructure protection.”

He believes there should be a shift to whitelisting approaches for code packages, integrity controls and anomaly detection features that operate at supervisory layers, operating systems that have smaller attack surfaces, and security models that are more strict about access to process memory and the kernel.

Eric Knapp, director of critical infrastructure markets at NitroSecurity, agrees that whitelisting is essential to fight zero-days, as well as strong edge policies to make it harder to access target networks.

“We’ve always hardened the entry points into SCADAs and internet connection sharing (ICS) networks by securing the enterprise network that contains them, while leaving those critical networks relatively unprotected from the inside,” Knapp says. “The control systems have to be as hard if not harder to breach – a defense-in-depth strategy comprising elements including specialized ICS firewalls, and compatible network and application whitelisters.”

Lessons from Stuxnet
Few would argue that traditional security strategies are sufficient in a post-Stuxnet world. The attack in Iran should have taught security professionals many things, says Michael Assante, president and CEO of the National Board of Information Security Examiners (NBISE), a nonprofit that develops examinations and certification requirements. “One realization is that the perimeter protection model used to protect critical systems is more aligned with cyberthreats of yesterday and is most effective against less directed and intelligent types of cyberattacks.”

Stuxnet also demonstrates the need to address security and resilience at the design and building stage, says Assante, former CSO at the North American Electric Reliability Corp. (NERC). “We can’t continue to look solely toward owners and operators and expect to bolt on security to manage risk around difficult-to-secure technology.”

Meanwhile, legislation may help change the regulatory structure around critical infrastructure protection, he says. “The key will be balance. Incitatives are not the entire answer, neither is prescriptive regulation.”

Copycat attacks to follow
But perhaps the biggest impact is yet to come. It is the descendents of the worm that are causing concern for a lot of security personnel. “Even if they can’t get hold of sample code from Stuxnet, it helps ill-intentioned people understand which threat vectors are vulnerable,” says Symantec’s Rowney.

A version of the base code was among a cache of emails that the activist hacking group Anonymous stole from HBGary, a security company that was studying the threat. Though this easy-to-read “study” version is a reduction of the original binary code, experts contend there is enough there to supply miscreants with a foundation on which to build copycat attacks. Some expect these to occur within weeks.

And just where the next attack may come from or who it may target is any-one’s guess. Rowney points to the fact that Stuxnet was clearly written with a disciplined approach that likely took six to 10 coders working for six months to produce. “It doesn’t sound like hackers in a basement or an Eastern European cyber gang,” he says. “This sounds like nation-state.”

Rowney hopes nothing like Stuxnet is seen again. But, he admits, it is hard to rule out. “The stakes are entirely raised,” he says. Ill

STUXNET: Up close

■ Stuxnet was a targeted attack on five different organizations.

■ 12,000 infections can be traced back to these five organizations.

■ Three organizations were targeted once, one was targeted twice, and another was targeted three times.

■ All targeted organizations have a presence in Iran.

■ Three variants of the worm exist and a fourth variant likely exists but has never been recovered.

Source: Symantec

Geographical distribution of Stuxnet infections

- Michael Assante, president and CEO, NBISE

We must better develop and equip the workforce...
Protecting the castle gates

UTMs and anti-malware gateways often are our key protection at the perimeter. But, in many cases we are seeing little innovative advancement in the products that we looked at this month.

The nature of internet-borne threats is such that if we do not advance, we actually regress. There comes a point where the UTM will take over for the anti-malware gateway and, some mavens predict, the firewall as well.

Traditionally, the UTM was a combination only of firewall, IDS/IPS and anti-malware gateway. Today, vendors all add something extra: it may be, for example, a broader interpretation of malware, including such things as anti-spa, protocol blocking and web content filtering. That puts UTMs in the same ballpark as other tools, such as anti-malware gateways and web filtering products. In fact, it is not uncommon for a vendor to submit the same product for UTM and anti-malware gateway reviews. This expanded anti-malware functionality becomes part of the larger product, which the vendor now calls a UTM. As we have written in the past, the UTM has supplanted the multipurpose appliance of years past.
Anti-malware gateways

A strong anti-malware gateway solution can stop email and web-based threats before ever making it inside the enterprise environment, says Michael Lipinski.

Malware is that group of threats for which we never seem to have enough protection. Next to insider threats, malware may well be the greatest security challenge we face in securing the enterprise. We see components for malware protection in endpoint security products, IDS/IPS solutions, and purpose-built desktop offerings for things like anti-virus, anti-spam, phishing and web content filtering. This first Group Test looks at the products that deliver another layer of protection for malware. These products deploy and defend at the gateway against email, web and application threats, such as viruses, worms, spam, spyware, adware, phishing, keyloggers, trojans, rootkits, downloaders and various levels of zero-day threats. Malware prevention is truly a layered defense worthy of a holistic multitiered approach. That said, personally, I would prefer to have a strong gateway solution so email and web-based threats can be stopped before ever making it inside the environment.

The products we review address some or all of the threats listed above. There are products that are stronger or focus more on email and/or web content. Most of the solutions we reviewed address both. Most of the products came to us as an appliance, while the others were delivered as software or software ISO versions (an image file on a DVD loaded onto hardware). Regardless of the offering, all the products this month were fairly easy to get installed and running. Most had very simple setups for basic network connectivity and default protection. There were some that still used a command line initial setup, which did surprise us a bit since this is such a mature product category. There are differences in the deployment methodologies that should be considered. Some products support a bridged/pass through operation, others support a proxy-based deployment, while some support both options. Performance versus level of protection has to be weighed when choosing the best deployment method. You’ll also want to look for clustering options for those products working in proxy mode. Most of the tools did support some enterprise features, such as high-availability deployment configurations and the ability to send configuration and log data to external sources.

We found that alerting and reporting did differ greatly in the products, so you will want to pay particular attention to what you need in this area when evaluating these products for yourself. The tools all shipped with their version of the dictionaries/libraries needed for identifying, quarantining or removing the threats they know about. One thing we looked at was the ability to easily create policies for unknown, blended or zero-day style threats. We did not assess the products for their catch rates or throughput performance. We evaluated the implementation process, the usability of the products once installed, the amount of protection provided, the enterprise capabilities of the solutions, visibility and presentation of the data, reporting, logging and alerting capabilities and, finally, value for the price and support offerings. We found solutions that deployed very quickly with little impact to the enterprise infrastructure and required very little technical savvy, while still delivering quite a bit of protection.

There is no magic wand for defending against threats, so this is an area you will want to spend some time evaluating. You will also want to evaluate whether an integrated web and email offering is better for you than a separate, dedicated web and email solution. Additionally, you should understand if the product you choose is capable of scanning both incoming and outgoing traffic. Most of the products will boast about the advantages that their threat and vulnerability databases/libraries bring them. I believe it is more important for the products to provide your technical team with the ability to be able to determine from the data what the real threat is and then provide the tools to customize a remediation. In the end, you’ll have some tough choices to make. These were all good products.
### M86 Secure Web Gateway v10.0

- **Vendor**: M86 Security
- **Price**: Starts at $4,980 per user for a subscription license for 10,000-plus users for one year.

**Features**
- **Ease of use**: ★★★★★
- **Performance**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★

**Strengths**
- Very flexible for controlling and managing employees, and can be customized and extended using a variety of plug-ins.
- Good value for the money.

**Weaknesses**
- The user interface can be a bit hard to use.

**Value for money**: ★★★★★

**OVERALL RATING**: ★★★★★

---

### McAfee Email and Web Security Virtual Appliance v5.6

- **Vendor**: McAfee
- **Price**: From $17 (25 users or less) to $88 (10,000-plus users) per user for virtual appliance per year.

**Features**
- **Ease of use**: ★★★★★
- **Performance**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★

**Strengths**
- Behavior-based scanning engine with nice reporting.

**Weaknesses**
- McAfee requires constant attention to stay ahead of threats with custom policies. The user interface is a bit hard to use.

**Value for money**: ★★★★★

**OVERALL RATING**: ★★★★★

---

### NETGEAR ProSecure STM300 v3.0.0-43

- **Vendor**: NETGEAR
- **Price**: $2,995 (STM300 one year bundle)

**Features**
- **Ease of use**: ★★★★★
- **Performance**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★

**Strengths**
- The ProSecure Web/Email Security Threat Management Appliance is an appliance-based, web and email security solution that protects against all web-based threats.

**Weaknesses**
- The user interface is a bit hard to use.

**Value for money**: ★★★★★

**OVERALL RATING**: ★★★★★

---

### Panda Security GateDefender Performa SB

- **Vendor**: Panda Security
- **Price**: $1,699 for appliance with “total protection” licenses for one year.

**Features**
- **Ease of use**: ★★★★★
- **Performance**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★

**Strengths**
- Good value for the money.

**Weaknesses**
- Interface is a bit hard to use.

**Value for money**: ★★★★★

**OVERALL RATING**: ★★★★★

---

**SC MAGAZINE RATING**

- **Ease of use**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★

**SC MAGAZINE RATING**

- **Ease of use**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★

**SC MAGAZINE RATING**

- **Ease of use**: ★★★★★
- **Documentation**: ★★★★★
- **Support**: ★★★★★
SonicWALL NSA 3500

Price: $6,870, including hardware, subscription with 24/7 support and anti-spam for one year

Contact: www.sonicwall.com

The SonicWALL NSA 3500 is designed to provide multi-protection at the gateway for anti-virus, anti-spyware, anti-spam and a real-time cloud anti-virus service. Gateway Anti-Virus and Anti-Spyware are provided by SonicWALL's patented Reassembly-Free Deep Packet Inspection engine and are powered by signatures provided by SonicWALL GRID Network and an in-house research team. The NSA 3500 is also capable of blocking spam and access blocking sites to users classified as dangerous based on an IP reputation system.

The product comes complete with a firewall, application firewall, secure wireless controller, SSL VPN, VPX, and anti-spyware and anti-virus capabilities. It can be deployed in a unified threat management (UTM) capacity or as a complement to other gateway offerings. We tested it as an anti-malware tool and used the malware capabilities along with the application firewall. The offering can be deployed in a route mode or in a Layer 2 Bridge mode. There are enterprise capabilities supporting port redundancy and load balancing.

Trend Micro Enterprise Security for Gateways

We deployed it in bridge mode and as such had it installed and running in minutes. The secure web-based user interface employs a tree-based menu navigation model for managing and configuring the various capabilities. Email scanning is handled through the anti-spyware module and can scan email transmitted through SMTP, IMAP or web-based mail. The application firewall allowed us to configure blocking for various protocols of applications, including access to HTTP proxy sites.

We liked the dashboard's capabilities, although it was possible to import or to get other tools reviewed this month, but the data was there. While reporting was lacking, according to the documentation, you can purchase an upgrade to enhance reporting capabilities.

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★

OVERALL RATING ★★★★★

Strengths: Support for SSL scanning, easy setup, desktop anti-virus validation, deep packet forensic classification capabilities.
Weaknesses: Very light on reporting.

Verdict: Full service offering or a great complement to an existing gateway solution.

BeSecure NDP-1005G Anti-Malware v4.0.0-213

Price: $6,140

Contact: www.wedgepointworks.com

Wedge Networks' BeSecure NDP-1005G is a content inspection and filtering network appliance that offers a complete solution for protecting network endpoints from spyware, trojans, worms and viruses. It also provides a spam detection engine and keyword or URL-based content filtering engine. The BeSecure appliance is a 10Gbps solution capable of high-accuracy web, email and FTP anti-malware protection for inbound and outbound traffic. The appliance has engines for anti-spam, anti-virus and web filtering and supports scanning for HTTP, FTP, IMAP, POP3 and SMTP.

Kaspersky is used for the malware signature database and to detect viruses, worms, spyware, adware and trojans. The unit also contains a Cloudmark anti-spam, anti-phishing engine that is updated every 45 seconds. In addition, it uses a complete Secure Computing/McAfee Web Filter database with 90 plus web categories. The keyword filtering capability was a great tool for deep word and pattern inspection for data leakage prevention. The appliance can be deployed in various versions of proxy or transparent modes, giving users a full suite of deployment choices. High availability configurations are available to provide performance and redundancy in all deployment scenarios. Setup was very easy. It defaulted to a bridge mode and was installed and working in minutes. The dashboard/user interface was pleasing. There is a nice menu-driven event query tool with good drill-down filter capabilities, email event reporting by incident type, and a well-done web-based reporting tool that works as a series of stats or graphs. Logging is syslog-based either on or off the appliance. Support is only included for 30 days, and there are three options for purchasing additional help beyond the warranty. Documentation included a one-page to get users into the system and to do the basic setup. The appliance costs $6,140, including hardware, for up to 500 users and an anti-malware software license for one year.

SC MAGAZINE RATING

Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★

OVERALL RATING ★★★★★

Strengths: (GLP and pattern matching capabilities, very nice interface, dashboard)
Weaknesses: Support and yearly renewals can be substantial
Verdict: Had everything we were looking for. Higher on the price scale, but delivers a lot of capability and performance.

INFORMATION ASSURANCE

Defend Networks and Information. Impress Potential Employers.

Preventing data theft, reassuring customers, complying with federal regulations. Just some of the reasons why securing information is such a high priority for employers. Seize your opportunity, with a certificate or a master’s degree from University of Maryland University College (UMUC). Whether you’re a manager or an IT professional, you’ll learn how to protect systems and information against deliberate attacks or accidental damage.

Enroll now.
800-888-UMUC • umuc.edu/data

- Designed as a National Center of Academic Excellence in Information Assurance Education by the NSA and the DHS
- Recognized as a Professional Science Master’s by the Council of Graduate Schools
- Financial aid and an interest-free monthly payment plan available
- Program is offered entirely online
Unified threat management (UTM)

The ability to distribute protection across a large enterprise is critically important in today’s threat environment, and UTMs may be mature enough to help, says Peter Stephenson.

PRODUCT SECTION

PICK OF THE LITTER

This year we had a galleon of products for our UTM Group Test, and while some exhibited interesting innovation, most were quite similar to what we saw from these vendors in the past. There are two areas, though, where we saw growth in capability: user interface and the addition of data leakage prevention (DLP) functionality.

Today’s UTM does not much resemble the UTMs of the past, however. While the genre has reached maturity over the past few years, there has been significant growth since the product type originated, both in the number of products and in their functionality.

Typically, today’s UTM can be expected to contain a firewall, anti-malware and IDS/IPS. For a long time this combination of services dictated the definition of a UTM. Today, though, there is almost no universal configuration that defines a gateway product as a UTM. However, if the gateway has a lot of different functionality and includes the requisite firewall, anti-malware and IDS/IPS, we can call it a UTM.

There is a lot of functionality beyond those main pieces, of course. Many, if not all, UTMs now include application protocol blocking. This functionality started to become important with the advent of such Internet application protocols as peer-to-peer in its various forms and instant messaging, as well as such often-abused application as BitTorrent. Blocking application protocols at the gateway goes a long way toward reducing risks, both technical and legal.

Web content filtering is another capability finding its way into UTMs. This, along with anti-malware, probably covers the overwhelming majority of threats against the enterprise entering through the perimeter. Technical specialists in companies that deal in these two functions estimate that more than 80 percent — or say even higher — of all threats to the enterprise are internet borne and come in via web surfing.

What’s new...really?

For all this talk about maturity of the product type, nonetheless there are products that are showing some level of innovation in their new releases. While we saw products that have not changed materially in years, we also saw some that were sparkling fresh with new or extended capabilities and smart new dashboards. When you are looking at a bunch of products with little to distinguish one from another, these stood out even more.

The new dashboards are, we believe, especially important. Since the advent of UTMs and other types of gateway appliances, the issue of how to get 10 pounds of information into a few pounds of space has posed real challenges. With screens screaming that you should try to cram as much information as possible into matchbook-sized boxes on the dashboard, you need to take some definitive action. Today’s dashboards tend to be more organized, contain less trivial information and allow the user to customize more than ever before.

Buying a UTM

The second is, “What are the architecture requirements for my enterprise that a UTM can/must support?” It may be that you are already addressing some of the functionality that a particular UTM covers and it may make no sense to buy that particular UTM. On the other hand, the UTM may do a better job than your current solution to whatever problem you are trying to solve.

Not all of the functionality in a given product is equally robust. Sometimes the technologies present in that functionality are from other sources, either purchased, licensed or OEM’d. Look very closely at reviews of the pieces, not just the whole. For example, you will see at least one UTM that appeared last month [Web Content Management Group Test]. At that time, we looked only at one aspect of the product. This month we look at the rest of the product and the solution as an integrated whole. This gives you an opportunity to check both the product and its parts.

GROUP TEST | UTM

Specifications for UTM tools

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>Anti-virus</th>
<th>Anti-spam</th>
<th>Anti-phishing</th>
<th>Web content filter</th>
<th>Application control</th>
<th>IPsec</th>
<th>SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADTRAN NetVanta 2630W</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Astecore Security Gateway v8</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Elitecore Technologies Cyberoam CR100ia</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>eSoft InstaGate 604 v5.0.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Fortinet FortiGate 60c</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>gateProtect GPZ 2500 v8.7</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>NETGEAR ProSecure UTM50</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Panda Security Gateway defender Integra SB</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SecPoint ApS Protector v5.5.7e</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>VASCO Data Security axSGUARD Gatekeeper Enterprise 7.6.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>WatchGuard Technologies XTM 505 v2.14</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>ZyXEL ZyWALL USG500 v2.21</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
ADTRAN NetVanta 2630W

Astaro Security Gateway

Cyberoam CR100ia

eSoft InstaGate 604

---

**GROUP TEST | UTM**

**ADTRAN NetVanta 2630W**

The NetVanta from ADTRAN is powered by SonicWALL OS to provide solid gateway security. This product features gateway anti-virus, intrusion prevention, firewall and VPN connectivity, as well as secure wireless networking with the ability to incorporate a 1G USB antenna for failover. Furthermore, this gateway provides web content filtering and application protocol blocking.

We found this product to be an easy setup. Since it is based on the SonicWALL OS, it includes the easy-to-follow setup wizards that are included with SonicWALL devices. The setup wizard is accessed through the web-based interface and helps set up the initial IP and networking configurations. After the setup wizard is complete, all other configurations can be done through the web interface, and most of the configuration consists of turning various protections on or off by simply clicking a button.

Documentation included a getting-started guide. This provided the steps necessary to get the product up and running on the network with basic configuration. It included clear, step-by-step instructions, as well as quite a few screen shots and diagrams. The rest of the documentation is supposed to be available on the web user portal, but under ‘support documents’ for this product, there were none listed at press time, and we cannot evaluate what we don’t have.

ADTRAN offers several support options through agreements. Customers get access to software updates, firmware upgrades and phone and email technical support starting at eight-hours-a-day/five-days-a-week levels and going up to 24/7 with four on-site visits.

At a price of $1,295, including one year of security subscription service and firmware updates, this product is a good value for the money. The NetVanta offers a lot of easy-to-use functionality at a reasonable price.

---

**Astaro Security Gateway**

Last month we looked at this tool’s web content filtering capabilities and now we look at this product as a whole gateway. Aside from solid web content management and application control, the Astaro Security Gateway offers a fully configurable firewall and intrusion prevention system, including port scan and denial-of-service protection.

This tool also has a gateway-based, anti-virus engine that scans web traffic for viruses, spyware and other malware.

As we found last month, this solution is quite easy to set up and configure. The initial setup is guided by a wizard, which is launched at the first login to the GUI. This wizard helps not only configure the network setup but also assists in setting up an initial policy for the web filter and other security settings.

After the wizard is complete, all further management is done through the GUI, which we found to be easy to navigate and, overall, quite comfortable to use.

Policy is also easy to configure with the majority of the protection functionality enabled by simply clicking a button to turn it on. For added flexibility, gateway anti-virus, spam protection, firewall options and application blocking can be set by importing already existing groups and users from Active Directory.

Documentation included an easy-to-follow quick-start sheet, as well as a full administrator guide built into the appliance interface. The guide covered basic management of the appliance through advanced configuration.

Support is also the same whether it is licensed for just the web content management features or is fully licensed for UTM protection. Astaro offers two subscription plans that provide eight-hours-a-day/five-days-a-week or 24/7 phone and email technical support, access to updates and access to a vast online support area. This includes documentation downloads, a knowledge base, user forum and other resources.

At a price just under $3,000 for the fully loaded bundle, we find this product to be a good value for the money. The Astaro Security Gateway offers a lot of good features, and the appliance provides a lot of solid starting point and, in most cases, only minor tweaking is necessary for full protection.

Documentation included a quick-start guide that detailed the steps to connect to the network and complete the setup wizard. Also included were several configuration guides and a user guide. We found all these to be well-organized and to include many screen shots and configuration examples.

Cyberoam provides support based on its TVS, or Total Value Subscription, program. Based on the level of TVS support, customers get access to eight-hours-a-day/five-days-a-week or 24/7 technical support, updates and firmware upgrades.

At an out-the-door price of $1,295, with the first year of support included, we find this product to be a solid value for the money. This appliance offers granular, identity-based policies and many protection features that are easy to configure.

---

**Cyberoam CR100ia**

The Cyberoam CR100ia from Elitecore Technologies provides solid gateway protection features above and beyond the usual UTM feature set. This product has all the functionality of a UTM – such as gateway anti-virus, spyware and spam protection, web content filtering and firewall and IPS – but its strength is in its flexibility and configurability when it comes to application management and security. This product uses identity-based controls to provide a high amount of control over applications such as IM, chat and file transfers. At just under $3,000 for the unit, plus about $1,500 annually for the ThreatPack and just over $500 annually for technical support, this product can be a little expensive upfront. However, we find it to be a good value for the money based on its solid feature set and easy configurability.

---

**eSoft InstaGate 604**

The InstaGate 604 from eSoft provides full UTM protection to the small to midsize business environment. This product features a full stateful firewall with deep packet inspection and real-time protection and then can be customized with specific eSoft ThreatPaks, such as the Web ThreatPack that includes gateway anti-virus, web content filtering, intrusion prevention, bot detection, and IM and P2P application blocking.

When it comes to setting it up, not much has changed since we last saw this product, which is a good thing. This tool is about as close to plug-and-play as it gets. The initial deployment is guided by a web-based setup wizard and takes just a few minutes to actually run through. But at the end of the wizard, the InstaGate downloads all available updates so that after setup is complete, it is updated and ready to go.

As for the GUI, with a very organized layout, it is still quite easy and intuitive to navigate. While the appliance is pretty much ready to go after the setup wizard, tweaking and customizing policies and rules is easy to do within the interface. Also featured on the interface is a dashboard that eSoft has named ThreatMonitor. This provides near-real-time statistics that are easy to read and provide a solid bird’s eye view of the latest threats and policy violations.

Documentation included a quick-start guide that illustrates the steps to connecting the InstaGate to the network and completing the setup wizard, and also a full user guide that details advanced configuration and management of the appliance and its features. Both are clear and well-organized.

Support provided by eSoft included 90 days of free phone aid as part of the purchase price of the appliance, and ongoing support purchased as part of a plan.

At just under $3,000 for the unit, plus about $1,500 annually for the ThreatPack and just over $500 annually for technical support, this product can be a little expensive upfront. However, we find it to be a good value for the money based on its solid feature set and easy configurability.

---

**GROUP TEST | UTM**

---

**SC MAGAZINE RATING**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Value for money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

**Features**

- Excellent feature set.
- Weaknesses: Some documentation was not available via the web portal nor provided with the appliance.
- Verdict: A potentially good product, but suffers from lack of documentation.

---

**SC MAGAZINE RATING**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Value for money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

**Features**

- Solid functionality with many configurable features.
- Weaknesses: None that we found.
- Verdict: The web content management as a full product is part of an equally competent UTM with a good overall feature set.

---

**SC MAGAZINE RATING**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Value for money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

**Features**

- Easy to deploy with a lot of granular controls.
- Weaknesses: None that we found.
- Verdict: Solid UTM. Our Recommended product this month.

---

**SC MAGAZINE RATING**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Value for money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

**Features**

- Easy to configure with many features available through ThreatPaks.
- Weaknesses: A little pricey upfront.
- Verdict: Total cost of ownership can raise the buy-in price. Still, a good value over time.
Fortinet FortiGate 60c

gateProtect GPZ 2500

The FortiGate 60c from Fortinet provides quite a bit of power packed into a small appliance. This tool feels right at home in small to midsize environments and is packed with features, such as a firewall, intrusion prevention system, application control, data leakage prevention, web content filtering and gateway-based malware protection.

The FortiGate 60c can be set up in two ways. The first is mostly manual and is done through the web GUI. The second is by using the Forti-Explorer software included on a CD with the device. With Forti-Explorer, setup can be completed through a wizard, which helps set a basic configuration including network information and IP settings. After the appliance is initially configured, all further management can be done through the web GUI. We found this GUI to be fairly easy to navigate and we had little trouble getting around.

The strength of this product is configurability. The FortiGate offers a lot of policy flexibility and configurable options with granular controls. Creating policies and rules for functions such as the firewall and web content filter is quite easy, but it is a manual process and does take some time to configure.

Documentation was comprised of a short quick-start guide that provided the steps for initial configuration, with a focus on configuring through the FortiExplorer application. Other guides provided included one for administrators and a few other supplemental materials.

Fortinet offers 90 days of eight-hours-a-day/five-days-a-week support included with the purchase and additional support is part of an annual contract thereafter.

At a price just under $850 for the appliance and the first year of security services – anti-virus, intrusion prevention, web filtering, anti-spam/application control FortiGuard Services updates, as well as eight-hours-a-day/five-days-a-week support and firmware upgrades – we find this product to be an excellent value for the money.

The second option is creating a blank desktop through the eGUI application and configuring all the zones and groups manually. Last year when we reviewed this product, we said it was complicated and confusing to set up and manage and that the eGUI design was uncomfortable to use. We have to say that since the last review we have spent a little more time getting to know how the gateProtect eGUI works, and we now can say that this interface is actually quite simple to use.

The company offers 30 days of support 24/7 via an online portal included in the price of the product. After the 90 days, customers can purchase additional support at various levels through a contract.

At a price just shy of $25,900 – including UTM software and one-year premium support – this product carries a very hefty price tag for a product in this category. However, based on its extremely flexible and easy-to-manage eGUI, we find it to be a reasonable value for the money.

This solution is intended for the very large and complicated infrastructures of large corporate environments, and the price definitely reflects that.

Panda Security GateDefender Integra

The ProSecure UTM from NETGEAR offers a full-function UTM appliance for smaller networks. It features a firewall that not only filters based on static rules but also can provide application-layer protection. Also included with this product is an intrusion prevention system that scans traffic via protocols such as IP, ICMP, TCP and UDP and protects against possible attacks to the network with malware and spam protection and web content filtering.

At a price of $1,800 for the appliance, software and one year of support, we find this tool to be an excellent value for the money. The NETGEAR ProSecure UTM offers a solid setup feature that is easily configurable for almost any size environment.

During our test, we noticed a few quick issues with the help of a short setup wizard. This wizard helps get the product up and running with a basic configuration in place. However, after the setup wizard is complete, there is still a bit of configuration left to do.

The remaining configuration and management is all done through the web-based interface, which we found to be a little awkward to navigate at first.

During our test, we noticed that a lot of our mock attacks were getting through the appliance, so we navigated to the base policy for the IPS and found the default for a great majority of the IPS signatures was to simply report versus block or reject. This could be a problem outside of the lab if an attacker manages to compromise the firewall of the appliance. They might be logged, but at that point the damage is already done.

Documentation included a short installation guide, as well as a full user guide. We found both guides to be easy to follow with many diagrams and clear instructions, but we would have liked to see more screen shots in the user guide.

Panda offers 24/7 support as part of its total protection package. Customers can access phone and email support, as well as an area on the website with a knowledge base and other resources. At a price just under $1,900 – with 50 user “total protection” licenses for 12 months, including 24/7 phone and email technical assistance, next business-day replacement of hardware and firmware and software updates.

The appliance deploys quite quickly with the help of a short setup wizard. This wizard helps get the product up and running with a basic configuration in place. However, some of the configuration out of the box needs quite a bit of tweaking; this product does offer a lot of features for the cost.

Panda Security offers 24/7 support as part of its total protection package. Customers can access phone and email support, as well as an area on the website with a knowledge base and other resources.

At a price just under $1,900 – with 50 user “total protection” licenses for 12 months, including 24/7 phone and email technical assistance, next business-day replacement of hardware and firmware and software updates.

The appliance deploys quite quickly with the help of a short setup wizard. This wizard helps get the product up and running with a basic configuration in place. However, some of the configuration out of the box needs quite a bit of tweaking; this product does offer a lot of features for the cost.

The strength of this product is configurability. The FortiGate offers a lot of policy flexibility and configurable options with granular controls. Creating policies and rules for functions such as the firewall and web content filter is quite easy, but it is a manual process and does take some time to configure.

Documentation was comprised of a short quick-start guide that provided the steps for initial configuration, with a focus on configuring through the FortiExplorer application. Other guides provided included one for administrators and a few other supplemental materials.

Fortinet offers 90 days of eight-hours-a-day/five-days-a-week support included with the purchase and additional support is part of an annual contract thereafter.

At a price just under $850 for the appliance and the first year of security services – anti-virus, intrusion prevention, web filtering, anti-spam/application control FortiGuard Services updates, as well as eight-hours-a-day/five-days-a-week support and firmware upgrades – we find this product to be an excellent value for the money.

The second option is creating a blank desktop through the eGUI application and configuring all the zones and groups manually. Last year when we reviewed this product, we said it was complicated and confusing to set up and manage and that the eGUI design was uncomfortable to use. We have to say that since the last review we have spent a little more time getting to know how the gateProtect eGUI works, and we now can say that this interface is actually quite simple to use.

The company offers 30 days of support 24/7 via an online portal included in the price of the product. After the 90 days, customers can purchase additional support at various levels through a contract.

At a price just shy of $25,900 – including UTM software and one-year premium support – this product carries a very hefty price tag for a product in this category. However, based on its extremely flexible and easy-to-manage eGUI, we find it to be a reasonable value for the money.

This solution is intended for the very large and complicated infrastructures of large corporate environments, and the price definitely reflects that.

Panda Security offers 24/7 support as part of its total protection package. Customers can access phone and email support, as well as an area on the website with a knowledge base and other resources.

At a price just under $1,900 – with 50 user “total protection” licenses for 12 months, including 24/7 phone and email technical assistance, next business-day replacement of hardware and firmware and software updates.

The appliance deploys quite quickly with the help of a short setup wizard. This wizard helps get the product up and running with a basic configuration in place. However, some of the configuration out of the box needs quite a bit of tweaking; this product does offer a lot of features for the cost.
The Protector from SecPoint offers a combination of anti-virus, intrusion prevention system, web content filtering, application protocol blocking and spam protection in one appliance. The anti-virus engine is comprised of three engines – ClamAV, BitDefender and Kaspersky – that can be used separately or all together.

Installation and deployment is quite straightforward and it did not take us long to get the appliance up and running with a basic configuration. The product is deployed between the network and an existing firewall as it does not have a firewall of its own. After the appliance is placed into the network, the setup wizard can be accessed through the GUI. This wizard helps set basic network information and policy configuration. After the completion of the wizard, all further management is done through the web GUI.

We were pleased with the GUI that was used. Setting up the appliance as well as the configuration and management was easy through the web GUI with a user-friendly interface. We also found this to be a valuable tool for managing the appliance as it allows for easy access to the system through the web-based interface.

The quick-start guide provided a few short steps that made it easy to connect the appliance to the network and access the setup wizard.

As of a price of just $630 – including one-year licenses for intrusion detection and prevention, anti-virus and content filtering services – this product is an excellent value for the money for smaller environments looking for an affordable UTM with some good features.

**GROUP TEST | UTM**

**SecPoint Protector**

**VASCO Data Security aXsGUARD Gatekeeper**

**WatchGuard Technologies XTM 505**

**ZyXEL ZyWALL USG50**
The gods must be angry

The presence of more than 70,000 variants of the Zeus banking Trojan annually is any indication, the gods – especially the Greek “Father of Gods and Men” – must be very angry. Or, more likely, it is just criminal greed run amok. Whatever it is, malware such as Zeus is causing headaches in the financial services industry at record levels. The emergence of commercial-grade crimeware is arguably the number one threat to websites are limited to the list in the user attaches the dongle, available when the user is finished. That is all there is to it. The key piece of this, of course, is that the IronKey computer never goes where it is not supposed to be. Is it possible to circumvent the protection? Yes. However, there may be severe penalties if you do, such as being compromised. Those penalties could be quite costly, so there is an incentive to play by the rules. The most logical approach, of course, is to follow the NACHA and FBI guidelines and select one or more computers that can be designated as online banking computers. Those policies would not be used for anything else. There also is an available option that forces the use of IronKey.

The tool is fully encrypted and write-protected to Federal Information Processing Standards (FIPS), so stealing the device is not going to help the bad guys. Optionally, users can add an RSA SecureID for additional authentication. The product encrypts the computer’s keyboard so keyloggers are ineffective. The IronKey session is conducted within a virtual machine, so infections on the host computer do not affect the online banking sessions, which are isolated.

The IronKey device is moveable between computers, and the administrative console requires two-factor authentication. The admin console is simple to use and has lots of functionality. It is about what you’d expect from a first-class product in today’s market: statistics, trending, policy management and more. But there are some unique features as well, such as geolocation for events in the logs and Silver Bullet Services. These services provide assurance that IronKey devices are authorized and in good standing.

The system can be set to allow browsing to a number of selected websites. The IronKey Trusted Access for Banking service can prevent man-in-the-browser, keylogging, screen scraping and man-in-the-middle attacks. These are prevented because users cannot go where they are not supposed to, and browsing is secured through the Trusted Access Network, and online banking is conducted within a virtual machine. For the bad guys using crimeware, that means three strikes. You’re out! – Peter Stephenson

APRIL

InfoSec World Conference & Expo 2011 April 19-21

This annual event will deliver more than 70 sessions, dozens of case studies, multiple tracks, in-depth workshops, two co-located summits and more than 100 exhibitors. Providing education to all levels of information security pros, this gathering offers practical sessions that provide the tools to strengthen security implementations with-out interfering with business operations.

Venue: Orlando, Fla. Contact: msi.com

Infosecurity Europe 2011 April 19-21

Celebrating its 16th year, Infosecurity Europe provides an education program more than 300 exhibitors and a diverse range of new products and services. The free, three-day event draws on the experience of technical experts, government officials and end-users from high-profile corporations. The event enables security pros and business managers to establish a commercial justification for information security, refine their security policies, and select the most appropriate solutions to support their security strategy in order to safeguard their company’s reputation and assets.

Venue: London. Contact: infosec.co.uk

counter-eCrime Operations Summit 2011 April 26-28

This fifth annual gathering will be hosted by the Anti-Phishing Working Group (APWG) along with its sponsors, CyberSecurity Malaysia and MyCERT. It will engage questions of operational challenges and the development of common resources for first responders and forensic professionals who protect consumers and enterprises from the e-crime threat every day. Presenters will offer case studies of national and regional economies under attack, narratives of successful transnational forensic cooperation, as well as models for cooperation and uni-fied response against e-crime and data resources for forensic applications.

Venue: Kuala Lumpur. Malaysia Contact: apwg.org

counter-eCrime Operations Summit 2011 April 27-29

This is a meeting for IT and business execs and pros who are responsible for implementing and managing business process management. Learn more about technologies that enable business agility. Gather best practices on the art of process control. Become more efficient, consistent and competitive.

Venue: Baltimore. Contact:artner.com

JUNE

Int’l Cloud Computing Conference & Expo June 6-9

The organizing principle of this event is to ensure - through keynotes, sessions, and an expo floor – that attendees leave with abundant resources, ideas and examples they can apply immediately to leveraging the cloud, helping them to maximize performance and minimize cost.

Venue: New York. Contact: cisocloudcomputingexpo.com

MAY

SuperStrategies 2011 May 10-13

More than 70 topics will be presented at this gathering, including: how information as-surance contributes to meeting the organization’s goals and vision, auditing your customers, continuous monitoring for internal fraud and integrity, implementing risk-based audit-ing, complexities and challenges of implementing enterprise GRG, data risk management, red flags in vendor audits, and social network sites’ emergence.

Keynotes include Greg Ip, The Economist, speaking on the economic outlook for 2011.

Venue: Chicago Contact: msi.com

CISO Executive Forum May 11-12

The theme for this month’s event is privacy and law. The two-day gathering features speakers, panels, an expo pavili-on and plenty of opportunity for networking.

Venue: St. Paul, Minn. Contact:issa.org

SC Congress Canada June 14-15

SC Congress Canada is a unique conference and expo experience for the information security industry that offers up practical solutions to help private and public sector CISOs thwart cyber attackers, safeguard as-sets, come into compliance with countless regulatory mandates, and, ultimately, contribute to the overall profitability of their organizations. Information security leaders will be on hand to share their insight and knowledge so that attendees will leave armed with actionable information they can use to return once they offer their services.

Venue: Toronto. Contact: www.scmagazineus.com
Are you prepared for a breach?

Companies should take numerous steps to mitigate potential risks.

Taking a proactive approach to data breach issues is advisable, say Richard Blumberg and Gary Kibel.

Y ears ago, legally imposed data security requirements were rare and limited to those in specific industry niches. Those in the financial services industry had the Safeguards Rule under the Gramm-Leach-Bliley Act of 1999 (GLB) and members of the health care industry had the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Today, GLB and HIPAA are just the tip of the iceberg when it comes to laws that require an organization to implement, maintain and document adequate security measures, regardless of its line of business. In fact, a company can find itself under such an obligation through multiple sources. Therefore, a prudent firm should not wait until a clear and direct obligation exists before taking steps to secure its systems and processes. A legal obligation to do so may be just around the corner, or one may already exist unknown to the entity.

Contained within the American Recovery and Reinvestment Act of 2009 is the Health Information Technology for Economic and Clinical Health Act, or HITECH Act. One of the many changes brought on by the HITECH Act was the modification of HIPAA to significantly increase the obligations imposed on business associates. Business associates are those organizations that perform activities on behalf of a covered entity that involve protected health information.

The PCI Security Standards Council is continuously updating its data security standards (PCI DSS). PCI DSS was established by the credit card companies to ensure the security of cardholder data. Among the changes is a recognition of the various parties who may have access to cardholder data, and therefore, an assurance must be made that all such parties maintain adequate security over such data. Though this is a self-regulatory process, the PCI DSS has been incorporated into many state laws.

Perhaps overlooked are requirements that can be imposed on an organization merely by signing a contract with another business. Many business-to-business agreements contain data security requirements, sometimes buried within an exhibit to the contract.

How to respond? Companies should take numerous steps to mitigate potential risks, including: Maintain a written information security program, train employees, perform annual security assessments/audits, and use intrusion detection systems.

Despite a company’s best efforts, breaches can still occur. When they do, a company should first gather internal resources to review what type of incident has occurred. A team of individuals should be in place from human resources, legal, public relations, information technology and top management. IT should review the data that was potentially exposed to determine what type is involved. The type of data will determine if notification is required under state law. Next, notification letters to affected data subjects may need to be drafted in compliance with applicable state breach notification laws. If credit card data is involved, the company must notify affected card brands.

Call centers should be set up if the breached company does not have internal resources to handle calls. Automated systems should handle high volumes should the population exceed reasonable numbers. After the data breach is handled, the company should analyze the incident and outline potential areas of improvement to avoid future incidents.

Whether required by law, sound data security practices, and taking a proactive approach to these issues, is always advisable.

Richard Blumberg is director of data breach response services at Equifax, and Gary Kibel is a partner at Davis & Gilbert LLP.

Are you overpaying for Oracle Database?

Hint: you’re overpaying for Oracle Database.

The first thing to consider when thinking about DB2® for your business: it’s as low as 1/3 the cost of Oracle Database. Then consider DB2 on Power Systems™ with 3x the performance per core of Oracle Database on SPARC, in TPC-C and SAP SD benchmarks. Overall, an inoculated case for IBM. There’s more where that came from, too.
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. With a unified management console that scales to support small and large business networks, ESET NOD32 delivers advanced proactive protection for all your endpoints across Windows, Mac and Linux platforms.

Experience the difference for your business; request a Free Business Edition trial at www.eset.com/business_trial

© 2011 ESET, LLC. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, LLC. All other names and brands are registered trademarks of their respective companies.