FEATURES:

FLEXIBLE STANCE

Lofty Perch’s Mark Fabro is using his knack for communication to spread SCADA awareness  P20

Five more years
The new Canadian government is the same as the old – but with a majority vote. We explore the cybersecurity implications  PC1

Forensic intel
As breaches become the rule and not the exception, digital investigations are more important than ever  P28
Editorial

Accounting for transaction assurance

Given the majority of today’s headlines, the fact that nine out of 10 companies have been breached during the last year is far from shocking.

According to recent research from Ponemon Institute and Juniper Networks, many of the 583 U.S.-based IT and IT security practitioners responding to the survey have not only experienced a successful attack against their networks, but 59 percent of them have seen their infrastructures successfully compromised at least a couple of times during the year.

On the positive side, I suppose, most have been able to ferret out just where data was lost or exposed. In those instances where the IT pros were able to delineate the source, attacks typically were launched by outsiders.

The news seems to mirror just a couple of stories that emerged across North America recently. In June, 283,000 Honda and Acura customers in Canada fell victim to attackers hitting the companies’ websites to steal customer information stored in a database. Meanwhile, Citibank in the United States reported that same month that cybercriminals had penetrated its online banking platform, likely exposing the personally identifiable information of about 200,000 customers.

Insider abuse is still a huge problem, as well. Even with the updates to Federal Financial Institutions Examination Council (FFIEC) guidance that were released in July, which direct financial institutions conducting “high-risk transactions” to implement layered security to mitigate threats, the breach of Citibank’s transaction platform likely would have been successful, say many experts. While the FFIEC document defines layered security as “different controls at different points in a transaction process,” calling for dual customer authorization or transaction monitoring/anomaly detection, most banks haven’t really begun investing in such tools, experts contend.

That’s why, for the 2012 SC Awards U.S., we’ve added new categories to account for technologies that help to minimize online fraud. Most organizations are reliant on their web presence to conduct transactions with their customers. Finding the best ways to safeguard these exchanges is critical.

The deadline to submit nominations for the SC Awards is Aug. 26. You can visit www.scmagazineus.com/awards to learn more. We’ll look to celebrate finalists and winners in all the groups during February’s RSA Conference in San Francisco. Stay tuned for more details.

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

Most banks haven’t really begun investing in [layered security] to mitigate threats.”
SAFE NEVER SLEEPS.

Safe is advantage.
Safe is profit.
Safe is outright liberating.

But safe doesn’t come easy.
Especially when the dark forces are plotting night and day.

It requires that delicate combination of brains and obsession.
A brutally effective, global team that can snuff out danger before it gets dangerous.

That’s McAfee, the world’s largest dedicated security company.

We live and breathe digital security. Our job is to stay one step ahead.

We know that today real security isn’t about “where,” it’s about everywhere.
Every device, every connection, every location, every second.

It’s because we never sleep, that you can sleep better.

©2011 McAfee, Inc. All rights reserved.

www.mcafee.com/safe
Implementing fixes
What can companies do to protect their end-users and their own critical data as staff accesses social networking sites daily? We discuss best practices and other tactics and tools.

ON DEMAND
Perimeter security
Border defense still has a role in a company’s security architecture, but just what is it? The perimeter has been described as the ‘hard shell’ on the outside of a network that protects the ‘soft’ inside, which has led to a promotion of a defense-in-depth security approach.

Securing the cloud
Enterprise end-users are becoming more reliant on cloud computing applications and virtualized environments to enable the quick sharing of information. And while some companies are being cautious with their moves to the cloud, others are taking some risks.

FOR MORE INFO
For information on SCWC 24/7 events, please contact Natasha Mullia at natasha.mulla@haymarketmedia.com.

Shouldn’t you be demanding more from your SSL solution than just encryption?
VeriSign® SSL, now from Symantec, includes more than just industry-leading authentication and encryption. You can add a daily website malware scan for increased protection. You can make your customers feel more protected and generate more site traffic by displaying the VeriSign seal in search results. All at no extra cost. Chosen by over 93 percent of the Fortune 500® VeriSign SSL is setting a whole new standard for online security and trust. See for yourself with a 30-day free trial at verisign.com/ssl/free-30day-trial
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, United States in North America and India in the Asia-Pacific region. Source: Symantec

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

VANCOUVER, B.C. — The website of grocery store chain T&T Supermarket was struck by a cyberattack, resulting in the exposure of 58,000 customer names, contact details, usernames and passwords. Website visitors also might have been tricked into downloading malicious software onto their computers.

CHICAGO — Retail chain Michaels was recently hit with a second lawsuit over a point-of-sale skimming attack that affected stores in at least 20 states. The latest class action suit, filed in U.S. District Court in Illinois, claims the craft chain failed to secure its payment terminals and took too long to notify customers of the breach.

ABILENE, KAN. — Cybercriminals stole $63,000 from the bank account of the car dealership, Green Ford Sales, after infecting the PC of the company’s controller with the data-stealing trojan Zeus. The company’s bank, First Bank Kansas, has recovered all but $22,000 of the fraudulently transferred funds.

BALTIMORE — A disgruntled former employee of the city’s Substance Abuse Systems treatment and prevention authority was sentenced after hacking the corporate network to display porn in the CEO’s computer presentation. Walter Powell, 52, received a two-year suspended sentence and three years of probation.

TURKEY — The hackivist collective Anonymous took credit for infiltrating and defacing 74 government websites as a protest to web-filtering regulations set to take effect in August. In June, Turkish authorities charged 32 people with ties to Anonymous following DDoS attacks. Both incidents are related to the group’s so-called “AntiSec” movement.

GERMANY — Two men, 18 and 23, were sentenced for using trojans to hack into computers of record executives that contained unreleased songs and photos belonging to popular musicians, including Lady Gaga and Kesha. The younger of the two intruders earned 18 months in prison, while the other received an 18-month suspended sentence.

RUSSIA — Two hackers are believed responsible for stealing more than $500,000 from bank accounts in Turkey. Authorities believe the men tricked users into installing keylogger trojans on their computers, which enabled the crooks to gain access to their bank accounts to conduct 265 fraudulent transfers between 2005 and 2007.

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

U.K. — A 26-year-old Yorkshire man was charged with trying to hack the internal system of Facebook. He was arrested following an investigation launched by the FBI and Metropolitan Police. The suspect was released on bail, but faces extradition to the United States, where he could receive up to 10 years in prison. No Facebook data was compromised.

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

JAPAN — Medium-level activities
Parliament passed a law that sets penalties for convicted malware creators and purveyors. A guilty ruling can send virus writers to prison for up to three years and fine them as much as $6,200, while malware spreaders can receive two years behind bars and fines of $3,700. The law also permits cops to confiscate email communications of suspects from ISPs.

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

ABILENE, KAN. — Cybercriminals stole $63,000 from the bank account of the car dealership, Green Ford Sales, after infecting the PC of the company’s controller with the data-stealing trojan Zeus. The company’s bank, First Bank Kansas, has recovered all but $22,000 of the fraudulently transferred funds.

BALTIMORE — A disgruntled former employee of the city’s Substance Abuse Systems treatment and prevention authority was sentenced after hacking the corporate network to display porn in the CEO’s computer presentation. Walter Powell, 52, received a two-year suspended sentence and three years of probation.

TURKEY — The hackivist collective Anonymous took credit for infiltrating and defacing 74 government websites as a protest to web-filtering regulations set to take effect in August. In June, Turkish authorities charged 32 people with ties to Anonymous following DDoS attacks. Both incidents are related to the group’s so-called “AntiSec” movement.

RUSSIA — Two hackers are believed responsible for stealing more than $500,000 from bank accounts in Turkey. Authorities believe the men tricked users into installing keylogger trojans on their computers, which enabled the crooks to gain access to their bank accounts to conduct 265 fraudulent transfers between 2005 and 2007.

CHICAGO — Retail chain Michaels was recently hit with a second lawsuit over a point-of-sale skimming attack that affected stores in at least 20 states. The latest class action suit, filed in U.S. District Court in Illinois, claims the craft chain failed to secure its payment terminals and took too long to notify customers of the breach.

VANCOUVER, B.C. — The website of grocery store chain T&T Supermarket was struck by a cyberattack, resulting in the exposure of 58,000 customer names, contact details, usernames and passwords. Website visitors also might have been tricked into downloading malicious software onto their computers.

SEAL BEACH, CALIF. — The names and Social Security numbers of 300,000 individuals who applied for state benefits was posted online. The data was exposed by Southern California Medical-Legal Consultants, which helps medical providers recover insurance.

ABILENE, KAN. — Cybercriminals stole $63,000 from the bank account of the car dealership, Green Ford Sales, after infecting the PC of the company’s controller with the data-stealing trojan Zeus. The company’s bank, First Bank Kansas, has recovered all but $22,000 of the fraudulently transferred funds.

BALTIMORE — A disgruntled former employee of the city’s Substance Abuse Systems treatment and prevention authority was sentenced after hacking the corporate network to display porn in the CEO’s computer presentation. Walter Powell, 52, received a two-year suspended sentence and three years of probation.

TURKEY — The hackivist collective Anonymous took credit for infiltrating and defacing 74 government websites as a protest to web-filtering regulations set to take effect in August. In June, Turkish authorities charged 32 people with ties to Anonymous following DDoS attacks. Both incidents are related to the group’s so-called “AntiSec” movement.

RUSSIA — Two hackers are believed responsible for stealing more than $500,000 from bank accounts in Turkey. Authorities believe the men tricked users into installing keylogger trojans on their computers, which enabled the crooks to gain access to their bank accounts to conduct 265 fraudulent transfers between 2005 and 2007.

CHICAGO — Retail chain Michaels was recently hit with a second lawsuit over a point-of-sale skimming attack that affected stores in at least 20 states. The latest class action suit, filed in U.S. District Court in Illinois, claims the craft chain failed to secure its payment terminals and took too long to notify customers of the breach.

VANCOUVER, B.C. — The website of grocery store chain T&T Supermarket was struck by a cyberattack, resulting in the exposure of 58,000 customer names, contact details, usernames and passwords. Website visitors also might have been tricked into downloading malicious software onto their computers.
The SEGAPass website was hit by hackers.

**Top 10 malicious programs**

- **AdWare on top**
  - **AdWare.Win32.FunWeb.id**
  - **Trojan-Downloader.JS.Agent.izq**
  - **AdWare.Win32.FunWeb.ip**
  - **Trojan.JS.Popupper.aw**
  - **Trojan.JS.Redirector.pz**
  - **Trojan.HTML.frame.dl**
  - **Trojan.JS.Redirector.qa**
  - **Trojan.JS.Redirector.py**
  - **Trojan.JS.Redirector.qb**
  - **Exploit.HTML.CVE-2010-4452.bc**

**Malware Vertical encounter rate**

- **158% IT & telecom**
- **146% Education**
- **123% Retail & wholesale**
- **108% Banking & finance**
- **108% Food & beverage**
- **85% Government**
- **77% Health care**

**Phishing** A modest three percent drop

- **25,000**
- **22,500**
- **20,000**
- **18,079**
- **17,586**
- **17,376**
- **16,355**

After a rather significant, 33 percent spike in phishing attacks recorded in May, the June numbers, although still high, saw a modest three percent drop. The composition of attack methods remained nearly unchanged – 81 percent of phishers used hijacked websites to launch their attacks. Commercial hosting, free hosting and compromised computers represented hosting methods used in lower ratios through last month.

**Top breaches of the month**

- **Sega London**
- **Sony Pictures New York**
- **Citibank New York**

 After a rather significant, 33 percent spike in phishing attacks recorded in May, the June numbers, although still high, saw a modest three percent drop. The composition of attack methods remained nearly unchanged – 81 percent of phishers used hijacked websites to launch their attacks. Commercial hosting, free hosting and compromised computers represented hosting methods used in lower ratios through last month.

**Zombie IPs**

- **India 17.3%**
- **Brazil 10.3%**
- **Russia 5.4%**
- **Vietnam 8.0%**
- **Other Asia 18.9%**
- **China 3.8%**
- **Pakistan 3.1%**
- **Indonesia 4.2%**

The biggest increases in month-over-month zombie activity occurred in India, Vietnam and China, while the largest decreases were evident in Russia and “other” European nations.

**Spam rate** Compared to global email

- **0%**
- **50%**
- **100%**
- **150%**
- **200%**

The chart above reflects the encounter rate of web malware across a selection of industry verticals. Rates above 100 percent reflect a higher-than-median rate of encounter and rates below 100 percent reflect a lower-than-median rate, becoming obsolete.

**Top 5 attacks used by U.S. hackers**

1. Zeus trojan
2. Gbot trojan
3. Sinowal trojan
4. Adclicker trojan
5. TDSS Downloader trojan

**Top 5 attacks used by foreign hackers**

1. SpyEye trojan
2. Zeus trojan
3. Rogue DCHP trojan
4. Sinowal trojan
5. TDSS Downloader trojan

There were 1,380,556 attacks in the United States last month, primarily originating from Scranton, Pa.; Chicago; Atlanta; Dallas; Redwood City, Calif. There were 588,367 foreign attacks last month, primarily originating from Seoul, S. Korea; Odessa, Ukraine; and Beijing and Guangzhou, China.

**Top 10 spyware threats**

1. **Trojan.Win32.Generic Trojan**
2. **Zugo Ltd (v) misc. (general)**
3. **INF.Autorun (v) trojan**
4. **Exploit.PDF-JS.Gen (v) exploit**
5. **Trojan.Win32.Jppgiframe (v) trojan**
6. **Trojan.JS.Redirector.cd (v) trojan**
7. **Trojan-Spy.Win32.Zbot.gen trojan**
8. **Pinball Corporation (v) adware (general)**
9. **Adware.Win32.Gen adware (general)**
10. **GameVance adware (general)**

Phishing scams have become increasingly common on social networking sites as fraudsters have become savvier and bolder in their attacks. In recent months, scammers have used surveys, competitions and the promise of adult content to entice internet users into divulging their personal information. (v) is a detection that has come directly from VIPRE. Source: Sunbelt Software

**Spam rate indicates the accumulated emails tagged as unsolicited.** Source: Frost & Sullivan Report

**Phishing threat activity (global)**

- **USA 12.23%**
- **Indonesia 9.62%**
- **Japan 6.82%**
- **Canada 5.60%**
- **Italy 4.48%**

534,801,553 (as of July 7)

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

Transport Canada has warned of inadequate security at the nation’s airports in a recent review. The report suggests that attackers could enter planes using phony boarding passes. The review of the Canadian Air Transport Security Authority, originally commissioned last year by then-Transport Minister John Baird, highlighted the possibility of using fake or duplicated boarding passes to get onto a plane.

**THE QUOTE**

APT is when someone does everything security says they should and still gets owned.”

—Dan Kaminsky, security researcher

**THE SC MAGAZINE POLL**

What is your take on LulzSec?

- 15% They will help expose wrongdoing and secrets.
- 18% I like the lulz
- 34% They are nothing more than mischief-makers.
- 32% They will prompt companies to better safeguard their assets.

To take our latest weekly poll, click on [www.scmagazineus.com](http://www.scmagazineus.com).

**THE STATS**

- **50 days**
  - LulzSec said it was “disrupting and exposing corporations, governments... the general population...”

- **700 documents**
  - nabbed from the Arizona Department of Public Safety released by LulzSec in June.

**Debate**

**FOR**

The Obama administration’s proposed increase in the sentences cyberattackers can face sends an important deterrent message. As we continue to see on an almost daily basis, attacks are difficult to stop, can have millions of victims and can be launched from anywhere in the world. Cybercriminals who target the most sensitive government and private networks — to steal or attack critical national security, corporate and personal information — need to know they will face serious penalties. While the message will not be heeded by every attacker, the proposed increase in the applicable statutory maximum term of imprisonment gives prosecutors important flexibility in sentencing those who target our most sensitive computer networks. And it sends a significant message about the seriousness with which the United States takes cyberattacks, which can provide an example for other countries, encouraging them to take the problem more seriously. The higher potential prison sentences for violations of the U.S.’s Computer Fraud and Abuse Act (CFAA) gives law enforcement the authority to pursue cybercrime, and is an important component of the trust framework for online communications. However, court decisions have extended its reach well beyond the computer hacking it was enacted primarily to address. CFAA liability turns on whether one “accesses” a computer “without authorization” or in “excess of authorization.” To some prosecutors and courts, this means one violates the CFAA if they don’t adhere to the terms of service when using something like MySpace or Facebook because they are “accessing” their computers in excess of authorization. Prison, fines and lawsuits for violating terms of service? Let’s fix the statute first so everyone understands what it prohibits. Then, we can decide whether the administration’s proposal to double penalties, impose mandatory minimum sentences, eliminate first-time offender provisions, and subject the family home to forfeiture, on account of CFAA violations of a wayward teenager in his bedroom, should become law.

**AGAINST**

The Computer Fraud and Abuse Act (CFAA) gives law enforcement the authority to pursue cybercrime, and is an important component of the trust framework for online communications. However, court decisions have extended its reach well beyond the computer hacking it was enacted primarily to address. CFAA liability turns on whether one “accesses” a computer “without authorization” or in “excess of authorization.” To some prosecutors and courts, this means one violates the CFAA if they don’t adhere to the terms of service when using something like MySpace or Facebook because they are “accessing” their computers in excess of authorization. Prison, fines and lawsuits for violating terms of service? Let’s fix the statute first so everyone understands what it prohibits. Then, we can decide whether the administration’s proposal to double penalties, impose mandatory minimum sentences, eliminate first-time offender provisions, and subject the family home to forfeiture, on account of CFAA violations of a wayward teenager in his bedroom, should become law.

**WHAT IS IT?**

A large number of vulnerabilities are reported in Sun/Oracle Java SE, which affect JDK and JRE 6 Update 25 and earlier, JDK 5.0 Update 29 and earlier and SDK 1.4.2_31 and earlier.

**HOW DOES IT WORK?**

The critical vulnerabilities exist in various libraries and are of different classes. These range from a use-after-free error in the JP2EPXR plug-in (when cloning the underlying DOM element) to multiple integer overflow errors in cm.dll (when parsing various structures in color profiles) and a stack-based buffer overflow in jsound.dll within the “XExpand-Affl inflammation” function (when parsing IMA4 compressed soundbank streams).

**SHOULD I BE CONCERNED?**

Anyone with a vulnerable version installed should be very cautious when viewing web pages containing Java content.

**HOW CAN I PREVENT IT?**

Oracle released updated versions in June, which can be installed to address the vulnerabilities.

Source: Carsten Eiram, chief security specialist, SecureCode

---

**For more on LulzSec, see “The{lulz}ed” by Chris St.getParam(‘trafficData’).getName() in the next month’s SC Magazine.”

**THE PRICE OF PROGRESS**

LulzSec is disrupting the techno-geek industry’s self-image and showing that not everything is under control — at least not always.

CHRIS ST. GETHARDT, SC MAGAZINE

**THE MONTH**

Sun/Oracle Java SE

**THE WMAGAZINE POLL**

What is your take on LulzSec?

- 15% They will help expose wrongdoing and secrets.
- 18% I like the lulz
- 34% They are nothing more than mischief-makers.
- 32% They will prompt companies to better safeguard their assets.

To take our latest weekly poll, click on [www.scmagazineus.com](http://www.scmagazineus.com).

**THE STATS**

- **50 days**
  - LulzSec said it was “disrupting and exposing corporations, governments... the general population...”

- **700 documents**
  - nabbed from the Arizona Department of Public Safety released by LulzSec in June.

Source: LulzSec
Preparing for the inevitable

A dizzying string of high-profile data breaches this year, coupled with the staggering cost resulting from such exposures, has rattled up demand for cyber risk insurance.

This year, businesses are expected to take out about $800 million in policies, according to estimates from Betterley Risk Consultants. The insurance industry currently offers “first-party” policies, which cover the damage or theft of an organization’s assets, and “third-party” policies, which cover losses directly related to the breach, including customer attrition and victim notification.

Most of the interest now is around third-party policies for organizations that want to transfer risk, said Larry Clinton, president of the Internet Security Alliance.

Driving the up tick in demand is the rising cost of breaches and the realization that no organization is immune, Clinton said. Breaches cost organizations an average of $7.2 million in 2010, up from $6.8 million the previous year, according to a recent study by Symantec and the Ponemon Institute.

By purchasing third-party cyber risk insurance, organizations take an unknown – the eventual cost of the breach – and turn it into a known by paying a premium and deductible, said Rick Betterley, president of Betterley Risk Consultants.

“Instead of having a several million dollar loss, you pay a $100,000 premium,” he said.

The cyber insurance application process is often lengthy and requires a fair amount of work. But on the positive side, it can sometimes uncover weaknesses in an organization’s security posture not obvious before, Betterley said. Third-party insurance also provides, to some extent, a roadmap for responding to a breach, he added.

Such policies are highly attractive to midsize firms in particular, Betterley said. A recent study conducted by his company of middle-market organizations indicated that 25 percent of respondents planned to purchase cyber insurance in the next 18 months.

An insurance policy for cyber risks is not for everyone, though. Some small firms might find their level of risk does not justify the cost, Betterley said. Too, very large firms that are routinely breached may discover that cyber insurance premiums exceed the benefits they offer.

— Angela Montanaro

$800,000,000
Estimated volume of cyber insurance premiums purchased in 2011.

Source: Betterley Risk Consultants

Jobs market
Me and my job

Stiven Weidner
Manager, Business Continuity, Catholic Health East

How do you describe your job to average people?
My primary job is to help our physicians and clinicians provide health care services in the event of a crisis. I do this by creating systems and processes that work when the power goes out, information systems go down, or our facilities become unusable. As part of the information security office, I also have the opportunity to develop security policies and procedures, document and help coordinate security incidents and other issues, and support security assessments.

Why did you get into IT security?
Formerly, I was a network analyst tasked with protecting the company’s perimeter. Later, when managing global data centers, I worked to protect information from internal and external threats. My business continuity duties require me to identify and mitigate risk to the business from a loss of information integrity and availability. Working in the security office is actually an ideal spot for the business continuity professional, as many of the responsibilities for data protection cross over into both areas.

What was one of your biggest challenges? Convincing corporate executives that business continuity is more than backing up data. Business continuity protects the organization by ensuring critical functions continue, even in adverse conditions. Disaster recovery is really just a part of the overall business continuity program.

What keeps you up at night?
As the only business continuity professional in our organization, I continue to experience significant challenges implementing tools and processes when there are so many other competing priorities.

For what would you use a magic IT security wand? I’d use it to develop a single, integrated security tool that would solve all our current and future security issues — including business continuity, of course!

Skills in demand

With evolving technology and emerging threats, companies are struggling to find security engineers capable of managing and delivering projects.

What it takes
While strong technical skills are always in demand, the need for those who can design, integrate and operationalize security controls is significant. These roles include well-developed social skills, a clear understanding of technical requirements, a consultative approach and the ability to manage complex projects.

Compensation
Salary is similar to traditional security engineering roles — $90k to $120k — but the qualities that companies look for are changing.

— Jeff Coste, director, Araneus Consulting

Briefs
Company news

HyTrust, maker of virtualization security and compliance solutions, has named Mercy Caprara chief financial officer. She will be charged with driving and overseeing the company’s financial strategy and planning. Most recently, Caprara served as CFO of TriCipher, an identity services provider, recently bought by VMware. www.hytrust.com

Chris Hoff has joined Juniper Networks. The former director of cloud and virtualization solutions at Cisco, Hoff has said on his blog that he was drawn to Juniper for its staff, technology, execution and the “need to change the way the world thinks about, talks about and operationalizes security.” Hoff plans to continue to work on the nonprofit CloudAudit and the HackNsf Conference. www.juniper.net

DellSecureWorks has teamed up with Qualys to deliver vulnerability management services to its global base of customers. Under the partnership, DellSecureWorks will integrate, manage and resell the QualysGuard suite, which includes vulnerability management, web application scanning, and PCI and policy compliance services. www.dell.com/securerworks www.qualys.com

Dome9, provider of firewall management as-a-service for public and private clouds, including Amazon EC2 and RackSpace, has named David Meizlik vice president of marketing. Meizlik formerly served as director of product marketing and communications at Websense. www.dome9.com

Eddie Schwartz has been named the first-ever CSO of RSA. He assumes the role after EMC, which owns RSA, acquired NetWitness, a network monitoring firm where Schwartz served as CTO. At RSA, which sustained a high-profile breach in March, Schwartz will work with the internal security team and contribute to product strategy. www.rsa.com

SafeNet, maker of data protection and software rights management solutions, has named Chris Fedde president and CEO. He takes over for Mark Floyd. Fedde has been with SafeNet since 2001 and most recently served as president and COO. He has helped the company expand its market share in the federal government and commercial sectors. www.safenet-inc.com

WhiteHat Security, provider of web application security services, has acquired static code analysis firm Infrared Security. As part of the deal – terms of which were not disclosed – WhiteHat will add the technology to its dynamic vulnerability testing solution, WhiteHat Sentinel. www.whitehatsec.com

Jack Daniel has joined Tenable Network Security, provider of vulnerability scanning services, as product manager. Daniel is the co-founder of the Security BSides and director of the National Information Security Group (NAISG). www.tenable.com

Follow us on Facebook and Twitter

McDonald’s has named its 13th CEO, Steve Easterbrook. He replaces Don Thompson, who was tapped by McDonald’s to lead the turnaround that failed. www.mcdonalds.com
Sweat the small stuff

Ron Baklarz
CISO, Amtrak

O ver the last several weeks, we have seen high-profile cybersecurity breaches involving RSA, the CIA, Sony, the U.S. Senate and the FBI’s InfraGard name a few. What did we learn from the recent LinkedIn rash of high-profile security breaches? To me, it reinforces the concept of “sweating the small stuff,” or, simply, paying attention to the details germane to information security. These breaches are primarily the result of opportunistic attacks waged against exploitable and known vulnerabilities.

To support this position, consider June 27, when the Department of Homeland Security provided a Top 25 list of software errors. This list, called the Common Weakness Enumeration, develops a scoring system and risk analysis framework for evaluating the seriousness of flaws and prioritizing weaknesses. If you thought that this new list looks a lot like the OWASP (Open Web Application Security Project) Top 10 Web Application Security Risks, you would be correct. The OWASP Top 10 list has been around since about 2004, and scanning tools have been built to assess websites against the vulnerabilities included on the OWASP list. It would be reasonable to assume that security-conscious organizations would routinely assess their infrastructure against these standards.

According to a June Anti-Phishing Working Group (APWG) survey, the most targeted and attacked website suite of tools are ones that employ LAMP (Linux, Apache, MySQL and PHP/Java) as the application platform in 81 percent of attacks; Apache as the web server in 81 percent of attacks; MySQL as the database in 81 percent of attacks; and PHP/Java as the application platform in 82 percent of attacks. If not properly configured and maintained, the use of LAMP could be an extremely vulnerable combination of technologies and potentially rate it an organization’s cyber-risk factors.

When considering the LAMP model, the lack of security patch application in any one of the four technologies could provide attackers with an opening. In the breach of RSA earlier this year, it only took one or two employees to activate the phishing email. And, having a CISO responsible for cybersecurity might have negated or at least minimized Sony’s compromise.

While changing corporate cultures and practices with regard to security is extremely difficult, a sound information security posture includes the old but effective combination of security infused at the people, process and technology levels. In the rush to reach for the “clouds,” cut corners and save money, the security details can’t be overlooked.

---

Before we leave our discussion of phishing, there are several high-profile examples of expensive VoIP security breaches, and a disturbing portion of them have been caused by rather elementary security flaws, like weak passwords, the failure to detect rogue calls or even configure and maintain firewalls appropriately. It is unrealistic to rely on employees to be responsible for VoIP security. They just want an easy and reliable way to make calls. Fortunately, IT managers and CSOs can do several things to shore up their phone system.

Proper configuration of the firewall is especially important in an environment where the VoIP system is remotely accessible via the Internet. I recommend that only IP phones and the VoIP telephony provider’s servers be allowed to access the company’s private branch exchange (PBX). Strict firewall configuration is a preference, but a company may have mobile clients who change their IP addresses often.

In addition, password-protection techniques aren’t foolproof. A critical layer of defense also is creating systems that use “rules” and getting real-time alerts when they are violated. If an admin knows the business will never make an international call, then disable that capability. If that is not possible, limit the number of calls. Rules like these will tip an admin off to attacks and enable a quick reaction to minimize the damage.

APTs: New term, old problem

S culb divers are fond of saying that to survive a shark encounter you must only swim faster than your buddy. It is conventional wisdom in the security world too: If I have bars on my windows and you don’t, I’ll feel safer. But consider the elite security practitioners among us. Who has the talent, resources and motivation to protect their infrastructure, employees and customers? Are RSA and Google on your list of exceptional swimmers? They’re on mine, yet both have been reverbereating in the news under breathless headlines proclaiming a new era of advanced persistent threats (APTs). If their defenses weren’t adequate, what hope is there for the rest of us?

The truth is: We don’t know.

But we know (or should know) what we have that is of value. In a broad sense, we also know what kinds of harm can come to those valuables (see “confidentiality, integrity, availability, breach thereof”). We also know that we’re immersed in a threat/countermeasure arms race that started decades ago when we learned that some people who use computers—shudder, I know—cannot be trusted. While it is true that more and more sophisticated techniques increasingly target applications, content and consumers of content (namely, human beings), we’re well advised to come up for air just long enough to remember that attackers will use the simplest approach available to get the job done.

So let’s pause for a reality check. Do we have a clear sense of what we need to protect and where it is? Do our employees know what is expected of them? Do they have our trust and confidence? Are we focused on protecting things of value from risk or harm, or are we bogged down on regulatory compliance issues?

There may come a time when the fastest swimmers are the ones with no secrets to protect at all. Until then, let’s forgo the APT hysteria long enough to make sure we’re doing a good job on the fundamentals.

---

Will Irace
director of threat research, Fidelis Security Systems

Simple best practices for VoIP

T he cost savings and flexibility benefits of voice-over-Internet protocol (VoIP) have made the technology popular with enterprises and small businesses alike. However, as its prevalence has grown among business users, so has its popularity among hackers.

There are several high-profile examples of expensive VoIP security breaches, and a disturbing portion of them have been caused by rather elementary security flaws, like weak passwords, the failure to detect rogue calls or even configure and maintain firewalls appropriately. It is unrealistic to rely on employees to be responsible for VoIP security. They just want an easy and reliable way to make calls. Fortunately, IT managers and CSOs can do several things to shore up their phone system.

Proper configuration of the firewall is especially important in an environment where the VoIP system is remotely accessible via the Internet. I recommend that only IP phones and the VoIP telephony provider’s servers be allowed to access the company’s private branch exchange (PBX). Strict firewall configuration is a preference, but a company may have mobile clients who change their IP addresses often.

In addition, password-protection techniques aren’t foolproof. A critical layer of defense also is creating systems that use “rules” and getting real-time alerts when they are violated. If an admin knows the business will never make an international call, then disable that capability. If that is not possible, limit the number of calls. Rules like these will tip an admin off to attacks and enable a quick reaction to minimize the damage.

---

Speak truth, not spin

Ron Baklarz says he was dismayed by the post-compromise, defensive articulation by RSA and Sony that they had been victimized by extremely sophisticated attacks.

“APTs, in fact

It turns out that RSA was victimized by an advanced persistent threat (APT)-type attack that began with a relatively unsophisticated attack, but successful phishing email compromise.

Have personnel in place

Further, he says, with 12,000 subsidiaries and approximately 168,000 employees, Sony did not have anyone in a CISO capacity. It is currently scrambling to fill this position.

Fill the hols

Someone once said, “To attack us, the terrorists only have to be right once. To stop them we have to be right 100 percent of the time.” This holds true in cybersecurity as well.

It is unrealistic to rely on employees to be responsible for VoIP security.”
The mere mention of a risk assessment can instill myriad responses from the targets of the request. Resistance, fear and the age-old, “We don’t have the time or resources,” are the usual responses when departments are approached with this subject. Who can blame them? It is like getting a letter from the IRS saying you are going to have your income tax returns audited. You know you didn’t do anything wrong. Well, not on purpose. Everything is in order. You think. You did the best you could to follow their rules and regulations. Why you?

Enterprises can achieve ROI by doing an in-house risk assessment, says Kris Rowley, CISO of the state of Vermont.

The same goes for risk assessments. The number of state and federal regulations change on what seems to be a monthly basis. They become more convoluted, complex and demanding all the time. States, companies, health care providers and businesses do their best to keep up and stay compliant, but it is an uphill battle. However, it is a battle that needs to be fought.

One of the keys to doing a successful risk assessment is to get buy-in from those departments that need to do the assessments. As security professionals, it is our job to help IT employees and business managers understand this process and the reasoning behind it. It is important that they realize that a risk assessment is not being done for punitive purposes, but rather, as a proactive process within the security framework of the enterprise.

Risk assessments can be outsourced to third parties, and a professionally written report will be returned with all the results and answers to all your questions. However, in the long run, this might not be an approach that will best meet the needs of your organization. There are many benefits to doing an in-house risk assessment. Besides the obvious benefits of determining compliance with numerous state and federal regulations, application inventory, security controls and all the other requirements of whichever standard measure is being used (NIST, ISO, FIPS, etc.), there are numerous secondary benefits that cannot be achieved by a third-party assessment.

Foremost, there is a transfer of knowledge from the security professional to the business unit or IT staff regarding security awareness and best practice. People involved in the assessment project will be confronted with questions and, in working with a security professional, there will be a gradual propagation of knowledge that will help to change their perspective regarding information security.

The image of security being the “bad guy” may also find some resolution by doing an in-house risk assessment. Enterprise environments tend to be large and spread out and, subsequently, departments are isolated from each other. It is easy for a bad image to propagate in such an environment. Security is usually the department telling others that they cannot do what they want to do. Increased communication and collaboration between departments and security during a risk assessment may help to mitigate that stigma along with the risks. It is difficult to maintain a negative opinion once people work together and get to know each other as individuals.

Kris Rowley is CISO of the state of Vermont. She is also on the governance board for the Norwich University Advanced Computing Center, teaches at a local community college and does information security presentations for community education.
Mark Fabro successfully married tech knowledge and C-level chops to help elevate his role and SCADA security to the next level. Dan Kaplan reports.

There was a time in Mark Fabro’s career when he was perfectly content avoiding the men and women in the corner offices. After all, it was the early 2000s and Fabro was buried deep in the weeds of critical infrastructure research, focusing on challenges like threat profiling and recognition, risk analysis, intrusion testing, data collection and “grid” cracking. Coveted skills, for sure, but not something to which a power company CEO was giving much thought at the time.

“Really, the insider was one of the only things you had to worry about, other than natural or manmade system incidents or failures that could impact production,” recalls Fabro.

Then, around the middle of the decade, things started to quickly change. The systems that manage, direct and regulate utilities, like chemical plants and oil-and-gas refineries, increasingly became connected to the public internet and the corporate network, effectively opening the door for the first time to the threat of malware.

All of a sudden, the prospect of a hacker shutting off the lights to millions of people shifted from a Hollywood script idea to something that could at least pass the plausibility test.

The men and women in the boardroom started perking up. And with that, Fabro’s career path changed.

Suddenly came the need for people with technical talents who could also convey the threat and business challenge posed by supervisory control and data acquisition (SCADA) systems to upper management, in easy-to-understand terms.

Fabro, who now serves as president and chief scientist of Lofty Perch, was a natural. In June, as a testament to his work in this field, he was named information security professional of the year at the 2011 SC Awards Canada.

Fabro, whose company specializes in assessments, training and compliance strategies for critical infrastructure teams, says industrial control systems – which provide “national security, economic security and quality of life” – traditionally were isolated from the corporate environment. But that changed with the rise of internet connectivity.

“The business demanded they start getting connected and working together,” Fabro, 44, explains. “Now you have executives who want to instantaneously know what’s going on in the control system environment. The competitive advantage lies in how fast you can get situational awareness from your control system into the corporate space to shape and meet supply and demand.”

With each passing year, Fabro’s skill set has become more valuable. Back in 2007, the largest SCADA-related headline-grabber was the release of a video, produced for the U.S. Department of Homeland Security, which depicted a “hacker”-controlled turbine shaking wildly until pieces break off and plumes of smoke fill a test lab.

But it wasn’t until 2010, with the emergence of Stuxnet, the first malware ever written specifically for industrial control systems, that the narrative of a ticking time bomb really took flight. Stuxnet gave life to additional research, and so far this year, the relatively nascent U.S. Industrial Control Systems Cyber Emergency Response Team, part of US-CERT, revealed a number of vulnerabilities affecting SCADA products. Not all have been particularly serious, but their evidence shows that researchers are paying close attention.

And most critical infrastructure operators, as well as product vendors, don’t appear entirely ready to battle these new threats.

According to a joint study earlier this year from McAfee and the Center for Strategic and International Studies (CSIS), which surveyed 200 IT security executives working at utilities in 14 countries, 40 percent believe their sector’s vulnerability to attack has increased since last year.

Meanwhile, vendors have been slow to respond to product vulnerabilities, as they are not used to dealing with critical flaws that need quick patching.

Enter Fabro

Michael Assante, the former chief security officer at the North American Electric Reliability Corp., which oversees U.S. electric grid operators, says he contracted Fabro a few years ago to work with the utilities so they could better understand their risks.

“One of the major contributions that Mark brought to the table is the issue of understanding cybersecurity in the context of industrial technology, control systems and SCADA,” Assante says. “Mark does an incredible job of bridging the gap between the hard, technical story and how it matters to you. He just has a lot of resonance when he speaks.”

Assante cites his reasonable and responsible approach that never relies on the fear card. Fabro also has a way of connecting – not just with business executives – but also those SCADA experts who may not be too familiar with cybersecurity.

“The other very important element is Mark can sit down with a control systems engineer and have the capability of communicating,” Assante says.

“He can translate how you think about security, knowing the mission is to keep that system up and running.”

Mark Fabro, president and chief scientist of Lofty Perch
Experts preach patience as the control system community matures.

“We're somewhere in the early to mid-90s right now, compared to quote-unquote internet security. There really isn’t much awareness yet. We just aren’t a lot of guidelines for folks to follow. It’s a very new juncture.”

“But this general lack of polish around SCADA security doesn’t mean the systems are not vulnerable.”

“With the amount of records going on in these industrialized systems, it would be foolish to think that an adversary is not interested in compromising an element of the North American critical infrastructure.”

“With the amount of records going on in these industrialized systems, it would be foolish to think that an adversary is not interested in compromising an element of the North American critical infrastructure.”

“So be prepared to see some things that are exciting simply can’t fix.”

“So what are some of the major challenges the industry faces? Help us separate the FUD from the reality.”

“As of late, the industry seems to be having some difficulties showcasing the great work it has been doing, and there seems to be a continuous surge of nay-sayers that just do not want to support the fact that we are making progress.”

“There is a very large amount of vulnerability research being released that seems to take priority and overshadow their efforts. In a post-Stuxnet world, the public seems to be more concerned with the hype surrounding each and every vulnerability rather than some of the great work being done by vendors, asset owners and information-sharing communities.”

“Once an adversary is able to get through the vendor access channel or corporate domain, they find themselves in an environment that is sensitive to enumeration and large data bursts.”

“The IT profile of many of these critical infrastructure systems is circa 1995.”

“Mark Fabro: SCADA security can be unexciting at the best of times, and unless you create interest, you risk having key decision makers not get on board with the cause. Having been in cybersecurity for almost 20 years, and focused on SCADA, control systems, and critical infrastructure for about 12 of those, the diversity of cultures demands you discover creative ways to get the message across. But the technologist has not gone away, and in fact those skills are called upon almost every day to help shape the solutions and countermeasures that passion and excitement simply can’t fix.”

“SCADA: Protecting the smart grid (which delivers electricity to suppliers to consumers using two-way digital technology) is obviously a focus for power companies. Is enough being done in this area?”

“French: The smart grid is, of course, on everyone’s utility’s agenda, and security is a key focus area. There is a lot of activity in the security area, but the responsibility to secure the architecture includes the asset owners and the vendors and others that provide communications (i.e., backbone).”

“I believe that we as a community need to do a better job at trying to define just what the smart grid is, as it can mean a lot of things to a lot of people, and that can shape how security is approached. There are many parts to this thing.”

“There are many different technologies involved that do a lot of different things and each one needs to be looked at from a security perspective.”

“SC: Aside from your work at Lofty Perch, can you describe some other projects with which you are involved?”

“MF: I have a few things that are ongoing, and almost all of them are in support of outreach and education. I am lucky to be involved in the Canadian Industrial Cybersecurity Council, which I chair, and our focus is to review Canadian public sector security activities or programs and ensure they take into account vital SCADA and control systems.”

“MF: My experience has taught me that strong SCADA/control systems security programs are created by teams – teams that are comprised of both IT security and control system engineers. Modern SCADA and control systems have matured to be very IT-based, but the uniqueness and nuances associated with industrial automation simply does not allow for IT security best practices to always be mapped directly.”

“I recommend that collaborative teams be formed, and that the great products developed by ISA (International Society of Automation), NIST or the Department of Homeland Security Control Systems Security Program (CSSP) be used as a starting foundation for program development.”

“MF: As of late, the industry seems to be having some difficulties showcasing the great work it has been doing, and there seems to be a continuous surge of nay-sayers that just do not want to support the fact that we are making progress.”

“There is a very large amount of vulnerability research being released that seems to take priority and overshadow their efforts. In a post-Stuxnet world, the public seems to be more concerned with the hype surrounding each and every vulnerability rather than some of the great work being done by vendors, asset owners and information-sharing communities.”

“Once an adversary is able to get through the vendor access channel or corporate domain, they find themselves in an environment that is sensitive to enumeration and large data bursts.”

“The IT profile of many of these critical infrastructure systems is circa 1995.”

“Mark Fabro: SCADA security can be unexciting at the best of times, and unless you create interest, you risk having key decision makers not get on board with the cause. Having been in cybersecurity for almost 20 years, and focused on SCADA, control systems, and critical infrastructure for about 12 of those, the diversity of cultures demands you discover creative ways to get the message across. But the technologist has not gone away, and in fact those skills are called upon almost every day to help shape the solutions and countermeasures that passion and excitement simply can’t fix.”

“There are many different technologies involved that do a lot of different things and each one needs to be looked at from a security perspective.”

“SCADA: Protecting the smart grid (which delivers electricity to suppliers to consumers using two-way digital technology) is obviously a focus for power companies. Is enough being done in this area?”

“French: The smart grid is, of course, on everyone’s utility’s agenda, and security is a key focus area. There is a lot of activity in the security area, but the responsibility to secure the architecture includes the asset owners and the vendors and others that provide communications (i.e., backbone).”

“I believe that we as a community need to do a better job at trying to define just what the smart grid is, as it can mean a lot of things to a lot of people, and that can shape how security is approached. There are many parts to this thing.”

“There are many different technologies involved that do a lot of different things and each one needs to be looked at from a security perspective.”

“SC: Aside from your work at Lofty Perch, can you describe some other projects with which you are involved?”

“MF: I have a few things that are ongoing, and almost all of them are in support of outreach and education. I am lucky to be involved in the Canadian Industrial Cybersecurity Council, which I chair, and our focus is to review Canadian public sector security activities or programs and ensure they take into account vital SCADA and control systems.”

“MF: My experience has taught me that strong SCADA/control systems security programs are created by teams – teams that are comprised of both IT security and control system engineers. Modern SCADA and control systems have matured to be very IT-based, but the uniqueness and nuances associated with industrial automation simply does not allow for IT security best practices to always be mapped directly.”

“I recommend that collaborative teams be formed, and that the great products developed by ISA (International Society of Automation), NIST or the Department of Homeland Security Control Systems Security Program (CSSP) be used as a starting foundation for program development.”

“As of late, the industry seems to be having some difficulties showcasing the great work it has been doing, and there seems to be a continuous surge of nay-sayers that just do not want to support the fact that we are making progress.”

“There is a very large amount of vulnerability research being released that seems to take priority and overshadow their efforts. In a post-Stuxnet world, the public seems to be more concerned with the hype surrounding each and every vulnerability rather than some of the great work being done by vendors, asset owners and information-sharing communities.”

“Once an adversary is able to get through the vendor access channel or corporate domain, they find themselves in an environment that is sensitive to enumeration and large data bursts.”

“The IT profile of many of these critical infrastructure systems is circa 1995.”

“Mark Fabro: SCADA security can be unexciting at the best of times, and unless you create interest, you risk having key decision makers not get on board with the cause. Having been in cybersecurity for almost 20 years, and focused on SCADA, control systems, and critical infrastructure for about 12 of those, the diversity of cultures demands you discover creative ways to get the message across. But the technologist has not gone away, and in fact those skills are called upon almost every day to help shape the solutions and countermeasures that passion and excitement simply can’t fix.”

“There are many different technologies involved that do a lot of different things and each one needs to be looked at from a security perspective.”

“SCADA: Protecting the smart grid (which delivers electricity to suppliers to consumers using two-way digital technology) is obviously a focus for power companies. Is enough being done in this area?”

“French: The smart grid is, of course, on everyone’s utility’s agenda, and security is a key focus area. There is a lot of activity in the security area, but the responsibility to secure the architecture includes the asset owners and the vendors and others that provide communications (i.e., backbone).”

“I believe that we as a community need to do a better job at trying to define just what the smart grid is, as it can mean a lot of things to a lot of people, and that can shape how security is approached. There are many parts to this thing.”

“There are many different technologies involved that do a lot of different things and each one needs to be looked at from a security perspective.”
Will the new Canadian government make changes to the nation’s cybersecurity strategies? Danny Bradbury examines the agenda.

Canadian politics has been uncharacteristically dramatic of late. There have been two elections since 2006, the first resulting in a continued minority government, which left the Conservative party relatively constrained. However, the most recent election, held in May, saw the Conservatives finally gain a majority, effectively ensuring them a five-year term with greater powers.

What does this mean for cybersecurity? Will a more powerful government choose to drive home more stringent security measures in the same way that President Obama pushed through comprehensive initiatives south of the border in the early days of his administration?

It is worth looking at. Some of the security- and privacy-related legislation that the government was already trying to push through have all but disappeared. Most notably, Bill C-29, legislation designed to reform Canada’s federal privacy law, was killed before it could get beyond its second reading. This was a controversial proposal because it made the issue more open-ended and less defined.

The privacy bill likely died when Parliament adjourned in March, says Michael Geist, Canada research chair in internet and e-commerce law at the University of Ottawa. “PIPEDA faces another statutorily mandated review this year, so any future government is likely to wait for the results of that review before reintroducing privacy reform.”

Perhaps one bright spot, the government reappointed Privacy Commissioner Jennifer Stoddart for another three years. Significantly, Stoddart isn’t afraid to go against the government that appointed her, when necessary. She was among several privacy commissioners who, in a joint letter to the government in May, denounced a collection of draft bills concerning lawful access. The letter concerned one bill in particular, C-52, the Investigating and Preventing Criminal Electronic Communications Act. Stoddart, among others, was particularly concerned about the absence of limits on access powers, along with the wide scope of information required for warrantless collection by telecommunications firms.

“Read together, the provisions of bills C-50, C-51 and C-52 (augmented by changes in bills C-22 and C-29) would substantially diminish the privacy rights of Canadians,” said the letter. The bills make it possible for the government to access private information more readily while removing legal controls on the practice, it continued.

The Canadian Internet Policy and Public Interest Clinic at the University of Ottawa warns that the legislation, as previously drafted, would require telecoms to build spyware backdoors into their services, enabling law enforcement to more readily intercept communications. It would also allow authorities to identify anonymous online users, even when the information would not be useful in an investigation, the organization said.

A prevailing trend is the likely or promised reintroduction of legislation in the new parliament to amplify policy that was already laid out by the minority government. The Conservatives figure to more easily vote through legislation, and proposals that it reintroduces may be stronger than in the previous parliament.

Surveillance and laxer privacy legislation may be on the table, but what about the continuation of the government’s cybersecurity strategy? Its main commitments to the issue came in the form of an official strategy, launched after a couple of false starts in 2010. The strategy had three main purposes, says Nick Galletto, partner at Deloitte Canada. It was designed to secure government systems, encourage partnerships with the private sector and educate Canadian residents about basic cybersecurity issues.

Dave MacMahon of Bell Canada is a security expert who also works with SecDev, a Canadian company focused on internet security analysis and consulting, says the private sector is getting the short end of the stick. “The cybersecurity strategy for the government to date has been a strategy for the government, not for Canada,” he says.

“The strategy is about protecting the government infrastructure.”

But, starting security inside the government may yield some significant benefits, MacMahon says. He argues that the market is the most important driver for internet security. Money talks, and those organizations with the most cash can drive home the security message to technology vendors.

“We can measure the level of malicious traffic online after a policy document is put out, but the biggest force is the dollar,” MacMahon says.

Indeed, the federal government buys $14 billion worth of goods and services each year from suppliers. A procurement strategy focusing heavily on security would help to persuade vendors to include it in the products. This has already happened in the states. Last year, the New York Office of Cybersecurity and Critical Infrastructure Coordination introduced the Application Development Security Procurement Language, intended specifically for custom-code development. It outlined a template designed to make software projects more secure.

This has also happened at a federal level. In 2006, the U.S. Department of Energy unveiled a Cybersecurity Procurement Language for Control Systems, designed to nail down a procurement language for SCADA systems that could be used by the public and private sector alike.

This begs the question: How advanced is the Canadian government in building such procurement practices, both internally and for possible use by private sector organizations?

The government is engaging the business community to help pin down and protect critical elements from cyberattack. Through public works, it launched some initiatives around identifying and protecting the critical national infrastructure, Deloitte’s Galletto says.

“What will be interesting is whether any of this gets mandated through regulation, or whether it is a collaborative approach to ensure that they’re doing all the right things,” he says.

The next five years hold some significant challenges for the government as it continues to tighten up its security stance. One thing will be easier: introducing legislation that will raise the hackettes of privacy and digital rights groups. In this area at least, Canadian politics can only get more interesting.
Amid a hodgepodge of national laws, calls for a global data exchange standard grow louder, reports Greg Masters.

Pirates continue to plunder the sea lanes in some parts of the world, armed with AK47s instead of cutlasses, but a new iteration of piracy has become more common – this form well hidden from sight and employing nothing so primitive as swords or guns.

Today’s cyberthieves, armed with computers linked to the internet and a variety of hacking skills, can penetrate networks anywhere in the world to abscond with corporate treasures and violate the privacy of individuals. In fact, according to a recent report from the World Economic Forum, cybersecurity ranks in the Top Five “risks to watch” for stakeholders across government and the private sector.

But, just who is responsible for protecting the privacy of individuals and organizations – particularly when data traverses national boundaries – has become a hot topic for debate.

Despite 46 states having breach notification laws, and compliance mandates that order adherence to privacy restrictions, such as Sarbanes-Oxley and HIPAA, this country lags the European Union in prescriptive requirements, experts say. Europeans, far more sensitive to the possibility of data exposure, owing to their experiences under authoritarian regimes during World War II, passed the Data Protection Directive, which offers a comprehensive system throughout the EU that incorporates recommendations made 30 years ago by the Organization for Economic Cooperation and Development (OECD), an organization comprised of 34 countries that was founded in 1961. While the United States endorsed the OECD’s recommendations, it never implemented them.

“It would be nice if there was a standard way to do it,” she says.

Clients in each country must compile data transfer agreements that incorporate such standards as ISO 2700 or NIST. The next level implements standards from FISMA, a government dictate that adds another layer of data safeguards across the globe, she says.

“It would be helpful for corporations if there were a global standard with bare minimums, Titus says. “It would go a long way to create a framework beginning with the United States and the EU.”

There’s been a lot of dialog around such a development, but little to nothing has been actually implemented, she says.

Too, it is expensive to manage all the data privacy laws. “There’s no Gantt chart (a type of bar graph that illustrates the start and finish dates of a project)
that shows the country, the standards it upholds, and the gap between its’ and the United States.“ For example, he says, No one seems to have a workable response. Thompson is not aware of any group, public or private, moving toward a global standard that could take the guesswork out of the process. Nations and corporations are still grappling with what data is private and what needs to be protected, he says. “It is murky when moving data across borders,” Thompson says.

And this ambiguity is causing head-
aches for a lot of people and organiza-
tions. Those wishing to shop for a cloud service provider, for example, must weigh not only which service offers the best rates, but with the rapidly evolving legal ramifications, which can provide some measure of protection.

In the past, negotiating a service level agreement with a cloud provider wasn’t a big issue, says Thompson. Now, though, with new laws being implemented in various countries, the logistics become more prohibitive, he says. For example, a German customer’s data may not be moved out of the country, so how is that viewed as 

private data, say, via a password reset, 

may prove to be a gateway to identifi ca-
tion. What might not be considered 

considered private in the United States 

might prove to be a gateway to identifi ca-
tion. What might not be considered private in the United States

may prove to be a gateway to identification. What might not be considered private in the United States

can be penetrated. Compounding the 

problem, an “identity ecosystem,” according to

Thompson says. “And, from a digital 

perspective, it is getting murky.

But there is some measure of hope. In his position as chair of the RSA Conference, Thompson is in a position to observe what the hot topics are. And despite the buzzwords of the day being cloud and cyberwarfare, when one digs deep into the agenda, privacy is the big ticket item, he says. Based on the pro-

posed laws for sessions at the annual confer-
ence, both here and in its European edition, he’s seeing issues being raised around transfer of data and the privacy implications.

Controlling the airwaves

And action would be most welcome as enterprise and government operations continue to expand across borders and, as a result, face potential risks from 

foreign intruders more familiar with the lay of the land.

Foreign office threats is sure to be a big topic this coming year, says Rich Baich, a principal analyst in the secu-

rity and privacy practice at Deloitte & Touche LLP. But, while most attention has been focused on privacy laws, what’s been missing, he says, is a comprehensive understanding of telecommunications laws, particularly those affecting telecom infrastructure owned or controlled by a foreign nation-state.

“We understand what the FBI can do,” Baich says, referring to traditional means of surveillance of telecommunication, such as VoIP or cell phone calls. “But do organizations understand who owns the rights to their data when that data is being transmitted in foreign nations?”

The message seems to be: No one should be trusted. The data flowing among corporate headquarters and remote satellite offices, particularly in foreign countries, is subject to a number of variables, namely foreign-controlled network infrastructure. This is different from privacy laws, he says. “Can you trust the phone guy?” he asks.

How can corporations opening an office overseas entrust the buildout of their office to contractors. As an illustra-

tion, he mentions the American embassy built in Moscow in the mid-1980s that had to be redone once it was discovered that the building was infested with bugs of the snooping variety. The threat of unauthorized access by 
criminals is just one of the challenges of a foreign-controlled network infra-

structure. The system is also vulnerable to eavesdropping by foreign intelligence services interested in intercepting corpo-

tate or government proprietary data. It is more than a matter of doing due diligence, Baich says. When leaving your host country, the laws are going to be different. “If you’re an executive, what sort of encryption are you using?” he asks. And when that executive returns, how can it be determined they are not bringing back something unwanted on their laptop?

The risk, Baich says, is that state-spon-

sored entities, perhaps in cahoots with criminal gangs, can use any number of techniques to monitor, intercept, modify or disrupt the communications of any corporation or government agency from any number of points in the network path. Devices can be implanted any-

where, including within the central office of the telco.

As well, intruders can use social engineering to dupe a email recipient into providing a password or another key needed to view corporate assets. Or, the public and private wireless networks can be penetrated. Compounding the 
situation, “lawful” intercept rules are not likely to be consistently applied across nation-state boundaries, Baich says.

The new Cold War

Baich says his job is to let people know they have to think of security differ-

tently as opportunities for attack always rest outside of a traveler’s environment. Supply chain nation has been real for years, since at least World War II, he says. When one goes to a foreign country, they can become a target for corporate espionage. “The Cold War is still on,” Baich says. “It’s just a different domain.”

Any look at the top IT security risks for the coming year should include an examination of why a person is being targeted, and a look at what of value is being sought. Criminals seek to pen-

etrate the network of a mining company, for example, because they want to know where the company next will be drilling, Baich says. Or, an e-commerce provider is hacked, say, to tinker with the code so that a penny can be siphoned from every transaction.

For Titus of Unisys, the question really boils down to who is in charge of security in the United States. Is it Christopher Painter, the U.S. Depart-

ment of State’s first coordinator for cyber issues, appointed in April? Among his duties is to coordinate the department’s global diplomatic engagement on cyber 

issues and serve as a liaison to public and private sector entities. But, Titus asks, when at this point the U.S. govern-

ment has not even settled whether laws governing overseas data transmission are a diplomatic or corporate issue.

But does she see some evolutions in 
governance coming from the White 

House, particularly the U.S. Commerce Department creating an internet ID, a cybersecurity effort that seeks to create an “identity ecosystem,” according to the White House Cybersecurity Coordinator Howard Schmidt. The final plan for the National Strategy for Trusted Identi-
cies in Cyberspace, announced on April 15, provides guidance on establishing secure online credentials to make inter-

net transactions more secure. Computer users would cease using unique pass-

words on each website they visit and instead employ a set of credentials rec-

ognized by multiple sites. However, the secure credential – software on a mobile device, a smartcard or a small token that generates one-time passwords – has yet to be devised.

Despite that, Titus calls for expanding the initiative and bringing in EU col-

leagues to get identity standards moving quicker. Further, while there seems to be some unity and sense to the moment to create an international set of standards for the transfer of data, Thompson points to his.

historical precedents that caused huge legal shifts, such as the failure of Enron, which gave rise to SOX, and rampant identity theft cases in the state of California, which gave rise to the first data breach notification laws in this nation.

“Since 9/11, the world has been called Armaged-
don yet,” says Thompson, “but there have been tremors.” He cites the recent breach of Epalon, an email marketing services firm, where so much data was compro-

ised that the consequences reverberated in the media and, thus, the status quo was shaken. “When will we cross that boundary to get an overarching law to kick in?” he asks. So far, there is no answer.

Global risks

Foreign carrier as the exploit vector

Corporate data center

(domestic)

Foreign carriers

■ Internet route poisoning

■ Wireless penetration

■ Physical access attack

■ Social engineering

■ Introduction of intercept device

Telco central office

Factors:

□ Physical controls of cable plant and central offices

□ Security awareness of workers

□ Security clearance of workers

□ Government collusion

□ Multiple nation-states

□ Overburdened workers

Users (foreign remote)

Baich says. Or, an e-commerce provider is hacked, say, to tinker with the code so that a penny can be siphoned from every transaction.

For Titus of Unisys, the question really boils down to who is in charge of security in the United States. Is it Christopher Painter, the U.S. Depart-

ment of State’s first coordinator for cyber issues, appointed in April? Among his duties is to coordinate the department’s global diplomatic engagement on cyber
F 0 R E N S I C  I N T E L

S


t down with a forensic investigator for an hour and you’re sure to hear some interesting stories. Like the time a digital investigation was initiated after a university student in Western Canada, who was using his school’s internet connection to distribute child pornography, left a thumb drive containing illicit material in a public computer. The perpetrator was, incidentally, nabbed by police after stopping by the school’s IT department asking if anyone had turned in the missing device.

Or, there was the time a forensicator – what digital investigators often call themselves – had to dig into a deceased employee’s computer to determine if anything work related caused the person to take their own life.

The field of computer forensics is still a relatively new discipline, and is constantly evolving. A combination of law and computer science, the field is defined as the practice of gathering and examining data from computer systems, networks and wireless devices in a way that, if necessary, will hold up as evidence in a court, according to the U.S. Computer Emergency Readiness Team (US-CERT), the operational arm of the National Cybersecurity Division at the U.S. Department of Homeland Security. Historically driven by human relations and legal issues, in cases like the examples above, digital investigations are now increasingly being launched following data breaches and suspected computer intrusions, experts say.

The frequency and sophistication of today’s cyberattacks, computer forensics has become an integral aspect of information security incident response plans, especially for those in government and the technology and defense industries.

A new reality

“Digital forensics in IT security is necessary to provide a new component called threat intelligence,” says Rob Lee, faculty lead for digital forensics at the SANS Institute, a leading source for information security training.

Lee, a forensicator for more than 15 years who has worked for the special investigations branch of the U.S. Air Force Office and as a contractor for the National Security Agency and CIA, says digital investigations can provide critical information about the tools, techniques and procedures leveraged by adversaries. Given today’s flourishing threat landscape, where advanced persistent threats (APTs), financially motivated cybercrime and hacktivism are rampant, the necessity of integrating forensics into incident response plans is becoming “a new reality,” he says.

Most organizations have already deployed a host of layered security defenses that are helping to keep intrusions at bay, experts say. Still, recent compromises of government agencies, security firms and international corporations show that no defense is foolproof, and determined adversaries can usually make their way in, says Dave Merkel, CTO of Mandiant, a firm that specializes in cyber incident response and computer forensics.

“Even with a great security staff and a high budget, the likelihood that you can be compromised is high,” says Merkel, who has been a digital investigator for a decade and a half. “Every organization we see can be breached.”

And that’s precisely the reason why many forward-thinking organizations, which are looking for better ways to fight back, have bolstered their forensic capabilities.

Forensic investigations are a central part of the federal cybersecurity strategy, according to an analyst at US-CERT, the agency tasked with responding to and defending against cyberattacks targeted at the executive branch of government. US-CERT currently has seven full-time staffers to analyze federal government hard drives in response to evidence of intrusions, and the team is growing rapidly, having doubled in the past 18 months.

Cybersecurity investigations are a different breed of forensics than traditional human relations and legal cases, experts say. While any digital investigation necessitates forensic best practices, such as maintaining a so-called chain of custody (see sidebar), the goal of a cyber incident response-driven inquiry is not necessarily to catch a criminal and get a successful prosecution, says SANS’ Lee.

The main purpose is, rather, to determine the extent of a compromise and fully eradicate adversaries from all their hiding places within the network. In addition, such investigations are meant to determine how an intruder gained access to enterprise systems, where they went, what they were after and whether any data was taken.

The US-CERT analyst, who asked not to be named, says forensic examinations begin as a reactive information security activity, but often turn into a proactive investment. Within the agency, such examinations often yield information about how a piece of malware operates and how an attack was carried out. This information is fed back to the network analysis team, which can come up with ways to better detect similar threats in the future. This information is also shared, when appropriate, with the public.

Staying ahead of threats

Besides the government, every company within the defense industrial base is currently using forensics to better its security posture, Lee says. Such organizations, along with commercial technology firms, have historically faced some of the most frequent and advanced attacks. They consequently began using forensic threat intelligence to their benefit several years ago.

“The only way to stay ahead of [today’s threats] is to have a team that will help you generate additional threat intelligence,” Lee says. “That’s where digital forensics is becoming extremely useful in commercial and government organizations.”

Many other companies are behind the curve, however, according to a report released in March by McAfee and Science Applications International Corp., a scientific, engineering and technology applications company. The “Underground Economies” report, based on a survey of more than 1,000 senior IT decision-makers, reveals that just a quarter of organizations conduct digital investigations are becoming a key component of incident response plans, especially for the government, reports Angela Moscaritolo.
Many organizations have accepted social networking as part of doing business, but technology and governance can help control it. 

“Digital forensics is necessary to provide threat intelligence…”

— Rob Lee, faculty lead for digital forensics, SANS Institute

Most large and midsize businesses have some incident response capabilities, he adds. Few, though, have experience dealing with aggressive, targeted attackers. If not, the organization may choose to bring in a third-party computer forensic company to aid incident response activities. In such cases, the contracted investigators will likely deploy technologies that increase the ability to observe what’s going on.

Hunting for adversaries

Regardless of whether the company has the capabilities in-house or has contracted a third party, the next step is to go “hunting” for adversaries, Lee says. This involves examining the network for anomalies and using the information gathered to know what to look for.

“We have had situations where the company knows they were dealing with one kind of threat – an APT problem – and we do an investigation and find out that, indeed, they do,” Merkel says. “But, they also have a credit card breach we find by virtue of doing the investigation.”

For this reason, it makes sense to scope out the extent of a compromise before reacting to it, experts say. If just one infected system is cleaned at a time, hackers can react by moving laterally through the network to retain their foothold.

Instead, all infected systems should be taken down simultaneously, at which time the security team can improve its organization’s level of protection by deploying additional network defenses, creating blocks for the offending IP addresses, forcing users to change all their passwords and providing user education.

“It’s a continual process,” Lee says. “It’s like weeding a garden. You never win. You try to get the weeds out before they become an issue.”

ADMISLABLE:

Maintaining the chain

A chain of custody refers to the process for ensuring evidence has not been mishandled or tampered with, and will hold up in a court of law. Most digital investigations do not go to trial, but each one should be treated as if it were, says Joseph Shaw (picture), incident response analyst for a large health insurance company and senior threat investigator for MetNet, a managed security event monitoring and incident response handling firm.

The best way to ensure evidence will hold up in court is to:

Develop an incident response and forensic analysis plan.

Collaborate with a legal team to ensure all steps in the plan are covered.

Ensure staff conducting the investigation are trained and qualified.

Document everything with as much detail as possible, including when and how the evidence was collected and analyzed, who handled it, and how it was stored.

“In my opinion, every organization should have at least one trained individual to handle an incident to the point where they can competently handle evidence without fear of compromising the data,” Shaw says.

— Angela Moscaritolo

Aug. 25: Cloud computing

We look at the various issues that could crop up when using cloud services. With a goal of sussing out the threats and the fixes, this SC Magazine Spotlight edition will explain what organizations can do to remain outside hackers’ crosshairs.

Nov. 17: Social media security

The need to monitor and secure communications via Web 2.0 apps has become imperative to organizations. This Spotlight edition looks at the pros and cons of social media sites and how best to secure corporate assets.

A common pattern

While each digital probe is different, they generally follow a common pattern, according to investigators. For public- and private-sector organizations with advanced capabilities, the investigation is usually prompted after the security team discovers a compromise on some part of the network. At this point, the organization will have some knowledge about the incident, including an idea of where an intruder is on the network and, possibly, an offending IP address.

Through the examination of an infected machine, a forensic team can start to build an intelligence profile of the adversaries. As part of the investigation, malware is often passed to specialists in reverse engineering who can take it apart and determine how it is loaded, where it exists and the mechanism keeping it active. This threat intelligence is then fed back to security operation centers and used to scan for additional compromised machines.

Investigations play out a little differently at less-resourced firms. Often, these victim organizations don’t even know they have been breached and only find out through an external party, such as a technology firm, law enforcement body or government entity, says Mandiant’s Merkel.

A common pattern

Regardless of whether the company has the capabilities in-house or has contracted a third party, the next step is to go “hunting” for adversaries, Lee says. This involves examining the network for anomalies and using the information gathered to know what to look for.

“We have had situations where the company knows they were dealing with one kind of threat – an APT problem – and we do an investigation and find out that, indeed, they do,” Merkel says. “But, they also have a credit card breach we find by virtue of doing the investigation.”

For this reason, it makes sense to scope out the extent of a compromise before reacting to it, experts say. If just one infected system is cleaned at a time, hackers can react by moving laterally through the network to retain their foothold.

Instead, all infected systems should be taken down simultaneously, at which time the security team can improve its organization’s level of protection by deploying additional network defenses, creating blocks for the offending IP addresses, forcing users to change all their passwords and providing user education.

“It’s a continual process,” Lee says. “It’s like weeding a garden. You never win. You try to get the weeds out before they become an issue.”

Launched late last year, our new SC Magazine Spotlight editions were created to focus on one specific, timely issue afflicting the business world.

For editorial opportunities in these special “Spotlight” editions of SC Magazine, contact Editor-in-Chief Illena Armstrong at illena.armstrong@haymarketmedia.com. For sponsorship opportunities, contact Advertising Director David Steifman at david.steifman@haymarketmedia.com.

Coming soon...

SC Magazine, contact Editor-in-Chief Illena Armstrong at illena.armstrong@haymarketmedia.com. For sponsorship opportunities, contact Advertising Director David Steifman at david.steifman@haymarketmedia.com.
Can you be sure the security products you use have a high enough level of independent performance validation?

AVG, Computer Associates, K7 Computing, Kaspersky, McAfee, Prevx and Webroot are taking certification to the next level.

Safeguarding email from “vampires”

I teach a concept I have dubbed “Stephenson’s Theory of Vampires” to explain why otherwise well-secured networks still become infected with malware. In my theory, we understand that, mythologically, we are safe from vampires unless we invite them into our home. If we think of the enterprise as our home, we do all of the computing equivalences of protecting our home from vampires. We hang the garlic (firewalls), sprinkle the holy water (encryption) and hang out our best silver crucifixes (IPS). Then someone clicks on an email attachment or a phishing message and invites the vampire in.

This month, we have a couple of related product groups to add to our VPK (vampire prevention kit). Our first group, email security, allows us to protect the content of our emails, while the second group, email content management, protects us from virtual blood-suckers. These are, really, closely related product groups, and convergence is dictatoring that this probably will be the last year we look at them as separate groups.

That may be a good thing, though, because one really needs both, and this probably will be the last year we look at them as separate groups.

With this month’s crop of solid email tools, one should be able both to secure messages from prying eyes on the internet – where email seems to be about as private as a postcard – and keep those pesky vampires at bay.…two worthy and necessary objectives for any security administrator.

— Peter Stephenson, technology editor

What the stars mean

Outstanding. An “A” on the product’s report card.

Carries out all basic functions very well. A “B” on the product’s report card.

Fails to complete certain basic functions. A “D” on the product’s report card.

Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

How we test and score the products

Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a pre-determined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University.

We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technol-ogy editor.

All reviews are vetted for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.
Email security

Making email encryption transparent at both ends is the way to secure messages. There are two approaches, and Peter Stephenson and the SC Lab team help narrow down the options.

T
his month’s email security group is, arguably, a dying breed. The idea of encrypting email to provide security is, of course, going nowhere... it is a solid concept and is here to stay. However, we see this capability morphing into functionality on more universal email gateways that cover both security and content management. In fact, in some cases, it is moving into a more universal gateway that includes web content management. We think this is, actually, a good idea in today’s internet environment.

Email is a ubiquitous – some might argue the most ubiquitous – internet functionality used by today’s individuals and businesses. Statistically, a huge percentage of network intrusions are the result of malware, and the two primary sources of malware by a very high margin are email and the web. It is difficult to separate the two, such as in phishing and spear-phishing. Managing these two primary sources of trouble makes a lot of sense.

The products that we looked at were focused on encryption. However, it is not difficult to imagine the functionality of these products moving into a more comprehensive appliance.

Functionally, these tools fit into two categories: encryption and certificate authorities. The encryption products have some challenges to overcome and they mostly address the hurdles in similar ways. First, there is the challenge of where to perform the encryption. While transport layer encryption is, arguably, more secure than application layer encryption, it is also more inconvenient to do. Transport layer encryption needs a compatible device at each end to perform encryption and un-encryption. Application layer encryption does not.

At the sending end, application encryption has a lot of possible flexibility due to its nature. For example, policy-based products easily could make determinations about which outgoing emails should and should not be encrypted. They might, for instance, have a policy that says any email containing a Social Security number will encrypt automatically and transparently to the user – to protect the content. Without a policy being invoked, though, the email could go out as clear text. Protect that which needs to be protected and let the rest go. Just don’t make the user think about it.

When the message reaches the recipient there are some choices. One is to embed a link back to the clear text data in the message the recipient receives. He or she then clicks on the link, authenticates, and reads the message as webmail. Another choice is to attach an encrypted file to the message. The recipient clicks on the attachment, authenticates and the message opens. That can be a bit problematic on systems that don’t care much for attachments and routinely strip them off.

Selecting email encryption is really straightforward. First, decide whether application layer encryption is acceptable or if you require transport layer encryption. Next, look at recipient convenience and sender transparency. Products that require too much from users at either end will become support nightmares. Now, decide if your environment can tolerate the attachment approach or if an embedded link is your best bet. Embedded links are the primary approach taken by most organizations today.

There is a potential issue with the embedded link approach, though. Recipients are learning to avoid clicking on things in emails, so be sure that you can brand (customize) the message that comes with the email such that you can reassure the recipient that it is OK to click on the link. Finally, make sure that your own internal users don’t have to pay attention to encryption. Why? They won’t. As the administrator, you need to do it for them. That means that your product needs a good policy engine. Making email encryption transparent at both ends is the way to secure email. If you can do that, you’ll have a solid, safe encryption scheme. And, perhaps most important, meeting regulatory requirements for privacy will get that much easier.

Mike Stephenson contributed to this Group Test.

Specifications for email security tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Comodo Secured Email</th>
<th>Cryptzone Secured eMail</th>
<th>TrustTone Stealth</th>
<th>PGP Universal Gateway from Symantec</th>
<th>Trend Micro Email Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer encryption</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Transport layer encryption</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Supplied as hard-ware appliance</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Supplied as software for installation</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Supplied as a virtual appliance</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Client software required for internal users</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Client software required for external users</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Can be integrated with full email content management product</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Standalone product</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Encryption algorithm(s)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Policy-driven</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

There have been a host of data exposures and breaches in various Canadian provinces over the last year or two. This event will discuss the challenges and solutions involved in protecting some of today’s major attack vectors, and review privacy and data security policies that should be in place to adhere to both existing and perhaps impending regulations.
Comodo Secure Email

**Cryptzone Secured eMail**

- **Vendor**: Comodo Secure Email Solutions
- **Price**: $32 per certificate
- **Contact**: www.comodo.com

The Comodo Secure Email application comes as a free product. However, to use it in a corporate PKI environment, one needs to install commercial certificates, and there is a charge for that. The product operates at two levels: network level and MS Outlook-only. The network level operates at the network layer and applies to all supported email traffic, while the Outlook-only mode operates at the software layer. It is only available in a 32-bit version, while the network-level product also is available in 64 bits.

We tested the Outlook only version, but the main difference between the two is that in the network version one will need to specify an email client(s). The admin may purchase certificates to use as part of the corporate network – Comodo is a CA – or use the free Personal Email Certificate from Comodo for non-commercial applications. Personal certificates were our choice for testing.

When we selected the free personal certificate option, we were directed to fill out a form, which resulted in an email from which we could install the certificate. We also downloaded the application and installed it. The first time we ran the application, we received a cryptic error message and were offered an opportunity to send the message unencrypted. Thus, we expected the message to be signed only. However, the received message was not signed. Further testing showed that if the message was sent in Outlook’s plain-text mode, the product would not work.

Generally, we found the performance to be poor, and the product simply did not live up to its billing. While it is very easy to implement, the impact on the end-user is out of balance with the benefits of encrypting and signing emails.

We found the manual to be missing some critical answers, such as error message meanings and troubleshooting. The website, as well, is heavy on marketing and short on information. At the price, we would find the value to be very good, if not for the performance issues.

**SC MAGAZINE RATING**

<table>
<thead>
<tr>
<th>Category</th>
<th>★★★✩✩</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Features</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Performance</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Documentation</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Support</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Value for money</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★✩✩</td>
</tr>
</tbody>
</table>

**Strengths**
- One of the most popular sources of certificates available.
- **Weaknesses**
  - A difficult product to deploy that needs a stronger level of support and documentation.
- **Verdict**
  - Potentially a very nice product, but we found it fraught with implementation challenges. The Comodo certificates are among the most widely accepted in the industry, however.

The server then deploys the client, and we started that process. In the enterprise, the product uses group policy. Once the client is installed – we simply imported Active Directory users – the recipient receives an email that explains how to use the product. We then sent our first email. The recipient needs to install the client by clicking on a link in the message. There is no cost for this. Once installed, the user can open the received message by clicking on the attachment in the received email. Users create a shared secret between the sender and the recipient, and the process is then automatic from the second email on. Virtually any platform is supported for the reader, including smartphones and tablets.

We found this approach to be slick and easy to deploy. The documentation is prodigious and the website is first-rate. We found support to be a bit pricey for what was offered, however. Ninety days of deployment support is free, but after that support is 22 percent of net license cost. However, that support is only for 8-5 Monday through Friday. For an additional cost, 24/7 support is available. The support package keeps this one from being a superb value for the money.

**SC MAGAZINE RATING**

<table>
<thead>
<tr>
<th>Category</th>
<th>★★★✩✩</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Features</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Performance</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Documentation</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Support</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td>Value for money</td>
<td>★★★✩✩</td>
</tr>
<tr>
<td><strong>OVERALL RATING</strong></td>
<td>★★★✩✩</td>
</tr>
</tbody>
</table>

**Strengths**
- A solid, easy-to-deploy product that really gets the job done.
- **Weaknesses**
  - Given its cost, needs just a bit stronger support offerings.
- **Verdict**
  - A slick, easy-to-deploy and use product that needs a little fine-tuning in its support offerings.

Recommended.

Visit scmagazineus.com/awards to download your entry kit today.
TrustTone Stealth

PGP Universal Gateway Email

Installation begins with the usual network static management, IP configuration. After this, everything is done from the web interface. The administrative console is first-rate in its simplicity and comprehensive choices. One impressive piece of the implementation using the console is a network map showing where addresses need to go, which needs to be configured, and other important aspects, such as domains.

Once the system is deployed and certificates installed, the system can be branded for the organization, and policies can be added. Policies can be very granular, encrypting based on message contents, or the provided policy can be used. Policies can also be based on local regulations. The administrator’s manual is well-built out with many screen shots and diagrams, and support covers everything necessary for deployment and ongoing management at an industry standard rate of 20 percent of the product price after the first year, which is included. At a price of under $2,000 for a 50-user product, the value is excellent.

Trend Micro Email Encryption

Best in the context of a full content management system. Installation on PGP Desktop has several deployment options – from inline to part of a comprehensive content management tool. The encryption algorithm is AES-256, but message encryption is identity-based and Trend Micro proprietary. No certificates are required, and users register with Trend for authentication.

Internal use requires no client-side software. For web delivery, no recipient client is required, but there is an add-in for Outlook. If the recipient’s content filter blocks attachments such as those delivered by the product, Trend can provide characterization that will permit whitelisting. Management is done through a web interface.

---

**SC MAGAZINE RATING**

**Ease of use**

**Features**

**Performance**

**Documentation**

**Support**

**Value for money**

**OVERALL RATING**


gg

Strengths: Excellent performance, easy to use and deploy.

Weaknesses: None that we found.

Verdict: Simple, effective, secure.

This is just what this doctor ordered. We make it our Best Buy.

---

**SC MAGAZINE RATING**

**Ease of use**

**Features**

**Performance**

**Documentation**

**Support**

**Value for money**

**OVERALL RATING**


gg

Strengths: Typical PGP/Symantec reliability and support.

Weaknesses: Could be a bit easier to use and deploy. Can be pricey.

Verdict: A superb product for current PGP users, but absolutely worth looking at for any mid- to large-sized organization.

---

**SC MAGAZINE RATING**

**Ease of use**

**Features**

**Performance**

**Documentation**

**Support**

**Value for money**

**OVERALL RATING**


gg

Strengths: The best implementation we’ve seen in a long while and very strong support.

Weaknesses: As a standalone product, lacks features that we would expect.

Verdict: Clearly, this product is intended to be part of Trend Micro’s larger content-management gateway, and we find that this limits its effectiveness somewhat. If you already are running the larger application, however, this is a very strong offering.

---

DEFEND NETWORKS AND DATA. ADVANCE YOUR CAREER.

Every year, data breaches cost companies millions of dollars. That’s why it pays to know how to manage risks like cyber attacks, accidental damage and more. Get ahead in this fast-growing field with a certificate or master’s degree from University of Maryland University College (UMUC). Our nationally recognized programs can help you turn data loss prevention into career gain.

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and DHS
- Bachelor’s degree recognized as a Professional Science Master’s by the Council of Graduate Schools
- Programs offered entirely online
- Financial aid and an interest-free monthly payment plan available

800-888-UMUC • umuc.edu/data
**Email content management**

Tools to help with email content management are focused almost exclusively on prevention through some form of filtering, says Peter Stephenson.

**PICK OF THE LITTER**

Sophos Virtual Email Appliance is easy to deploy and manage. Policy configuration is guided by wizards for added ease of use. It is easy to deploy and manage. Policy configuration is guided by wizards for added ease of use. It gives built-in compliance and is focused almost exclusively on prevention through some form of filtering, says Peter Stephenson. It is even very large organizations.

**PICK OF THE LITTER**

McAfee Email Protection provides full email content management with built-in compliance and data leakage prevention. It gives solid content management for even very large organizations with high-policy standards. It is recommended.

**GROUP TEST | Email content management**

Specifications for email content management tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Anti-virus</th>
<th>Anti-spam</th>
<th>Anti-spyware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Astaro Security Gateway v8.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Axway MailGate v3.8.1</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Barracuda Networks Spam &amp; Virus Firewall 600</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>eSert ThreatWall 250</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Fortinet FortiMail v4.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>M86 MailMarshal Email Content Manager v7</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>McAfee Email Protection</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Proofpoint Enterprise Privacy and Enterprise Protection Suites v6.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SECNAP Rule18</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SonicWall Email Security Appliance 4300 v7.3</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Sophos Virtual Email Appliance v3.4.0.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Trend Micro InterScan Messaging Security v8</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>WatchGuard Technologies XCS 770R v9.2</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

**GROUP TEST | Email content management**

**How to buy**

Start with the form factor that fits your enterprise best. We saw a combination of software products (those that install on a server platform, such as MS Server 2008), virtual appliances (those that install from scratch either on hardware or on a virtual system), and hardware appliances. Your next step is to look at what similar functionality already exists in your enterprise. Do you need both content management and email security or can you separate the two?

Once you have laid the groundwork, consider what functionality you will need — i.e., are you already using an anti-spam gateway or service? As always, understand your environment, your requirements and the unmanaged threats against your enterprise, and then browse through this month’s offerings.

Mike Stephenson contributed to this Group Test.
Astaro Security Gateway

The Astaro Security Gateway appliance (mail applications only) comes to us again, this time highlighting some of its email content functionality. With this gateway, administrators can set policy to manage spam, encrypt messages and scan email for viruses. Furthermore, this tool allows users to access a web-based portal to manage their own spam quarantines, which can cut down the need for support intervention.

Getting this appliance up and running is a quick process. When it is connected to the network and the web GUI is accessed for the first time, the administrator is prompted to go through a configuration wizard. This wizard helps not only set up basic system settings, but also initial policy. The only problem we ran into was changing the default IP address. Only after the configuration is complete can a secondary address be created.

At the completion of the wizard, the administrator can now log in to the web GUI for fine-tuning and advanced configuration. We found this GUI to be nicely organized with a fairly intuitive layout. This offering provides a nice amount of configuration flexibility, as well as policy granularity.

Documentation included a quick-start guide, as well as a full administration manual. The quick-start guide outlines clear steps to getting the appliance connected to the network, while the manual covers everything else—from initial configuration to managing advanced functionality. We found both guides to be well organized with clear and easy-to-follow instructions.

Astaro offers free, web-based technical support via a knowledge base and online user forum. Customers also can purchase phone- and email-based assistance as part of a plan.

At a price just over $2,400 for the email protection piece of the appliance, we find this product to be a good value for the money. The Astaro Security Gateway offers a multitude of functionality and policy control at a reasonable price.

Axway MailGate

The MailGate from Axway provides full email content management functionality, as well as digital rights management and a little bit of policy compliance, all wrapped up into one appliance. One of the major policy settings deployed, administrators can create policy to protect against virus-infected emails and spam, meet compliance, including HIPPA and GLBA, and control documents through password-protected PDFs.

Installation and deployment of this solution is easy and straightforward. The initial configuration can be done by attaching a keyboard and monitor to the appliance and going through some quick steps to configure network and IP settings. Once the network settings are complete, all further configuration is done through the web GUI, which includes an initial deployment wizard. At the completion of the wizard, the appliance now has all network and license information and is ready for advanced configuration.

All management is also done through the web GUI, which is well organized with a clean layout. The main dashboard offers an overview of statistics and other useful system information. Policy is easy to configure with some default policies already in place, including around compliance.

These can be customized, or new policies can be created for more granular control.

Documentation included a quick-start card, setup guide and full administrator guide. The quick start card and setup guide work together to illustrate initial setup and configuration, while the administrator guide offers in-depth advanced configuration steps and other instructions. Both guides include clear, step-by-step instructions, examples and screen shots.

Axway offers two plans as part of an annual maintenance agreement. Customers can purchase either eight-hours-a-day/five-days-a-week or 24/7 plans.

At a price of $8,000, this product is a good value for the money. The Axway MailGate offers some basic functionality to protect the enterprise from email threats, as well as added functionality to manage data leakage.

SC MAGAZINE RATING
Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★
Strengths Solid functionality with easy-to-manage policy controls.
Weaknesses We would like to see more ways to change the default IP address.
Verdict Deployment can be a bit challenging, but aside from that, a first-rate product.

Barracuda Networks Spam & Virus Firewall

The Spam and Virus Firewall from Barracuda Networks provides a range of email content management functionality. With this product, email can be scanned for viruses and spam content, as well as possible phishing and spyware. Granular policies can be set up for both inbound and outbound mail, including preventing possible data leakage. Barracuda also provides cloud-based spam protection to prevent a large amount of unsolicited mail from even coming through to the enterprise.

We had this product up and running within a few minutes. The initial configuration is done by connecting a keyboard and mouse to the appliance and setting all network and IP information, and after that is complete, all further configuration and management is done through the appliance’s web GUI. We found this GUI to be a little overwhelming at first. There are many tabs and configuration menus to sift through, but after a few minutes of getting acquainted with the layout, we had no trouble at all getting around the console.

The one major issue about configuring this device is that pretty much everything is done manually without the help of wizards. With that said, this appliance has some very powerful controls and policy settings. Documentation included a short quick-start guide, as well as a full administrator manual. The quick start-guide does an excellent job of detailing the initial configuration process, while the administrator guide provides a great amount of detail on how to configure and use product features, thanks to many diagrams and a few screen shots included. We found all documentation to be well-organized and easy to follow.

Barracuda Networks offers basic, premium and enhanced support. Basic provides no-cost access to eight-hours-a-day/five-days-a-week phone and email technical support, as well as an online knowledge base and resource area. At a price just shy of $9,000, we find this product to be a good value for the money. This appliance can provide some excellent functionality once it is set up, configured and finetuned.

SC MAGAZINE RATING
Features ★★★★★
Ease of use ★★★★★
Performance ★★★★★
Documentation ★★★★★
Support ★★★★★
Value for money ★★★★★
OVERALL RATING ★★★★★
Strengths Solid features with many capabilities and controls. We had this product up and running within a few minutes. We found this GUI to be a little overwhelming at first. There are many tabs and configuration menus to sift through, but after a few minutes of getting acquainted with the layout, we had no trouble at all getting around the console.

Vender Barracuda Networks
Price $8,999
Contact www.barracudanetworks.com
eSoft ThreatWall 250

The eSoft ThreatWall 250 is a powerhouse in a little box. This product packs features, such as spam filtering, anti-virus policy compliance and gateway access control prevention; all by way of its Email ThreatPak. The appliance can be deployed transparently either at the gateway or between the mail server and the rest of the network, depending on the needs of the environment. It is also driven by the Distributed Intelligence Architecture from eSoft to quickly assess WPAM (World Post Access Model). It also examines viruses and other threats in both inbound and outbound email.

Deployment of this product is almost plug and play. When the appliance is initially connected to the network, it can grab a DHCP address from which the web GUI can be accessed. At the first run of the GUI, the initial configuration appears and, after a few quick steps, the appliance is up and running with a base configuration, as well as all its latest updates.

After all configuration and updates are complete, any additional management and configuration is done from the web GUI as well. We found the interface to be quite easy to navigate due to an intuitive and comfortable layout. Policy can be created with just a few clicks of the mouse.

Documentation included a short, quick-start guide, which outlined the initial setup procedure, and a user guide, which explained how to configure some of the product features. However, we found the user guide to lack in-depth detail on configuring and managing the appliance.

Customers receive 90 days of no-cost, phone-based technical support, along with ongoing access to online resources, such as a knowledge base and documentation.

At a price just under $2,000, plus $1,000 per year for the ThreatPak, we found this solution to be an excellent value for the money. The eSoft ThreatWall 250 offers easy controls with an excellent feature set at an affordable cost.

Fortinet FortiMail-100C

T he FortiMail-100C appliance from Fortinet allows for deployment in transparent or gateway mode, or as a functioning email server all on its own. It can scan both incoming and/or outbound email for viruses and other malware, as well as monitoring for spam and keeping message problems from coming into the enterprise.

This appliance can be set up and configured in just a few minutes. The initial setup is guided by a wizard at the first login to the web GUI. This wizard helps select the IP and network information and, after completion, all further configuration is done via the web interface as well.

We found the web interface to be simple to navigate with an organized layout. However, it takes a few minutes of using the appliance to get comfortable with how policy and settings are configured.

The flexibility of this tool lies in its many deployment methods.

It can be implemented in three different ways. The first is a full transparent deployment, which puts the unit inline between the mail server and the rest of the network. The second is gateway or proxy mode, which allows for the appliance to scan mail and then pass good mail on to the existing mail servers. Finally, a full deployment allows the appliance to be both a scanner and mail server for smaller environments.

Documentation included a quick-start guide, as well as a full administrator guide and other supplemental manuals. The quick-start guide does a good job of outlining the initial installation of the product in the network and how to access the configuration wizard. We found all documentation to be well organized and easy to follow.

Fortinet provides 90 days of eight-hours-a-day/five-days-a-week phone- and email-based technical support with purchase. After the 90 days, customers can purchase additional support.

At a price just under $1,800 per year for all the services, this product can be installed directly on the Microsoft Exchange email server and act as a hub transport service. This method of deployment allows for direct integration with Exchange and the existing environment, and provides full visibility in scanning email for viruses and other threats, as well as maintaining compliance with email policy.

We found installation all the way through to the appliance to scan mail and keep data leakage prevention software up to date, with many easy-to-follow configuration options. There is also a web-based configuration console that can be accessed from any machine on the network.

Documentation included a full PDF administrator guide. This covers the product from installation all the way through advanced configuration. We found it to be well-organized with easy-to-follow instructions and many screen shots and examples.

McAfee Security Email Protection

M cAfee Security Email Protection incorporates email content management with data leakage prevention and compliance standards. This product can be deployed along with the option of using the McAfee cloud-based service for added scanning capabilities to stop spam and other email problem before it even reaches the enterprise. This tool gives solid content management for even very large organizations, with high policy standards.

Deployment is done by installing the virtual appliance in a VMware ESX environment. Once the server is deployed, all management is done through the appliance’s web-based interface. This interface is quite extensive, but very easy to navigate due to its organized layout. Furthermore, the GUI incorporates a full dashboard, which allows for quick and easy viewing of email statistics and other useful system information.

This solution provides solid email content and policy management. It allows for use of compliance templates and built-in data leakage prevention through dictionaries and document fingerprinting techniques. Custom policy is also easy to configure, and the appliance offers flexible policy options that can be quite granular in nature.

Documentation included installation and administrator guides. The installation guide provided the steps necessary to install the virtual appliance and get it up and running in the VMware infrastructure. All documentation was well-organized with many screen shots, diagrams and configuration examples.

Customers already subscribed to McAfee protection services receive McAfee Global Protection support at no extra cost. This includes access to the McAfee email technical assistance.

With prices ranging from $25 per user per year all the way down to just under $5 per user per year for larger environments, this offering gives us an excellent value for the money. The McAfee Email Protection virtual appliance offers a solid amount of flexibility and functionality at a great price.
The deployment of this appliance works in conjunction with a cloud-based service. The tool becomes an email content management and data leakage prevention system on the distant end with the enterprise. This appliance provides solid features and functionality to manage email-based threats coming in and going out of the enterprise. This appliance can filter for spam, viruses and phishing emails – all while providing outbound content filtering – keeping the enterprise safe from possible data leakage and maintaining regulatory compliance.

The quick-start guide provided by the appliance is straightforward and took us only a few minutes to get up and running. We rebooted the device and manually configured the email content management function. The policy for data leakage prevention and regulatory compliance is easy to manage through the appliance. This appliance provides supported through an annual maintenance agreement with cost based on the number of users in the environment and options chosen. At a price just under $7,000 before support and maintenance subscriptions, we find this tool to be a good value for the money. The SonicWALL Email Security Appliance 4300 incorporates a multitude of functionality in an easy-to-manage platform.

Strengths
- Comprehensive feature set with a list of compliance and security features.
- Supportable security vulnerabilities with a minimal impact on performance.
- Simple configuration: users can use a wizard to simplify the process.
- Sophos provides 12/5 phone and email technical support.

Weaknesses
- The price is relatively high compared to other similar products.
- The interface can be overwhelming for users new to email security appliances.

Verdict
- Overall, Sophos Virtual Email Appliance is a good option for enterprises looking for comprehensive email security solutions.
Trend Micro InterScan Messaging Security

WatchGuard XCS 770R

already included with the appliance, or configured from the ground up depending on the needs of the environment. We found policies were simple to configure.

Documentation included installation and full administrator guides. The installation guide provided a good amount of configuration information on getting the virtual appliance deployed with an initial configuration.

Trend Micro offers a multitude of no-cost and fee-based support options. Customers with valid licenses get access to no-cost phone and email technical assistance, as well as access to product updates and upgrades and a vast online help area on the website. At a price of about $15 per user for an environment of 5,000 users, this product is not low cost by any means, but it does provide a solid set of features, high policy flexibility and a full hybrid appliance/cloud-based deployment. We find this product to be a good value for the money.

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

Strengths
Extensive policy flexibility for email content management.
Hybrid deployment.

Weaknesses
No dashboard.

Verdict
Excellent features and usability, if just a bit pricey.

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

Strengths
Highly configurable with easy-to-use controls.
Weaknesses
No dashboard.

Verdict
A solid product well worth your consideration.

AUGUST

» SANS Network Security 2011
Sept. 17-26
This event brings together network security training, certification and the latest research on important topics in the industry today. Choose from a lineup of more than 40 hands-on courses with in-depth training in security, forensics, management, or coding and development.
Venue: Las Vegas
Contact: www.sans.org/info/7673

» New England Information Security Forum Sept. 20-21
The Institute for Applied Network Security (ANS) assists execs and senior-level IT security risk pros in making better managerial and technical decisions. Speakers at this 12th edition include Marcus Ranum, Tenable Network Security; and Joel Scambray, Ciscorise.
Venue: Boston
Contact: www.miti.com

» SANS Ottawa 2011
Aug. 28-Sept. 2
SANS is bringing live security training courses in the fields of development, audit and forensics, taught by some of its instructors, as well as a number of Canadian speakers.
Venue: Ottawa, Canada
Contact: www.sans.org/info/76748

SEPTEMBER

» SecureWorld Expo Sept. 13-14
This two-day gathering is at the intersection of information security, physical security, compliance, IT audit, computer forensics, enterprise risk management, business continuity and security management.
Venue: St. Louis
Contact: secureworldexpo.com

» SANS Network Security 2011
Oct. 4-5
As mobile adoption spreads, controlling its risks becomes increasingly important. This conference will showcase companies that have adopted innovative security technologies and programs while still leveraging the power of smart and mobile devices. Attendees will learn best practices and hear the latest research on solutions to help plan and implement effective risk management in a mobile world.
Venue: Atlanta
Contact: www.miti.com

FEBRUARY 2012

» RSA Conference 2012 Feb. 27-March 2
The annual conference offers enterprise and technical professionals one-stop learning. Learn about the latest trends, get access to new best practices and gain insight into the practical and pragmatic perspectives on the most critical technical and business issues. As well, discover and evaluate products and services offered by the event’s sponsors and exhibitors.
Venue: San Francisco
Contact: rsaconference.org
It’s time to tell clients the truth

We need to start telling the hard truth. Otherwise the industry will continue to fail, says Errata Security’s David Maynor.

The hackers-turned-activists known as LulzSec have impacted security – whether for good or bad is still to be seen. One of these impacts is proof that the security industry as a whole has failed. LulzSec’s victims were companies that did everything right, with firewalls, anti-virus, and did everything right, with firewalls and web app scanners deployed to protect themselves against SQL injection. We then have long meetings and discussions about how I could find vulnerabilities the scanners couldn’t and how I could have bypassed the firewalls. The customer thought they had the problem solved – people’s careers were made on solving the problem – and I am powerless to convince them that the problem actually isn’t solved. Actually having broken in, just like a hacker would have, is not enough to convince them.

This need to satisfy customers shields them against the threats of the real world, like LulzSec. Vendors and customers are responsible. Until we as an industry start telling clients the hard truth, the industry will continue to fail. Until the clients of the security industry start realizing there is no easy answer, the industry will continue to fail.

My name is David Maynor. I’m a member of the cybersecurity industry. I don’t know how to fix this, but I apologize for my contribution to this failure.

David Maynor is co-founder and CTO of Atlanta-based Errata Security. Rob Graham, the company’s co-founder and CEO, contributed to this piece.
Our business is to protect your business

With industry-leading proactive malware detection, ESET antivirus solutions intercept and eliminate cyber threats before they can infect your business network.

Our award-winning heuristics technology offers aggressive server-to-endpoints malware defense for multiple platforms and virtual environments. All managed from a single console.


To download your free trial, go to www.eset.com/business_trial

**Limited time offer: 6 months FREE**

*With new 2-year license

7/1 - 9/30/2011

For terms, visit www.eset.com/q3promo

ESET NOD32 Antivirus 4
Business Edition

ESET Smart Security 4
Business Edition

ESET Mobile Security
Business Edition

ESET Gateway Security

ESET Mail Security

ESET File Security

© 2013 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.