Features:

The New Wave

Hands-on initiatives designed to hook students on security are gaining steam, says software engineer Alex Levinson  P18

Canada’s thorny hosting problem
The nation’s approach to human rights in cyber space is lacking  PC1

Guarding against a data breach
Our fifth annual survey asks security pros which threats they face and how they remediate them  P27

Bumper crop
A slew of new bills affecting cyber security policies are making their way through Congress  P34
Key Performance Indicator.
Ascending the ladder, rung by rung

The budgeting process is a timeworn battleground. It’s a routine that is especially gratifying for information security pros since they often find themselves joining a skirmish in which business divisions that generate revenue get the preferential treatment.

If you were a gambler, you’d definitely place your money on the other guy (whatever his department might be) to win the money fight because, well, he usually does. And the outlook looks to be similar in 2012.

According to SC Magazine’s fifth annual “Guarding Against a Data Breach” survey, 61 percent of the 488 respondents say their budgets related to IT security and data protection will remain the same this year. Another 34 percent expect an increase, which is down from last year’s 36 percent, and six percent are looking at a decrease in funding.

Experts say, though, there are some breaks in the gloominess. For one, there are quite a few companies hiring – mostly for the technology-specific roles that can support overarching security initiatives. For another, several activities are converging that are making security projects priorities for executive leaders.

Add to the mix an expected increase in examples of regulators actually enforcing compliance mandates this year, and executives are concerned. They want to ensure the right processes and technologies are in place to keep them out of these watchdogs’ crosshairs. After all, harsh fines or worse will do little for profitability.

As well, the legion of attacks we saw last year (yeah, you read right… I did write ‘legion’), has got some corporate heads running scared. They don’t want to be tomorrow’s next headline – which ultimately could equate to the loss of revenue, customers and investors.

And, it seems, leaders of private entities aren’t the only ones taking IT security more seriously. Just last month, the White House released the Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, which has been years in the making and involved input from both public and private sectors.

For some experts, its goals to build a more resilient cyberspace, better attack prevention efforts, establish new defenses and improve software development to create more resistant solutions are promising, if not a wee lofty. But, it’s yet another occurrence that helps set the stage for IT security to take its rightful place among business and government priorities near the top of the food chain.

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

“[Executives] want to ensure the right [security] processes and technology are in place.”
The rate at which attackers of all types have breached corporate and government secrets, the threat from insiders continues to escalate. However, there are solid defenses and strategies to combat this persistent threat. We take a look at the best ways to deal with these.

ON DEMAND
eSymposium: Fending off attacks from all sides
The rate at which attackers of all types breach corporate and government systems has risen rapidly. Whether spearheaded by organized cybercriminals, hacktivists, state-sponsored offenders or spearheaded by organized cybercriminals, the threat from insiders.

WHAT IS SCWC 24/7?
Insiders with access
With the economy continuing to lag, ethical boundaries become less of a guiding light. Employees with privileged access, believing their actions on the enterprise network are undetectable, are more and more tempted by easy gain. Whether transferring customer credit card data to gray market operators, or in cahoots with nation-states to sell government or military secrets, the threat from insiders continues to escalate. However, there are solid defenses and strategies to combat this persistent threat. We take a look at the best ways to deal with these.

ON DEMAND
eSymposium: Fending off attacks from all sides
The rate at which attackers of all types breach corporate and government systems has risen rapidly. Whether spearheaded by organized cybercriminals, hacktivists, state-sponsored offenders or insiders, these assaults highlight the need to be much more proactive and adaptive. In short, such programs must leverage people, processes and technologies to enable systems to be resilient. We learn from experts just what planning entails.

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

FOR SPONSORSHIP OPPORTUNITIES, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazine.com/scwc247.
India was top producer of zombie IP addresses
For October, the Asia-Pacific (APJ) region was the
leading source of all zombie IP addresses. Of the
countries making up the APJ, India was the top
producing country. For the other regions, the top
producers were Brazil in South America, the United
States in North America and the Netherlands in the
EMEA (Europe, the Middle East and Africa) region.

Source: Symantec
DataBank

ThreatStats

A breach of Sutter Health exposed 4.2 million identities

Spam
The world’s worst spam-support ISPs

<table>
<thead>
<tr>
<th>Position</th>
<th>ISP</th>
<th>Number of current known spam issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>telefonica.com.ar</td>
<td>59</td>
</tr>
<tr>
<td>2</td>
<td>unicom-cn</td>
<td>55</td>
</tr>
<tr>
<td>3</td>
<td>chinanet-zj</td>
<td>53</td>
</tr>
<tr>
<td>4</td>
<td>ovh.net</td>
<td>49</td>
</tr>
<tr>
<td>5</td>
<td>hinet.net</td>
<td>46</td>
</tr>
<tr>
<td>6</td>
<td>unicom-hl</td>
<td>44</td>
</tr>
<tr>
<td>7</td>
<td>ilad.fr</td>
<td>42</td>
</tr>
<tr>
<td>8</td>
<td>shawcable.net</td>
<td>40</td>
</tr>
<tr>
<td>9</td>
<td>chinanet-fj</td>
<td>40</td>
</tr>
<tr>
<td>10</td>
<td>telefonica.com.br</td>
<td>40</td>
</tr>
</tbody>
</table>

The networks listed knowingly provide service to spam gangs and ignore reports from anti-spam systems and internet users.

Source: www.spamhaus.org

Malware
Vertical encounter rate

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>157%</td>
</tr>
<tr>
<td>Retail &amp; wholesale</td>
<td>150%</td>
</tr>
<tr>
<td>Food &amp; beverage</td>
<td>140%</td>
</tr>
<tr>
<td>Health care</td>
<td>100%</td>
</tr>
<tr>
<td>Government</td>
<td>73%</td>
</tr>
<tr>
<td>IT &amp; telecom</td>
<td>70%</td>
</tr>
</tbody>
</table>

Phishing
Brands attacked remained identical

Spam rate Compared to global email

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.

Source: Cisco ScanSafe

Top breaches of the month

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sutter Health (Sacramento, Calif.)</td>
<td>A company-issued password-protected unencrypted desktop computer was stolen from its administrative offices.</td>
<td>4.2 million</td>
</tr>
<tr>
<td>UCLA Health System (Los Angeles)</td>
<td>A home theft resulted in the loss of an external computer hard drive.</td>
<td>16,288</td>
</tr>
<tr>
<td>The College of New Jersey (Ewing, N.J.)</td>
<td>A college network had a vulnerability that allowed applicants to see the personal information of other students.</td>
<td>12,815</td>
</tr>
</tbody>
</table>

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

542,649,127

Source: RSA Anti-Fraud Command Center

Top 5 attacks used by U.S. hackers

1. Downloader trojan
2. Zeus trojan
3. ZeroAccess trojan
4. TDSS Downloader trojan
5. Sinowal trojan

Top 5 attacks used by foreign hackers

1. Downloader trojan
2. Zeus trojan
3. ZeroAccess trojan
4. Sinowal trojan
5. Web-based exploit kits

There were 1,608,271 attacks in the U.S. last month, originating from Los Angeles; New York; Atlanta; and Cambridge, Mass.

Source: Dell SecureWorks

Spam rate indicates the accumulated emails tagged as unsolicited.

Received spam Top five regions

Source: Fortinet Threatscape Report

Top 10 threats

1. Salty.AT
2. CeeInject.CI
3. Carberp.C
4. Anomaly
5. CeeInject.CK
6. Fakerean
7. Cybot.G
8. Zbot
9. DynameRidtc
10. Winwebsec

Source: Kindsight

Internet dangers

Zombie IPs Global distribution

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

Source: Commtouch Software Online Labs

Top 5 attacks used by U.S. hackers

1. Downloader trojan
2. Zeus trojan
3. ZeroAccess trojan
4. TDSS Downloader trojan
5. Sinowal trojan

Top 5 attacks used by foreign hackers

1. Downloader trojan
2. Zeus trojan
3. ZeroAccess trojan
4. Sinowal trojan
5. Web-based exploit kits

There were 1,608,271 attacks in the U.S. last month, originating from Los Angeles; New York; Atlanta; and Cambridge, Mass.

Source: Dell SecureWorks

Spam rate indicates the accumulated emails tagged as unsolicited.

Received spam Top five regions

Source: Fortinet Threatscape Report

Top 10 threats

1. Salty.AT
2. CeeInject.CI
3. Carberp.C
4. Anomaly
5. CeeInject.CK
6. Fakerean
7. Cybot.G
8. Zbot
9. DynameRidtc
10. Winwebsec

Source: Kindsight
Canadian lawyers may have opened a legal can of worms by requesting the release of censored photographs. Paul Champ and Amir Attaran requested the release of redacted photographs taken of Taliban insurgents by the Department of Defence. The department’s refusal could open the door for legal challenges over the treatment of foreign detainees.

Two Ottawa lawyers had requested the release of photographs of Taliban detainees to find copyright infringers, similar to those used by content activist researchers. The file-sharing sites, according to officials, used anyone to reprogram ware updates, meaning anyone can reprogram the devices with malicious firmware.

Canadian government officials have been downloading copyright-protected items using file-sharing sites to infringe on copyright, while lawmakers would spend any amount of money necessary to avoid the Canadian privacy law.

Canadian lawyers may have opened a legal can of worms by requesting the release of censored photographs. Paul Champ and Amir Attaran requested the release of redacted photographs taken of Taliban insurgents by the Department of Defence. The department’s refusal could open the door for legal challenges over the treatment of foreign detainees.

Two Ottawa lawyers had requested the release of photographs of Taliban detainees to find copyright infringers, similar to those used by content activist researchers. The file-sharing sites, according to officials, used anyone to reprogram ware updates, meaning anyone can reprogram the devices with malicious firmware.

Canadian government officials have been downloading copyright-protected items using file-sharing sites to infringe on copyright, while lawmakers would spend any amount of money necessary to avoid the Canadian privacy law.

Canadian lawyers may have opened a legal can of worms by requesting the release of censored photographs. Paul Champ and Amir Attaran requested the release of redacted photographs taken of Taliban insurgents by the Department of Defence. The department’s refusal could open the door for legal challenges over the treatment of foreign detainees.

Two Ottawa lawyers had requested the release of photographs of Taliban detainees to find copyright infringers, similar to those used by content activist researchers. The file-sharing sites, according to officials, used anyone to reprogram ware updates, meaning anyone can reprogram the devices with malicious firmware.

Canadian government officials have been downloading copyright-protected items using file-sharing sites to infringe on copyright, while lawmakers would spend any amount of money necessary to avoid the Canadian privacy law.
A “critical” turning point

Recent string of alarming incidents highlights glaring shortcomings in the security of the nation’s critical infrastructure. Increasingly, the industrial control systems used to operate such facilities as water and electric plants are being connected to the internet, says Phyllis Schnect, vice president and CTO of global public sector for McAfee. While bringing these systems online allows for operational efficiencies, such as remote monitoring, it also introduces significant vulnerabilities into systems never designed to sustain such risks.

Experts for years have warned that critical infrastructure is vulnerable, but the threat became more than just conjecture when an FBI official, speaking at a conference in London in November, admitted that SCADA systems in three U.S. cities were compromised. “This will happen again and again,” Schnect said. Too, a recent anomalous incident at a facility in Illinois also put into question the accuracy and timeliness of threat information disseminated by the Department of Homeland Security (DHS), said Joe Weiss, managing partner of SCADA security firm Applied Control Solutions. He criticized the DHS, US CERT and WaterISAC (Information Sharing and Analysis Center), for failing to disclose the incident as a possible cyber attack to those in the sector. “All the DHS has said is that there is no evidence that a hack occurred, but there’s also no evidence that a hack didn’t occur,” Weiss said. Investigators wouldn’t be able to rule out a cyber attack because forensic and logging capabilities are not present for critical infrastructure control systems like they are in the IT world, he added.

Despite the issues, shortfalls can be overcome, Schnect said. The manufacturers of control system components are starting to implement more safeguards and are creating products that are less susceptible to attacks. As parts need replacing, plants now have the opportunity to use safer products. Critical infrastructure companies should bolster security investments and conduct risk assessments before bringing control systems online, she said.

But, getting buy-in for security will remain a challenge, she predicted. “The pessimistic side of me frowns when I realize that it takes something bad to happen to build security into systems,” she said. “It’s difficult to convince the people who hold the financial strings that this is an issue.”

— Angela Moscaritolo

160k Approximate number of public drinking water utilities in the United States

Source: DHS

JOBS MARKET
Me and my job

Kevin Sanchez-Cherry, Office of the Chief Information Officer, U.S. Department of Education

How do you describe your job to average people?

I tell people I develop policies, guidance and procedures to protect Department of Education systems and information.

Why did you get into IT security?

It was a combination of my dad working for IBM as a programmer, my interest in computers, and having worked in physical security. So IT security was the way. I was fortunate to be in the right place at the right time to be promoted from a lead computer operator to information security administrator.

What was one of your biggest challenges?

Ensuring the regular end-user community, and even power users, are not only being provided the training and awareness they need to do their jobs, but to help them understand that security is here to help them get their job done. When people understand security helps them, it will be easier to implement.

What keeps you up at night?

Planning and thinking about what I need to do to stay ahead of the bad guys and the malicious insiders. After reading about all the security breaches that have been occurring over the past few years, it makes one wonder if we are fighting a losing battle. Fortunately, with training for users and a continuous monitoring program in place to maintain vigilance, there is more that can be done. We haven’t lost the battle, yet.

Of what are you most proud?

The policies and guidance I have developed will help maintain a high security posture, and secure education data.

For what would you use a magic IT security wand?

I would use it to increase the IT security training budget and staff so that we can continue to get the word out about the benefits of security and the need for everyone to play their part in keeping education systems, networks and information protected.

2 MINUTES ON...

Michael Evans, VP of marketing, Mandiant

With senior leaders on customer requirements, knowledge sharing, strategy development, research and patents, McClure previously was senior VP and general manager of McAfee’s risk and compliance business unit. He replaces George Kurtz, who left to form his own company. www.mcafee.com

Rick Simmons, VP of North American sales, Solaris Networks

Monitor switching technology. Its solutions allow organizations to manage network traffic for data, voice, video monitoring and security. The deal lets NetScout advance its visibility capabilities. www.netscout.com

Rick Simmons as VP of North American sales. He will run the sales team and address customer and growth demands. Most recently, Simmons led area sales at whitelisting company Bit9. www.solarisnetworks.com

George Kurtz was senior VP and general manager of McAfee’s risk and compliance business unit. He replaces George Kurtz, who left to form his own company. www.mcafee.com

Kevin Sanchez-Cherry, Office of the Chief Information Officer, U.S. Department of Education

Joseph Weiss, managing partner of SCADA security firm Applied Control Solutions. He criticized the DHS, US CERT and WaterISAC (Information Sharing and Analysis Center), for failing to disclose the incident as a possible cyber attack to those in the sector. “All the DHS has said is that there is no evidence that a hack occurred, but there’s also no evidence that a hack didn’t occur,” Weiss said. Investigators wouldn’t be able to rule out a cyber attack because forensic and logging capabilities are not present for critical infrastructure control systems like they are in the IT world, he added.

Despite the issues, shortfalls can be overcome, Schnect said. The manufacturers of control system components are starting to implement more safeguards and are creating products that are less susceptible to attacks. As parts need replacing, plants now have the opportunity to use safer products. Critical infrastructure companies should bolster security investments and conduct risk assessments before bringing control systems online, she said.

But, getting buy-in for security will remain a challenge, she predicted. “The pessimistic side of me frowns when I realize that it takes something bad to happen to build security into systems,” she said. “It’s difficult to convince the people who hold the financial strings that this is an issue.”

— Angela Moscaritolo

160k Approximate number of public drinking water utilities in the United States

Source: DHS

JOBS MARKET
Me and my job

Kevin Sanchez-Cherry, Office of the Chief Information Officer, U.S. Department of Education

How do you describe your job to average people?

I tell people I develop policies, guidance and procedures to protect Department of Education systems and information.

Why did you get into IT security?

It was a combination of my dad working for IBM as a programmer, my interest in computers, and having worked in physical security. So IT security was the way. I was fortunate to be in the right place at the right time to be promoted from a lead computer operator to information security administrator.

What was one of your biggest challenges?

Ensuring the regular end-user community, and even power users, are not only being provided the training and awareness they need to do their jobs, but to help them understand that security is here to help them get their job done. When people understand security helps them, it will be easier to implement.

What keeps you up at night?

Planning and thinking about what I need to do to stay ahead of the bad guys and the malicious insiders. After reading about all the security breaches that have been occurring over the past few years, it makes one wonder if we are fighting a losing battle. Fortunately, with training for users and a continuous monitoring program in place to maintain vigilance, there is more that can be done. We haven’t lost the battle, yet.

Of what are you most proud?

The policies and guidance I have developed will help maintain a high security posture, and secure education data.

For what would you use a magic IT security wand?

I would use it to increase the IT security training budget and staff so that we can continue to get the word out about the benefits of security and the need for everyone to play their part in keeping education systems, networks and information protected.
A resolution to measure more

Dan Srebnick,
CISO, city of New York

We made it through the year-end festivities and are back at our desks, ready to tackle what is ahead during the new year, a time of reflection and resolution for many. For the CSO/CISO, it most certainly should be. It is a good time to resolve to improve on what we’ve done, but we must first be able to evaluate how we’ve done. Businesses, especially successful businesses, are driven by metrics. Metrics are equally important in public administration, where scarce resources amplify the need to manage efficiently and to make fact-based decisions.

Metrics that measure are good. Metrics that measure the right things are better. What are the right things to measure? Metrics must explain a security risk or challenge in a way that your organization’s management team can readily understand. These metrics must be actionable, meaning that they should show where you are today and where you need to be tomorrow to obtain or maintain the level of security or risk prevention that is right for your enterprise.

The CSO may want to implement a data security gateway strategy and plan to ask for funding, lest some important data gets misappropriated or misplaced on your watch. How many records containing private data are there in your data center? What would be the organizational cost if that database was breached?

The CSO not only needs to develop and monitor their own organization’s metrics, they need to understand the industry-based metrics that may be available. Have you read a recent “Data Breach Investigations Report” from Verizon Business, a “Global Internet Security Report” from Symantec, or a Ponemon Institute data breach cost study? These are three useful examples of valuable metrics tracking where the dangers lie and what the costs of those dangers have been across industry and government. Learn these numbers and use them in conjunction with your own to present a holistic, comparative picture of the security problems faced, how those problems manifest themselves in your environment, and the potential to indemnify your organization against future loss through security spending now.

So what to measure? Resolve to start with some basics. How many potential threats are detected through your various forms of monitoring on a monthly basis? Are damaging incidents appearing in places that you thought were adequately protected? Report on this to your management and governance bodies. You’ll sleep better at night. That sounds like a good resolution to me. Here’s to a safe and secure new year.

Opinions expressed are those solely of the author and not those of his employer.

iCloud and enterprise IT

When Apple announced iCloud at its Worldwide Developers Conference last June, it set acolytes abuzz with anticipation. While many in enterprise IT will no doubt dismiss the broader relevance of consumer cloud services like iCloud to their work, they do so at their peril.

In his keynote, Steve Jobs described iCloud as a common data storage and synchronization backend. iCloud syncs versions of every file the user creates on any device and then synchronizes these files across every device. These devices will all have access to the same data without having to email files or copy them to a memory stick. To quote Jobs, users can expect all of this magic to “just work.”

It’s a very appealing vision, and not just to consumers. Enterprise IT has been trying its best to deliver these kinds of services through a hodgepodge of technologies. Unfortunately, the results have typically been cumbersome to use and all too often break, much to the constant displeasure of an increasingly consumer-like corporate user.

IT naturally has very strong objections to enterprise use of these consumer cloud services. Data is not encrypted in the consumer cloud, so, if there is a breach like the one that occurred with Dropbox in June, sensitive information could fall into the wrong hands. Likewise, there are no service-level agreements to guarantee data availability.

Unfortunately, consumer cloud storage’s revolutionary functionality and ease of use will lead many enterprise users to deploy these services regardless of what IT’s policy may be. The folks in the IT department would be wise to take a hard look at how to deliver these new capabilities in an enterprise-grade fashion that magically “just works,” and manages to delight their constituency while maintaining the security and control over data.

Have a realistic discussion

We will get hacked and always have infected systems...”
When Alex Levinson graduated near the top of his class in January 2009 from Heald College in San Francisco, carrying an associate’s degree in computer networking with a concentration in information security, he fielded a surprisingly large number of employment offers in an economy that was on the fast track to the worst recession in more than 70 years.

Most of the offers were for positions like system or network administrator, decent entry-level posts for someone interested in IT. Levinson gave each some thought, but ultimately decided that a nine-to-five job wasn’t for him, not yet at least. “There were reasonable offers at the time,” Levinson, now 22, says. “But I just felt like I needed more.”

Months removed from the start of the financial crisis, the opportunities thrown Levinson’s way were telling of an industry in desperate need of young, motivated and highly skilled information security professionals, especially as organizations rely on computer networks in levels never thought possible.

Positions in information security fall under the STEM (science, engineering, technology and math) umbrella. These fields, according to the U.S. Department of Commerce, are paid higher than other industries, are less likely to experience joblessness and are essential to the nation’s competitiveness. Yet, studies show that fewer students are choosing to major in these areas, and the ones who do take longer to graduate.

Experts have attributed this to a number of factors, among them the belief that more and more IT jobs will be outsourced, a prevailing attitude among adolescents that science is too difficult a discipline on which to concentrate, a failure by high schools to adequately prepare pupils for these courses at the next level and a lack of understanding by colleges to place an emphasis on STEM student research, collaboration and support — rather than mere survival in class tracks known for their dog-eat-dog style of competition.

A profession, challenged

Security faces a more uphill climb than other STEM-related fields. According to a 2010 report from the Center for Strategic and International Studies, there are only about 1,000 individuals in the United States with the specialized security skills to defend cyber space, both at the public and private level. There needs to be at least 10,000.

Despite the rise of government-recognized National Centers of Academic Excellence in Information Assurance Education, which exist at more than 100 colleges across the country, many institutions treat security as a subset of a computer science degree.

“I think modern security education is so new that it’s still in a rapidly evolving phase,” says Mark Stamp, an associate professor at San Jose State University in California. “Just a few years ago, most graduates from computing-related programs would never have had a security course. Today, I don’t know what the exact percentage is, but I’m sure it’s more than half. And that number certainly is growing.”

Yet, while more colleges and universities seem to recognize the need to offer courses related to information security, many curricula appear to be a hodgepodge of subject matter, proof that academic institutions still don’t consider the discipline worthy of stand-alone status.

“And it’s a new and unsettled part of the curriculum, a lot of different things are taught in security courses,” Stamp says. “There is often a division of labor among various courses. The material taught varies widely — from high-level managerial platitudes to hardcore cryptography and everything in between. That is, security is often not treated as a coherent topic in its own right.”

This is a systemic weakness, Stamp says, that may be impacting the amount of skilled human capital making its way from lecture halls into the server room.

“I believe that computer science students should have an in-depth understanding of security, not just a surface-level overview,” he says. “The computer science students of today will be building the world’s critical infrastructure of tomorrow, and security mistakes can be costly. We don’t let people design bridges unless they know what they’re doing.”
Some educators have pushed for colleges to offer more specific courses in security that not only hone in on a specialty topic, but break down the taboo that instructors cannot teach certain lessons. In particular, George Ledin, a computer science professor at Sonoma State University in California, wants more schools to offer classes that center overworked professors who may not be as familiar with more narrow computer science topics and may be discouraged to ask students to think like a criminal. But Ledin says instructors must get past this.

“When you’re going to a medical school,” Ledin says. “You’re going to learn everything about the worse possible diseases. Likewise, if you’re a law student, you would benefit from learning more schools to offer classes that center security professionals. “What ended up happening just organically is that the volunteers were asked over and over again about their profession,” she says, adding that part of the work involves dissolving the myth for kids that it is security, pardon the phrase, a dorky job. “I think we need to dispel the ‘geek’ notion,” Peeler says. “I can say that as long as I’ve been working in this industry, I don’t think I’ve ever met a geek.” — Dan Kaplan

Healthy competition

After graduating with his associate’s, Levinson found that he was left craving more. In March of 2009, he got in his car and drove 2,700 miles to Western New York, where he matriculated at the Rochester Institute of Technology (RIT) to complete his degree. He started out as an applied networking and systems administration major, but quickly changed to information security and forensics. “I was good at it,” Levinson recalls of his decision to switch majors. “I noticed it was something that could keep me up.”

Levinson had the luxury of being accepted and enrolled into a program that offers a certificate in information security curriculum. As early as a few years ago, his only path for additional security education may have been through a certification program. “We’re just getting to the point where the weight of knowledge is getting large enough where students can expand their mind within the collegiate level,” he says. While at RIT, Levinson also had the opportunity to perform research, such as studying a controversial iPhone file that recorded the geographical locations of users. Still, while he was becoming well versed in defensive security strategies, he sought more action – in a word, competition.

In 2010, he saw a campus flier announcing the National Collegiate Cyber Defense Competition, a three-day event that asks teams to manage and protect a mock corporate network. Levinson and his fellow RIT teammates finished third out of nine regionally. He immediately was hooked. “Cyber security as a sport?” Levinson recalls. “It was crazy.”

That summer, he joined the big leagues when he earned a spot in the annual U.S. Cyber Challenge, launched in 2009 by the Center for Strategic and International Studies, and now run by the nonprofit Center for Internet Security (CIS). Not surprisingly, Levinson won a spot in the competition – held in three states that summer and featuring 35 participants – by using some hacker talent. “[My friend and I] brute forced the [qualifier online] quiz until we figured out which answers we got wrong,” he says. “We kept getting two questions wrong.”

The finals were held in Brooklyn and included four days of SANS Institute training leading up to a capture-the-flag competition, which pitted four teams of four against each other. This time, the contest asked the participants to play the role of the bad guy. Levinson’s team – which called itself “APT” in a tongue-and-cheek homage to the oft-overused advanced persistent threat buzzword – was able to successfully infiltrate a credit card database of a mock company, which helped it win the grand prize. “There’s a difference between trying to write an answer on a test about information security and being in a room and entering it on a keyboard while under pressure,” Levinson says. “At a lot of colleges, you go in and take tests and read books. But there’s something to be said for the hands-on, live-under-fire exercises.”

The competition ended with a networking event and career fair, featuring a number of government agencies and corporations looking to hire. Levinson now works as a security software engineer at Zynga, the world’s largest social game developer. “The connections that got me here wouldn’t have happened without competitive cyber security,” he says.

Mike Matonis, Levinson’s teammate, has since parlayed his victory into a job with CIS as a computer emergency response team analyst. He says the U.S. Cyber Challenge helps to break down the barriers that often prevent students from attending college, such as exorbitant costs, poor high school grades or a lack of accessibility to certain educational topics. In other words, if successful, these competitions may enable a whole new set of people to catapult into careers in information security.

“There are a lot of extremely capable and very talented people who haven’t done level-three calculus or can’t articulate or argue an abstract, complex encryption algorithm,” Matonis, 22, says. The competition allows for a quantifiable assessment of someone’s skill set, something educational upbringing may not be able to offer, he adds.

“[The whole competition side of it is important on a level that academia hasn’t gotten to yet],” Levinson says. “My experience tells me that companies can’t just hire someone with a competition and application of skill in a live environment is a really good indicator of where their skill set is at, where their talent lies.”

And it may also encourage some teenagers and young adults to reconsider their career paths. “They may have been destined to become real hackers,” says Will Pelgrin, chief executive of CIS and the former CISO of the state of New York. “This helps that generation [to] not go down the wrong path. There’s a moral compass to this.”

The hands-on nature of these challenges is not going unnoticed in the academic world. A number of colleges are getting on board with making security learning more active, including Pace University in New York – which just launched a new cyber security institute – all the way down to community colleges, like Hagerstown in Maryland, which recently announced the receipt of a $650,000 grant from the National Science Foundation.

Education efforts

Some educators have pushed for colleges to offer more specific courses in security that not only hone in on a specialty topic, but break down the taboo that instructors cannot teach certain lessons. In particular, George Ledin, a computer science professor at Sonoma State University in California, wants more schools to offer classes that center overworked professors who may not be as familiar with more narrow computer science topics and may be discouraged to ask students to think like a criminal. But Ledin says instructors must get past this.

“When you’re going to a medical school,” Ledin says. “You’re going to learn everything about the worse possible diseases. Likewise, if you’re a law student, you would benefit from learning more schools to offer classes that center security professionals. “What ended up happening just organically is that the volunteers were asked over and over again about their profession,” she says, adding that part of the work involves dissolving the myth for kids that it is security, pardon the phrase, a dorky job. “I think we need to dispel the ‘geek’ notion,” Peeler says. “I can say that as long as I’ve been working in this industry, I don’t think I’ve ever met a geek.” — Dan Kaplan

Healthy competition

After graduating with his associate’s, Levinson found that he was left craving more. In March of 2009, he got in his car and drove 2,700 miles to Western New York, where he matriculated at the Rochester Institute of Technology (RIT) to complete his degree. He started out as an applied networking and systems administration major, but quickly changed to information security and forensics. “I was good at it,” Levinson recalls of his decision to switch majors. “I noticed it was something that could keep me up.”

Levinson had the luxury of being accepted and enrolled into a program that offers a certificate in information security curriculum. As early as a few years ago, his only path for additional security education may have been through a certification program. “We’re just getting to the point where the weight of knowledge is getting large enough where students can expand their mind within the collegiate level,” he says. While at RIT, Levinson also had the opportunity to perform research, such as studying a controversial iPhone file that recorded the geographical locations of users. Still, while he was becoming well versed in defensive security strategies, he sought more action – in a word, competition.

In 2010, he saw a campus flier announcing the National Collegiate Cyber Defense Competition, a three-day event that asks teams to manage and protect a mock corporate network. Levinson and his fellow RIT teammates finished third out of nine regionally. He immediately was hooked. “Cyber security as a sport?” Levinson recalls. “It was crazy.”

That summer, he joined the big leagues when he earned a spot in the annual U.S. Cyber Challenge, launched in 2009 by the Center for Strategic and International Studies, and now run by the nonprofit Center for Internet Security (CIS). Not surprisingly, Levinson won a spot in the competition – held in three states that summer and featuring 35 participants – by using some hacker talent. “[My friend and I] brute forced the [qualifier online] quiz until we figured out which answers we got wrong,” he says. “We kept getting two questions wrong.”

The finals were held in Brooklyn and included four days of SANS Institute training leading up to a capture-the-flag competition, which pitted four teams of four against each other. This time, the contest asked the participants to play the role of the bad guy. Levinson’s team – which called itself “APT” in a tongue-and-cheek homage to the oft-overused advanced persistent threat buzzword – was able to successfully infiltrate a credit card database of a mock company, which helped it win the grand prize. “There’s a difference between trying to write an answer on a test about information security and being in a room and entering it on a keyboard while under pressure,” Levinson says. “At a lot of colleges, you go in and take tests and read books. But there’s something to be said for the hands-on, live-under-fire exercises.”

The competition ended with a networking event and career fair, featuring a number of government agencies and corporations looking to hire. Levinson now works as a security software engineer at Zynga, the world’s largest social game developer. “The connections that got me here wouldn’t have happened without competitive cyber security,” he says.

Mike Matonis, Levinson’s teammate, has since parlayed his victory into a job with CIS as a computer emergency response team analyst. He says the U.S. Cyber Challenge helps to break down the barriers that often prevent students from attending college, such as exorbitant costs, poor high school grades or a lack of accessibility to certain educational topics. In other words, if successful, these competitions may enable a whole new set of people to catapult into careers in information security.

“There are a lot of extremely capable and very talented people who haven’t done level-three calculus or can’t articulate or argue an abstract, complex encryption algorithm,” Matonis, 22, says. The competition allows for a quantifiable assessment of someone’s skill set, something educational upbringing may not be able to offer, he adds.

“[The whole competition side of it is important on a level that academia hasn’t gotten to yet],” Levinson says. “My experience tells me that companies can’t just hire someone with a competition and application of skill in a live environment is a really good indicator of where their skill set is at, where their talent lies.”

And it may also encourage some teenagers and young adults to reconsider their career paths. “They may have been destined to become real hackers,” says Will Pelgrin, chief executive of CIS and the former CISO of the state of New York. “This helps that generation [to] not go down the wrong path. There’s a moral compass to this.”

The hands-on nature of these challenges is not going unnoticed in the academic world. A number of colleges are getting on board with making security learning more active, including Pace University in New York – which just launched a new cyber security institute – all the way down to community colleges, like Hagerstown in Maryland, which recently announced the receipt of a $650,000 grant from the National Science Foundation.
The nation’s approach to human rights in cyber space is lacking, reports
Danny Bradbury.

On the frozen plains of Manitoba, construction is currently underway on a Canadian Museum for Human Rights. The building, which will showcase freedom issues around the world and celebrate Canada’s traditional role as a peacekeeper, will be the first national museum in 40 years. But while private donors and government officials struggle to create this physical monument, experts argue that Canada is ignoring the issue of human rights in cyber space.

In November, Canadian web hosting companies were criticized for hosting websites for the Syrian government. The Syrian government, which tortured Canadian citizen Maher Arar, is currently killing tens of civilians each day in a violent attempt to retain power, and has been accused of crimes against humanity by Human Rights Watch.

The issue came to light after the University of Toronto’s Citizen Lab produced another report on the use of filtering technologies by countries, including Syria. Its document, “Behind Blue Coat: Investigations of commercial filtering in Syria and Burma,” found that U.S.-firm Blue Coat had been selling its filtering technology to Syria and Burma, even though those countries have been targeted by U.S. export restrictions.

Ron Diebert, director of the Citizen Lab, explains that a U.S. journalist asked him about a North African company that the report had identified as carrying out the filtering. He decided to look into the company some more.

“I looked on the site of this company and it said that it had a co-location facility in Vancouver,” he says. “That company was Platinum, a 20-year-old software and services firm affiliated with The Kernel, a concern located in Dubai. Platinum had registered an IP block through Kelowna, British Columbia-based Rackforce. It hosted its website through Montreal-based iWeb. Citizen Lab began investigating the websites hosted by Platinum. “We started looking up IP addresses and realized that quite a few interesting websites are being hosted in Canada, including a streaming TV site that was in the sanctions list.”

The researchers found 17 Syrian government websites that were being hosted in Canada. They deliberated for a while, and did not approach the Internet service provider (ISP) in question directly, wary that there was also a free speech issue, Diebert says. The group finally decided to publish its findings when the Human Rights Watch report on Syria emerged.

Canada has been criticized for its hosting of specious websites before. iWeb was fingered in 2008 for hosting sites for Hamas and Hezbollah. These two groups are designated as terrorist organizations by the Canadian government. In that instance, iWeb eventually took down the offending pages after it found that the Arabic language versions of the sites included inflammatory material, such as instructions on concealing bombs. iWeb’s response to the latest Citizen Lab report was terse. The organization pointed out that the Canadian government has not barred Canadian companies from doing business with Syria in general. Only specific Syrian entities have been blocked with sanctions, it said, and other than Addounia TV, none of the entities mentioned in the report fell under that sanction. However, iWeb was, at least until recently, a host of Addounia.tv. That site is now hosted on a German server.

By focusing on what he sees as the more “convenient” aspects of the report, Diebert argues that iWeb is dodging the more important questions raised by Citizen Lab. The report points out that the presence of sanctions against sites like Addounia should be enough to bring into question the idea of hosting anything connected to the Syrian regime.

Companies like Web and Rackforce (which, according to Netcraft, also hosted Addounia.tv in 2008), are clear on this point, however. Rackforce CEO Brian Fry says there is a clear line beyond which ISPs can take action and take down websites. It has to be illegal.

That’s just the problem, though. Citizen Lab wonders whether the specific wording in Canadian government legislation covers website providers at all. The legal structure is unclear, he says. It needs government leadership, but, unfortunately, there isn’t any.

Diebert says there is a “vacuum” when it comes to Canadian thinking on issues such as these. On hearing of the Syrian hosting issue, the Canadian government launched a Royal Canadian Mounted Police investigation of the companies involved, which Diebert considers a kneejerk reaction. “I wish that it would have provoked a broader rethinking about cyber space policy in our country,” he says.

To be fair, Canada was one of 14 countries helping internet dissidents and activists at a conference in mid-December on internet freedom at the Hague. But Diebert argues that its level of involvement was telling.

And while it makes noises about supporting internet dissidents, Canada nevertheless allows companies, such as Netweeper, based in Guelph, Ontario, to sell internet-filtering technology to countries including Yemen, Qatar and the United Arab Emirates (UAE).

“They’re censoring the internet so that citizens in the UAE can’t get access to women’s health information because it contains the word ‘breasts,’” Diebert says. Policy makers should be paying serious attention to these issues, he adds.

“There is a question of what type of due diligence companies like these should do when it comes to hosting content like this,” he says. The problem for ISPs is that due diligence is hard to achieve when working with high customer volumes on razor-thin margins. Currently, transgressions must be highlighted by third parties, through the ISP’s abuse-reporting system, for it to reach the company’s radar.

“We have 1,500 customers and they have the ability to put up tens of thousands of websites each,” Fry adds.

When clients such as the Syrian government use intermediary companies to arrange hosting contracts for websites, it becomes difficult for companies like Rackforce to spot potential problems.

“We were well aware that we had Syrian customers that were hosted in our system,” says Fry. “That doesn’t mean that we knew that it had anything to do with the Syrian government or anything of the sort.”

Canada’s government may not be interested in working through such thorny policy issues with ISPs, but it has no problem imposing other policy decisions. Pending lawful access legislation in Canada could require ISPs, such as Rackforce, to introduce monitoring technologies that would enable law enforcers to retrieve information about internet users and their habits.

Such measures have Fry worried about the economic ramifications as ISPs (espe- cially smaller ones) struggle to introduce the necessary systems. He suggests that they need to be accompanied by financial incentives, such as tax credits.

If the government is ignoring such arguments, what hope is there for a considered response to issues such as due diligence in hosting and its implications for foreign policy in cyber space?

While Canada slumbers, the Russians and Chinese are actively developing their policies, treating cyber space foreign policy as a subject worthy of high-level consideration, Diebert says.

“We need to be part of something that shores up cyber space as an open commons,” he says. “We are really not doing that.”

Human rights
CANADA’S THORNY HOSTING PROBLEM
I n an advanced persistent threat (APT) attack, perpetrators research a specific target and customize the malware so that its signature cannot be identified by any existing anti-malware tools. Crimes of opportunity happen every day. A car door left unlocked leads to the theft of a wallet sitting on the front seat. A company laptop is stolen from the security checkpoint at an airport. A family out for a day trip comes home to find its front door open and its valuables gone. With crimes of this nature, the victim is often selected at random. Now, imagine that a crook not only breaks into your building, but creates a door that only he can see so that he can come and go at his leisure, stealing not only your property, but ideas you have written down or drawings for a new widget you plan to build. One might consider this unlikely for a house, but it happens every day to computers.

Generally speaking, crimes of opportunity are similar in nature to malware that infects millions of computers worldwide. With simple malware phishing attacks, the perpetrator generally is playing a numbers game—he sends out millions of emails containing a compromised link, for example, and hopes that a small fraction, or perhaps even fewer people, respond. Even if protective software stops 99 percent of the infected emails, and good computing practices prevent even more, the small number that get through often are enough to make a spam attack financially viable, says Christopher Smoak, a research scientist at the Georgia Tech Research Institute in Atlanta. On the other hand, in an advanced persistent threat (APT) scenario, the perpetrator spends a considerable amount of time researching a specific target, often customizing the malware so that its signature is not identified by any existing anti-malware software, Smoak says. Two characteristics of such sophisticated attacks are that the adversary has significant resources, both financially and technologically, and an end goal that might not have anything to do with pure financial gain.

With the Stuxnet attack on nuclear facilities in Iran in June 2010, for example, Smoak says the attackers had in-depth knowledge of how the Siemens supervisory control and data acquisition (SCADA) systems worked, as well as considerable financial resources to develop and deliver the attack. Such knowledge of how the hardware operated, as well as intelligence on the installation itself, likely took a long time to obtain, he says.

Smoak says similar characteristics have been identified in what McAfee Labs’ scientists recently dubbed Operation Shady RAT. The attack on more than 70 government, corporate and nonprofit entities was discovered when researchers came across a command-and-control server used by the attackers for directing remote administration tools, commonly called RATS. While investigating the server, McAfee came across log files dating back more than five years.

“The low-and-slow attack lends itself to an APT,” Smoak says. “It might take days, weeks, months or several years before it is even launched, and is designed to run for a long time.” As for why someone might opt for an attack that might not pay off for years, he says, “Sometimes it’s cheaper to steal the information rather than to build it yourself.” Other times, he says, the attack might be for geopolitical reasons, such as with Stuxnet.

Companies and government organizations of all sizes need to realize that their systems, the saying goes: those that have been compromised and those that don’t know they’ve been compromised. Using this truism as a baseline, Jonkman stresses the importance of using layered security technologies in conjunction with effective user training and education.

What is clear is that from an organizational level, “we’re leaking information like a sieve,” he says. “It used to be that we had a crunchy exterior perimeter (protection) with a soft inside. There’s no crunchy exterior perimeter anymore.”

Jeff Horne, practice manager of malware solutions for Denver-based Accuvant Labs, says companies need to recognize that either they have been compromised or they will be. Today’s attackers have sophisticated ways of bypassing perimeter protections, so Horne says organizations should focus on outgoing communications. There is little value to a hacker if they are able to compromise data on a server, but can not transfer it off the network, he says.

Horne recommends a two-pronged defense against malware. The first is to use a combination of network best practices to keep data secure. Next, in order to ensure that compromised assets cannot leave the network. Malware has become a commodity easily purchased over the internet, he says. This malware can be customized for a specific target so that it can bypass security protections. Companies must ensure that they have layered defenses and do not rely just on their firewalls or anti-virus software. Horne says. Defensive approaches, such as segregating mission-critical systems on protected virtual LANs (VLANs) or simply keeping some systems physically separated from the corporate network, can prevent access to certain machines if the network is attacked. Additionally, network managers can remove the ability for PCs in a network to talk directly to each other, requiring all file-sharing to instead be done via servers that can be better protected. By barring peer-to-peer communications, Horne says, a number of exploits can be stopped in their tracks.

Most important, however, security and network managers must stop unauthorized data from being sent off the network. This is more complicated, he says, because exploits can use innocuous codings holes to transfer data out.

If the network infrastructure was not built with security embedded into the underlying technology, then additional defenses will have to be tacked on to make up for the deficiencies, he says. One such weakness is allowing users to turn off automatic updates. While some users might have a valid reason for stopping updates, most employees need to have these updates turned on, even if they do cause a performance hit on their systems, Horne adds.

Proprietary software and Windows service packs also need to be updated on a regular basis, but for these applications is necessary to ensure that the upgrades do not crash the existing applications. Sometimes, he says, this process
At WGU we respect your time and intelligence, because what you know is more important than time in a classroom. WGU’s ONLINE competency-based approach puts you in control of your academic destiny... and your own security.

Master of Science
Information Security and Assurance

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

SECURITY TIPS
Top 10

1. Security is weakest at the human level. Therefore, organizations should:
   - Implement consistent security awareness training with associated testing to gauge effectiveness.

2. Enforce security in all projects at the concept phase. Incorporating controls later in the implementation results in increased costs and less effective results.

3. Develop procedures to ensure data stored on removable media devices is always encrypted. Delete files from flash drives as soon as possible.

4. Protect passwords. Change them often and do not write them down and leave them unsecured.

5. Develop an effective policy for use of social media to limit the potential loss of critical company information, while leveraging the marketing flair of social media.

6. Review access control frequently to prevent “privilege creep.” This is critical as employee roles expand.

7. Consider application whitelisting (allowing the use of good applications and prohibiting bad ones) for employees who routinely manage sensitive data.

8. Conduct periodic risk assessments to manage security spending effectively. Apply controls based on risk to the business.

9. Move to multifactor authentication where feasible.

10. Use a program that either prevents or warns you about navigating to a known spyware site.

Source: Unisys

Human nature, Titus says, is generally the weak link in a company’s data security posture. One’s culture is often based on helping people in need, she says, making social engineering an effective way to defeat security protections.

Companies need to “empower people to participate,” she says. Rather than punishing an employee who might step a C-suite executive from entering a secure area without proper credentials, employees need to know that if they follow proper precautions, their actions will not cause reprisals.
GUARDING AGAINST A DATA BREACH

THE 2012 SURVEY

CAN YOU SEE EVERYWHERE AT ONCE?
YOU CAN.

You can’t stop threats if you can’t spot them. That’s why HP Enterprise Security offers proven solutions that deliver context-aware visibility into security risk. There’s no better way to proactively detect security issues and drive situational awareness across your applications, operations, and infrastructure. The HP Security Intelligence and Risk Management platform provides integrated correlation, application protection and network defenses that can secure modern IT environments from sophisticated threats.

For more information go to www.hpenterprisesecurity.com

Advanced protection against advanced threats.

Copyright ©2011 Hewlett-Packard Development Company, L.P.
Data breach survey

SURVIVAL OF THE FITTEST

Budgets will be tight in 2012, but two-thirds of respondents to our survey believe they’ve got security covered. Illena Armstrong reports.

T
e evolve is to survive. It is a familiar scientific concept that can be encountered just as easily in business conver-
sations over the water cooler as it can be in classic pieces of literature.

Its place in the information security industry is about as sur-
prising as the enduringly humble budgets that still beleaguer most IT security departments. Despite these flat or, in some
cases, still declining funds, evolving to survive and perhaps even prosper through modest profit growth remains a driving
force for most organizations.

However, it also is a major motivator for others. As if in
salute to this Darwinian supposition, regulators and, of course,
cyber criminals continue to modify their plays to advance their
own causes even further.

As uncovered in SC Magazine’s fifth annual “Guarding
Against a Data Breach” survey, IT security leaders and their
executive bosses, meanwhile, are pushing ahead to take on
a 2012 that promises still more of the advanced cyber attacks
they saw last year, an increase in audits by compliance watch-
dogs, and a continuation of end-users and consumers relying
on an array of vulnerable technologies to conduct business.

And all these things are happening just as most economic
forecasters predict a drearier year than even they had imag-
ined only a few months ago. A recent Federal Reserve Bank
of Philadelphia survey reveals that the 45 forecasters queried
only expect a 2.4 percent jump of GDP growth this year versus
an earlier figure of 2.6 percent. The unemployment growth rate
also became less rosy in a matter of months, falling from a
previous estimate of 8.8 percent to 8.6 percent.

Show me the money

According to SC’s Data Breach survey, sponsored by HP Enter-
prise Security, of the 486 information security pros participat-
ing, 63 percent are confident that their company’s IT security
departments have the power, executive support and budget/
resources necessary to safeguard customer, client and other
critical corporate data. This is up from last year’s survey, which
saw 58 percent out of 468 respondents feeling such confidence.

“Budgeting is always a tricky business,” says Jeffrey Brown,
global information security program manager with GE Capital.

“Are your routers security devices or networking devices?
Does anti-virus software fall under operating system costs or
under IT security? While the allocations are not always clear,
I think, in general, there’s still a healthy amount of IT budget
going toward meeting security needs.”

Compared to last year’s 36 percent, a very close 34 percent
of respondents expect their budgets related to IT security proj-
ects and data leakage prevention efforts to increase. For most,
this funding will remain the same, with 61 percent predicting a
flat budget line. Meanwhile, 6 percent foresee a decrease.

Financial pressures, then, persist, but this reality rarely
changes, Brown says. That’s why information security leaders
must continue to make a sound business case for their efforts,
ensure the money they do have is spent wisely, and tackle
the top risks first. “This is basic risk management, really,” he
explains.

Even with these steps, though, financial support for IT
security is either level or dwindling in most public and private
organizations, say experts. There may be more talk going on,
but there is no uptick in spending, says Bruce Bonsall, former
VP and CISO with MassMutual, who is now an industry
consultant.

Jerry Dixon, director of analysis at Team Cymru, and former
head of US-CERT, agrees, explaining that his clients’ budgets
largely are consistent with last year’s, with most organizations
“squeezing every bit of life from their existing infrastructures.”

Wielding the right tool

Although many organizations are leveraging the technologies
they already have in place, some others are investing in various
technologies that further bolster protections against newer
threats, according to this year’s survey results.

Last year, various types of mobile security solutions led the
fray among the technologies that survey respondents were
looking to deploy in 2011. These same solutions have a decent
showing for possible implementation in 2012 at 41 percent.
However, it seems for many security practitioners, the need
to gain a better idea of what’s happening on the network is
overtaking some of their more longer-standing concerns. Half
of the survey participants cite network monitoring solutions
as top deployment priorities for the next 12 months. Another
38 percent are looking to roll out vulnerability management
solutions, and 13 percent are considering security incident
and event management (SIEM) deployments. (Editor’s note:
network monitoring, vulnerability management and SIEM
solutions were not included as choices in previous SC data
breach surveys).

“The so-called advanced persistent threat (APT) has
elevated the game,” says Bonsall, adding that business leaders
have accepted that they no longer can keep the bad guys out
of their networks without the right tools and processes in place.

Dixon says he is seeing a large increase in the testing and
purchasing of network monitoring solutions. As well, many
companies are re-energizing security awareness training for
their end-users since many attacks still rely heavily on social
tool engineering methods to gain initial entree into corporate
or government infrastructures.

“I think there’s a real concern that current security products
aren’t working,” he says. Companies have invested in various
solutions to fortify their networks, “yet they’re still having
major breaches.”

But, more traditional tools aren’t being discounted out of
hand. Alongside mobile security solutions, and now tools
that provide a more holistic view of the network, survey
respondents are considering for deployment this year email

Which drivers have aided in obtaining more resources
for initiatives associated with safeguarding data?

<table>
<thead>
<tr>
<th>Driver</th>
<th>2012</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory mandates</td>
<td>63%</td>
<td>56%</td>
</tr>
<tr>
<td>Possible negative impact</td>
<td>53%</td>
<td>56%</td>
</tr>
<tr>
<td>Possible profit loss</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>Customer demand</td>
<td>28%</td>
<td>28%</td>
</tr>
<tr>
<td>Exec. board demand</td>
<td>25%</td>
<td>27%</td>
</tr>
<tr>
<td>Budget hasn’t increased</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>Investor demand</td>
<td>8%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Which guidelines are priorities to comply with when it comes to protecting customer/client data that is stored or shared electronically by your company?

<table>
<thead>
<tr>
<th>Framework</th>
<th>2012</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPAA</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>PCI</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>SOK</td>
<td>41</td>
<td>37</td>
</tr>
<tr>
<td>State data breach laws</td>
<td>38</td>
<td>33</td>
</tr>
<tr>
<td>FISMA</td>
<td>27</td>
<td>29</td>
</tr>
<tr>
<td>E-discovery legislation</td>
<td>24</td>
<td>27</td>
</tr>
<tr>
<td>GLBA</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Red Flags Rules</td>
<td>17</td>
<td>14</td>
</tr>
<tr>
<td>FFEIC</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>European Union Data Protection</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>
Have you strengthened your security awareness and training for corporate employees to help safeguard customer, client and other critical corporate data?

<table>
<thead>
<tr>
<th>Year</th>
<th>Yes, but not enough</th>
<th>Yes</th>
<th>No</th>
<th>I don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>35</td>
<td>16</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2012</td>
<td>45</td>
<td>34</td>
<td>13</td>
<td>4</td>
</tr>
</tbody>
</table>

ON THE HORIZON: A national data breach law

Support by information security professionals for the passage of a national data breach law remains mixed, but few say such a law actually would impede their abilities to do their jobs.

Only 33 percent of practitioners participating in SC Magazine’s “Guarding against a data breach” survey believe that the passage of a federal data breach notification law would help them in their security efforts to protect customer or client data, while another 33 percent say it would not. Meanwhile, almost half of respondents believe the national law would not impede or hurt their strides in securing critical data. A mere 17 percent say it would, with another seven percent agreeing with this sentiment, but noting the negative impact would be limited.

André Gold, head of technology operations and security at Auto-Trader.com, agrees that such a law would do little to help organizations with their security efforts, especially in the ways that others, such as Sarbanes-Oxley or the Health Insurance Portability and Accountability Act (HIPAA), have.

The upward trend in security budgets makes perfect sense.”
—Becky Bace, president and CEO, Infidel

Jeff Combs, owner of security recruiting company J. Combs Search, and director of recruiting at Acumin.

“Every company is different, but given the uncertain economic climate, there will continue to be cost-cutting and consolidation — often at the expense of providing adequate security and IT risk management controls,” Combs says.

On a more positive note, Team Cyber’s Dixon says that while he is seeing more companies looking at managed security services because of limited budgets, many larger organizations are indeed hiring for a slew of technical security posts to cover firewall administration, network monitoring, and more. Given all the high-profile breaches that have occurred, worries about becoming the next publicized victim are pushing companies to staff up, he says.

“Let’s be honest, they’ve been understaffed for years,” he says.

Cheap tricks

Companies are relying on still other ways to fend off evolving attackers and be prepared for an increase in external audits by regulators. One major step toward meeting some basic security needs and staying in compliance is through the implementation of security training and awareness programs for end-users.

Compared to last year, there was an ever-so-slightly increase in the number of SC’s data breach survey respondents who have
Data breach survey

Which security solution is your company considering deploying to help safeguard data in the next year?

<table>
<thead>
<tr>
<th>Solution</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network monitoring</td>
<td>50%</td>
</tr>
<tr>
<td>Email management/content filtering</td>
<td>43%</td>
</tr>
<tr>
<td>Mobile security</td>
<td>41%</td>
</tr>
<tr>
<td>Database security</td>
<td>41%</td>
</tr>
<tr>
<td>Email encryption</td>
<td>39%</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>38%</td>
</tr>
<tr>
<td>Vulnerability management</td>
<td>38%</td>
</tr>
<tr>
<td>Web application security</td>
<td>34%</td>
</tr>
<tr>
<td>Two-factor authentication</td>
<td>31%</td>
</tr>
<tr>
<td>Cloud security</td>
<td>26%</td>
</tr>
<tr>
<td>SIEM</td>
<td>13%</td>
</tr>
<tr>
<td>Outsourcing security</td>
<td>12%</td>
</tr>
</tbody>
</table>

strenthened their end-user security training. Among their training methods, 70 percent of respondents send email updates to staff on information security/data theft; 57 percent offer periodic online training for employees; 55 percent provide regular, live training sessions for workers; 49 percent have newsletters on information security/data theft; and 13 percent turn to annual salary reviews that account for adherence to internal information security rules/guidance.

“Companies are realizing that it takes training to change culture,” says Gene Fredriksen, CISO of Tyco International. “It’s a cheap control. It also demonstrates due diligence.”

On top of giving more attention and dollars to staff training, companies are looking harder at the perceived benefits and cost-savings associated with security services. Among the other solutions that companies are considering making part of their programs this year, 12 percent of respondents are looking to outsource security. Another 26 percent are pondering cloud security services.

“This, in some ways, reflects the lead edge of the impact of the cloud,” says Bace. “When key IT functions are outsourced, a lot of the security provisions are either included as part of the function or else implemented by selection of a specific option in the service agreement. This requires a different type of professional with skills that may not be served by current models.”

But, cloud services, overall, are still young. Plenty of areas of concern exist that must be addressed before more organizations begin relying on them.

“Cloud is the only real sea change I see looking toward the future, and there is still little sense of how it will ultimately affect life in the IT and IT security trenches,” says Bace.

Yet, of the 488 respondents to the survey, more than a quarter (28 percent) say they are storing sensitive data in the cloud, with 18 percent using private clouds, 3 percent enlisting public clouds, and 7 percent relying on security-as-a-service (SaaS) providers.

Future

Cloud services, web applications, mobile devices and social networking all continue to be vectors of attack causing major concern for corporate executives, say experts. Then, there are the attack types to worry about: APTs, social engineering, malware and loads of others, which all are spearheaded by more sophisticated and often organized cyber criminals, hacktivists or state-sponsored attackers.

“This is why we’re seeing an increased emphasis on protections against APTs [through] network monitoring, SIEMs/PIEMs and vulnerability management, and social engineering [through] education training and awareness,” says Cline.

But, more than the investments in technologies and policies, security pros must continue to make the business case for their programs. Without this, the executive support they seek will continue to elude them.

“As the economy continues to struggle, the temptation will always be to cut from less tangible, non-revenue-generating areas like information security,” says GE’s Brown. “This is where security leaders need to keep abreast of the threat landscape, align their security objectives with business strategy, and, ultimately, know which budget battles they can concede and which they can’t.”

The methodology for this year’s study was as follows:

Email invitations were sent to approximately 50,000 IT security professionals. A total of 488 respondents completed the survey online, between Oct. 19 and Nov. 10. The results are not weighted, and the margin of error is +/- 3.7 percent.
A slew of new bills affecting cyber security policies are making their way through Congress. Stephen Lawton takes a look.

In a display of bipartisanship, party leaders said they would work with the White House to pass cyber security legislation during the 2012 presidential election year. While a number of bills are stalled in Congress, cyber security legislation seems to be garnering widespread support.

Although measures around data security often meet their demise on Capitol Hill due to disputes over wording or because other issues take priority, two bills – one in the House and the other in the Senate – appear to have a decent chance of passage.

The Cyber Intelligence Sharing and Protection Act of 2011 (H.R. 3923), introduced by Rep. Mike Rogers, R-Mich., recently passed through the House Intelligence Committee on a 17-1 vote and is now headed to the House floor. Meanwhile, two Senate bills also are working their way through the upper house, and have bipartisan support.

One of the bills, the Cyber Security and Internet Freedom Act of 2011 (S.413), is similar in nature to the recommendations of the House Republican Cyber Security Task Force, Senate Leader Harry Reid, D-Nev., says. Those recommendations have received bipartisan support, not only from Reid, but also from Sen. Joseph Lieberman, I-Conn., Tom Carper, D-Del., and Susan Collins, R-Maine, and establishes an Office of Cyber Space Policy within the Department of Homeland Security (DHS), as well as an infrastructure for fighting threats.

Larry Clinton, CEO of the Internet Security Alliance, says he is encouraged that legislators recognize that cyber security is an economic issue, not just a technical concern.

Clinton, who supports the House bill, recommends that legislation be passed that includes incentives for a company to employ improved security practices. “It’s in their economic self interest to be more profitable,” he says.

He likens the potential fiscal perks for strong security to that of the early 20th century, when government regulations made it economically beneficial for the electric and telephone companies to expand their services for universal access.

While the directive does not address the issue of privacy, companies in various vertical industries have created groups to share anonymized data about breaches so that they can better defend against them in the future. These groups, called information sharing and analysis centers (ISAC), were developed as a result of the presidential directive.

The current crop of proposed legislation goes beyond this presidential directive, however, and could codify into law changes to existing privacy laws.

ISA’s Clinton says the government is more accustomed to defending against an attack from a single entity. Cyber security is more akin to a terror attack where the enemy is harder to identify and might not be a single entity. Today’s regulations favor the attackers, he says.

Attacks are inexpensive to conduct and quite profitable. It is easy to obtain malware scripts. The tools for the attacks can be used multiple times. “The business model is great,” he says.

By changing the economic playing field through legislation and financial incentives for industry, Clinton adds, the government can make it more profitable to companies to build inherently more secure networks than having them count on the expense of remediating a problem as a cost of doing business.

“Because other issues take priority, two bills appear to have a decent chance of passage,” he says. “However, not all are pleased by the proposed legislation. “The Cyber Intelligence Sharing and Protection Act would create a cyber security exception to all privacy laws and allow companies to share the private and personal data they hold on their American customers with the government for cyber security purposes,” a statement from the American Civil Liberties Union (ACLU) says. The bill, the group points out, would not limit the companies to sharing only technical, non-personal data.

The Electronic Frontier Foundation (EFF) also voiced concern about the use of data collected by the federal government. “H.R. 3923) doesn’t limit what the federal government can do with the data or private communications that ISPs and others hand over, except to say that it can’t be used for regulatory purposes – apparently it can be used for law enforcement and intelligence targeting purposes.”

A competing bill, backed by Rep. Dan Lungren, R-Calif., and still in draft form, appears to appease some House Democrats as it would create a nonprofit entity called the National Information Sharing Organization, which would include members from federal agencies, corporations and civil liberties groups. The bill has received a more favorable response from some because it doesn’t assign a specific role for DHS.

Still, as organizations such as the ACLU and EFF express concern about the swapping of data among companies and the government, a presidential directive authorizing such sharing has been in place since 2003. President George W. Bush signed Homeland Security Presidential Directive-7, a direct response to the events of Sept. 11, 2001, as a way to gather information about potential future attacks. The act directs the secretary of the DHS “to maintain an organization to serve as a focal point for the security of cyber space. The organization will facilitate interaction and collaboration between and among federal departments and agencies, state and local government, the private sector, academia and international organizations.”

Specifically, the directive says federal agencies “…will collaborate with appropriate private sector and continue to encourage the development of information sharing and analysis mechanisms… to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.”

While the directive does not address the issue of privacy, companies in various vertical industries have created groups to share anonymized data about breaches so that they can better defend against them in the future. These groups, called information sharing and analysis centers (ISAC), were developed as a result of the presidential directive.

The current crop of proposed legislation goes beyond this presidential directive, however, and could codify into law changes to existing privacy laws.

ISA’s Clinton says the government is more accustomed to defending against an attack from a single entity. Cyber security is more akin to a terror attack where the enemy is harder to identify and might not be a single entity. Today’s regulations favor the attackers, he says.

Attacks are inexpensive to conduct and quite profitable. It is easy to obtain malware scripts. The tools for the attacks can be used multiple times. “The business model is great,” he says.

By changing the economic playing field through legislation and financial incentives for industry, Clinton adds, the government can make it more profitable to companies to build inherently more secure networks than having them count on the expense of remediating a problem as a cost of doing business.

“If you make it about corporate responsibility, it’s unsustainable,” he says. “You need to alter the economics so it’s in [the enterprises’] economic self-interest to be more secure.”

Today’s hacktivists publicize sensitive data, bring down networks, and cut off services. And the collateral damage to governments, businesses and consumers is mounting. To defend against this latest onslaught of cybercrime, our community must join forces. At RSA® Conference 2012, our community must join forces. At RSA® Conference 2012, today’s hacktivists publicize sensitive data, bring down networks, and cut off services. And the collateral damage to governments, businesses and consumers is mounting. To defend against this latest onslaught of cybercrime, our community must join forces. At RSA® Conference 2012, we have been preparing for an exciting 2012 as we somewhat change the format of our product pages. We know that you have wanted a bit more depth in our Group Test reviews, and just about the only way to do that is to increase the space that we allot to each product. That is exactly what we have done. Now, instead of a half-page per product, we will be devoting an entire page to each. That will let us tell you a bit more about our impression. That’s just one of our changes, though.

In addition, instead of having two Group Tests in each issue, we now will focus on a single group. This is important for a lot of reasons. First, taking up twice the space for an individual product doesn’t leave room for as many products in the same number of pages.

The second, and perhaps more important reason, is that the composition of the groups that have been tried and true over the years has changed markedly. Today, we have seen the demise of vendors in some groups to the extent that there simply are not enough players in that niche to make a worthy set to review. These vendors have been acquired, have gone out of business or have significantly changed their business. That attrition has left us with little to work with in some cases.

This month, we grouped multifactor and biometric authentication together in a single group. Even so, with numerous companies in the biometric space selling off their technology, we were left with just one. There are always unintended consequences to things that we change.

The big one for us is that we have the opportunity to carry out some-thing that we started over the past year or so: developing themes. Our theme this time is authentication, and we have a great crop of multifactor products keeping our lone biometric authentication tool company.

Also, we’re breaking down our star ratings system to include, in some cases, fractional designations – ¼, ½ and ¾ stars – to reflect the accuracy of our test criteria. Our final conclusions and ratings are subject to the judgment and interpretation of the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

Welcome 2012!

Here at the SC Lab, we have been preparing for an exciting 2012 as we somewhat change the format of our product pages. We know that you have wanted a bit more depth in our Group Test reviews, and just about the only way to do that is to increase the space that we allot to each product. That is exactly what we have done. Now, instead of a half-page per product, we will be devoting an entire page to each. That will let us tell you a bit more about our impression. That’s just one of our changes, though.

In addition, instead of having two Group Tests in each issue, we now will focus on a single group. This is important for a lot of reasons. First, taking up twice the space for an individual product doesn’t leave room for as many products in the same number of pages.

The second, and perhaps more important reason, is that the composition of the groups that have been tried and true over the years has changed markedly. Today, we have seen the demise of vendors in some groups to the extent that there simply are not enough players in that niche to make a worthy set to review. These vendors have been acquired, have gone out of business or have significantly changed their business. That attrition has left us with little to work with in some cases.

This month, we grouped multifactor and biometric authentication together in a single group. Even so, with numerous companies in the biometric space selling off their technology, we were left with just one. There are always unintended consequences to things that we change.

The big one for us is that we have the opportunity to carry out some-thing that we started over the past year or so: developing themes. Our theme this time is authentication, and we have a great crop of multifactor products keeping our lone biometric authentication tool company.

Also, we’re breaking down our star ratings system to include, in some cases, fractional designations – ¼, ½ and ¾ stars – to reflect the accuracy of our test criteria. Our final conclusions and ratings are subject to the judgment and interpretation of the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.

★ ★ ★ ★ ★ Outstanding. An “A” on the product’s report card.
★ ★ ★ ★ Carries out all basic functions very well. A “B” on the product’s report card.
★ ★ ★ Carries out all basic functions to a satisfactory level. A “C” on the product’s report card.
★ ★ Fails to complete certain basic functions. A “D” on the product’s report card.

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.

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.

The last change this year? Our new lab dog, Dillon. So with that, we at the SC Labs wish you a spectacular 2012, and my personal wish for you is that your net work!

—Peter Stephenson, technology editor

©2012 EMC Corporation. All rights reserved. EMC, RSA, the RSA logo and the RSA Conference logo are registered trademarks of EMC Corporation in the United States and/or other countries. All other marks are trademarks of their respective companies.

www.scmagazine.com • January 2012 • SC 37
Multifactor authentication

One cannot argue the value that this technology can deliver in validating an identity of someone wanting to access systems or applications, says Peter Stephenson.

Multifactor authentication is an all-encompassing grouping for products that provide a second- and/or third-factor method for validating a user’s identity. These products can include items such as tokens, certificates, biometric devices, one-time passwords, challenge-response solutions, mouse and keystroke pattern matching, and geolocation solutions. There are many sub-offerings in each of the above categories that we will discuss in more detail in our product reviews. The value that this technology can deliver in validating an identity of someone wanting to access systems or applications is clear. With an ever-growing list of government and private sector breaches, adding further levels of validation to confirm the basic credentials we all use in our jobs and personal lives should be a no-brainer. Today’s security risks employ sophisticated techniques that challenge even seasoned security professionals. What is worse is the growing “low-tech” targeting of our user base through simple social engineering and phishing attacks. The latter is what we wish to resolve through the validation of our users’ credentials via an additional source of information. For this month’s Group Test review, we tested multifactor authentication products. There were definitely some trends and a few surprises in the product sets, prompting us to do some additional research. One surprise in the products we examined was the limited participation of any true biometric offerings and even the lack of support for these devices. We all know simple name and password authentication methods are inherently insecure. Multifactor products offer a huge advantage in added security. That said, as passwords can be compromised, physical keys can be stolen. There is no such possibility in biometrics. Technicians analysts forecast the global biometrics technology market will reach $9.3 billion by 2014. We find that there is quite a bit of consolidation going on in this space. The standard fingerprint-and-hand geometry solutions are still there. We are seeing more and more work being done in the voice recognition space for the purposes of verifying identities and authenticating people. Another technology that came out of our research – that we did not have a chance to review, but is still worth mentioning – are the products that play in the continuous authentication space. These offerings attempt to address the risk of having a set of credentials comprised by revalidating the user beyond login. The tools we reviewed this month all supported multiple forms of second-factor authentication technologies. We did have a few that supported standard fingerprint readers and an authentication method. The solutions provided authentication against a user’s PC or directory, as well as offering additional authentication protection for various application, VPN and web-based services. One of the knocks against multifactor authentication solutions used to be the overhead involved in deploying in an enterprise environment. It was a pleasure to see that the products we reviewed really eliminated this as an issue. We were pleased with the availability of deployment capabilities, key management, recovery abilities, and management and alerting options.

Most of the offerings provided an easy means of deploying client software. There was also good support for user self-enrollment of tokens and self-reset for PIN and password issues, reducing the IT overhead associated with supporting these technologies. Pricing varied among the solutions, and it is important to understand the licensing as some are yearly renewals while others are one-time fees. Some of the offerings are also available in a SaaS model. As well, some products include token support, while others require separate purchasing. In any case, the price point of the solutions we reviewed really delivered a lot of protection for a very reasonable expense.

Mike Stephenson contributed to these reviews.

### Specifications for multifactor authentication tools

<table>
<thead>
<tr>
<th>Product</th>
<th>Centrally managed</th>
<th>Key recovery</th>
<th>AD/LDAP integration</th>
<th>Supports soft tokens</th>
<th>Supports hard tokens</th>
<th>Supports one-time passcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActivIdentity</td>
<td>☒</td>
<td>☐</td>
<td>☒</td>
<td>☒</td>
<td>☐</td>
<td>☒</td>
</tr>
<tr>
<td>CryptoCard</td>
<td>☐</td>
<td>☒</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Deepnet Security</td>
<td>☐</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>DigitalPersona</td>
<td>☐</td>
<td>☒</td>
<td>☒</td>
<td>☔</td>
<td>☔</td>
<td>☔</td>
</tr>
<tr>
<td>Entrust</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>PhoneFactor</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>SecureAuth</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Swivel Secure</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Vasco Data Security</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biometric device support</th>
<th>Application protection</th>
<th>PC protection</th>
<th>Audit/compliance reports</th>
<th>Alerting</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☐</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
</tbody>
</table>
**ActivIdentity 4TRESS**

**Authentication Appliance FT2011**

ActivIdentity 4TRESS Authentication Appliance FT2011 is a versatile server providing strong authentication to a wide range of services and online applications – such as virtual private networks (VPN), remote access, terminal services and web-based applications – through RADIUS, SAML v2-based authentication portal and web-service APIs. The tool is available as a hardware or virtual appliance. We evaluated the physical device.

We set up the tool using the terminal interface. We had to run a health check on the appliance and then perform the initial configuration to put it on our network. Once the network details are provided, one can browse to the secure web interface to perform the remaining configuration. At this point, we enabled the various components, such as the authentication server, portal, management console and token portal. We configured the various users for the interfaces/ports and let the setup complete. The process took about an hour. The appliance comes complete with an embedded Oracle database, and configuration of it is all done without any direct involvement. Once the product is loaded, one will need to note the various portals and communication ports for accessing various services. Anything needed can be accessed via the various appliance portals. It just takes some time to navigate back and forth among all the portals.

Centralized management is available through a set of web-based user interfaces. The 4TRESS Management Console is used for configuration, and day-to-day operations and administration. The Configurer Portal is used to modify and maintain low-level parameters, such as device and credential types, and authentication policies templates. The 4TRESS Authentication Portal is the SAML front-end portal that provides the logon interface for service provider authentication. The 4TRESS Soft Token Activation Portal allows end-users to securely and easily activate 4TRESS Soft Tokens. A nice feature of the various portals is that they can be rebranded and set up for multitenant hosted environments of organizations supporting multiple business units.

The appliance registers and remembers all machines the user has successfully authenticated. When a new machine is engaged, the user is required to logon with the username/password, and with an additional authentication lifecycle management for user credentials.

Another feature we liked was 4TRESS Fraud Detection, a cloud-based, device profiling, identification and risk-score technology. The centralized auditing is attractive. It is secure and contains all the data one would need for any compliance review. The documentation is also well done and helped us through the install and use of the appliance and client. Eight-hours-a-day/five-days-a-week support is available at 20 percent of list price, and 24/7 service is offered at 25 percent of list price.

The hardware appliance (with no hardware security module), including a one-year warranty, is $6,999. A user license for a midsize enterprise deployment is around $40, and for a midsize online banking deployment around $11. In both cases, volume discounts apply.

**Weaknesses**

- Pricey and a bit harder to use.

**OVERALL RATING**

- Value for money: ★★★★★
- Support: ★★★★★
- Performance: ★★★★★
- Ease of use: ★★★★★
- Features: ★★★★★
- Documentation: ★★★★★
- Support: ★★★★★
- Price: $6,999

**Strengths**

- Multitenant, fraud detection support.

**Verdict**

Good product for a large enterprise or SaaS service provider model.

---

**CryptoCard Blackshield Server v3.1**

The CryptoCard Blackshield Server v3.1 is designed as an authentication service delivery platform, automating all tasks around user and token management, provisioning, reporting and billing. The model we evaluated was the Service Provider Add-on, a version that allows for provisioning and/or on-boarding virtual servers to deliver a multitenant model, which means that a single instance can support multiple organizations or directories, each appearing to have their own enterprise server.

We kicked off the software load on our Windows server, and the process was fairly simple. The installer loads the software and a default PostgreSQL database. We then browsed to the localhost, a web-based interface, and used our Active Directory (AD) administrator credentials to login to the site. Through the web interface, we could import the license, configuring the connection to the database, and set up account information, self-enrollment policies and portal details. The documentation walked us through the process without issue. Once we completed the server setup, we installed the Blackshield Windows Logon client on one of our Windows test systems. (The client does require one to provide the path to the enterprise server, so that must be completed first.)

Users were added automatically through the lightweight directory access protocol (LDAP)/AD integration. Policy engines are easily configured to perform routine tasks, such as the automatic issuing of tokens, provisioning of users, revocations, and access control based on changes to a user’s security group memberships made in LDAP/AD. Tokens can be manually assigned and PINS issued, or there is the ability to bulk assign through LDAP/AD.

There is support for all cloud applications and services that support SAML 1.1 or 2.0. Additionally, there is support for virtual private network (VPN) and firewall devices supporting RADIUS, as well as vendor-specific applications, such as Outlook Web Access, Citrix, SharePoint, Salesforce.com, Google Apps and Microsoft Remote Web Workplace. New features in this version include support for SAML, support for MP-1 tokens on Android OS, SMS/one-time passwords via email, and additional token management reports.

There was standard/canned and customized reporting available. Alerting was also offered on both the dashboard and through email and text messaging. The management interface on the device is clean and is a good tool for viewing the enterprise at a glance and drilling down to user-level detail and management.

The documentation was helpful. We were even provided with welcome guides for various token types that might prove helpful in rolling out the various authentication components to a user base. Both eight-hours-a-day/five-days-a-week and 24/7 support options are available. Typical costs are 15 and 20 percent of server pricing for customers purchasing a license. Support is rolled into the monthly usage fee for clients adopting subscription licensing.

---

**RATINGS**

- Vendor: CryptoCard
- Price: $50/user (subscription includes support and tokens)
- Contact: cryptoCard.com
- Features: ★★★★★
- Ease of use: ★★★★★
- Performance: ★★★★★
- Documentation: ★★★★★
- Support: ★★★★★
- Value for money: ★★★★★

**OVERALL RATING**

- ★★★★★

**Strengths**

- Set up and deployed easily. Alerting was well done. Full device support.

**Weaknesses**

- Nothing worth noting.

**Verdict**

Good price point, nice standalone or multitenant platform, support for network- and cloud-based authentication.
Deepnet Security
DualShield v5.2

DualShield v5.2 from Deepnet Security is a unified authentication platform, using the versatile authentication server model. The tool protects the company against threats that protect data and control access to PCs and applications. There is support for virtual private networks (VPN), remote desktop protocol (RDP), email, web, cloud and mobile applications, including full SAML 2.0 support. The offering was delivered to us as server-based management and client applications, application-specific client deployments, and various one-time password (OTP) key fob and software-based tokens.

The installation package was intuitive. Once we launched the installer, it walked us through the deployment. We chose to load all the backend and frontend components, including the management console, and single sign-on (SSO), self-service and provisioning servers. One has the option to separate these in the environment for security and performance purposes, and deploying these modules on separate servers is recommended. We installed them all on the same server for our test. The installation took no more than five minutes, and we were ready to start. We applied the license keys and were off and running creating applications. The user interface was one of the better ones we’ve seen. We created a Windows authentication application and loaded the client on our test device. The client replaced the Windows graphical identification and authentication (GINA) with a Deepnet Security login that uses the Windows credentials along with the two-factor option.

DualShield supports a wide range of authentication methods, including on-demand password by SMS, email or mobile call (with support for most phone operating systems), and challenge-response, hardware and software OTP tokens, including RSA SecurID and Vasco Digipass Go. DualShield also supports static passwords, as well as question-and-answer voice and facial recognition, and keystroke dynamics (keystroke biometrics). TypeSense is a software-only authentication solution based on typeprint recognition that accurately identifies a user by the way they type characters across a keyboard. The installation of any new hardware is not required for TypeSense, as it works with a standard computer keyboard. Another feature, VoiceSense, is a text-and-language, independent biometric speaker verification system. And, FaceSense is a state-of-the-art authentication solution based on facial recognition technology that verifies a speaker’s identity in real time using a simple spoken phrase.

Other features to note: OTP passwords are also supported through Twitter Direct Message. The user has a central location to administer and manage all tokens. DualShield offers native Active Directory (AD)/lightweight directory access protocol (LDAP), email, web, cloud and mobile applications, including full SAML 2.0 support. The offering was delivered to us as server-based management and client applications, application-specific client deployments, and various one-time password (OTP) key fob and software-based tokens.

Support is available for 20 and 30 percent of list price. Documentation is comprehensive, but some areas need updating. Overall, we were really pleased with the quality, ruggedness and size of the U.are.U 4500 Fingerprint Reader that we tested. This offering also delivered a wide range of support for biometric devices, such as the company’s own branded Fingerprint Reader, as well as third-party devices and face recognition support for cameras built into HP notebooks. We were really pleased with the quality, ruggedness and size of the U.are.U 4500 Fingerprint Reader that we tested.

A knowledge base and eight-hours-a-day/five-days-a-week support is included with the subscription service. Additional options are available for fees of 15 and 20 percent of list price.

This product takes a unique approach. It wasn’t unwieldy to load and configure, even though the documentation was not as detailed as it could have been. Once it was loaded, however, the ability to have server admins manage and maintain a full featured enterprise solution like this, without requiring any new training, is a great idea. We have to admit, we are so used to purpose-built user interfaces for everything we do that it did take us a few minutes to get used to the idea of managing an application that delivers as much capability as this product does through the same interface we already employ for managing users.

DigitalPersona
Pro Enterprise v5.2

DigitalPersona Pro Enterprise v5.2 is a centrally managed suite of solutions – access management, data protection and secure communications that protect data and control access to PCs and applications. It provides a suite of security applications integrated into a multichannel authentication infrastructure that can be managed from the cloud or Active Directory (AD). It allows companies to control and enforce multiple security applications through a single control panel, and provides strong authentication, single sign-on, secure virtual private network (VPN) access, full-disk encryption, access recovery and secure email and documents. For our review, we focused on the multifactor authentication components.

The solution was delivered to us as a software offering. We loaded it on our Windows test server. The process required us to load several applications before installing the server component. Once we ran the server app, it extended the AD schema and created a “Defender” container and tab in our “Users and Computers Manager.” This approach was interesting as there was no special web-based GUI needed to manage the offering, it was all done through standard AD tools with the extensions. We licensed the product, imported a token and created policies. Because it was similar to working with standard AD menus, we got through all the implementation and setup, though the documentation was a bit lacking. The client side does have an attractive administrative console that can be used for local configuration and administration. If one wishes, that feature can be removed via a group policy object (GPO). There are additional password manager and privacy applications that can be loaded on the client as well. All the server side management and configuration was done through the Group Policy Management Editor.

There is support for a full suite of token types, including OATH-compliant soft and hard tokens, one-time passwords, PINs, or smart or proximity cards. This offering also delivered a wide range of support for biometric devices, such as the company’s own branded Fingerprint Reader, as well as third-party devices and face recognition support for cameras built into HP notebooks. We were really pleased with the quality, ruggedness and size of the U.are.U 4500 Fingerprint Reader that we tested. A knowledge base and eight-hours-a-day/five-days-a-week support is included with the subscription service. Additional options are available for fees of 15 and 20 percent of list price.

This product takes a unique approach. It wasn’t unwieldy to load and configure, even though the documentation was not as detailed as it could have been. Once it was loaded, however, the ability to have server admins manage and maintain a full featured enterprise solution like this, without requiring any new training, is a great idea. We have to admit, we are so used to purpose-built user interfaces for everything we do that it did take us a few minutes to get used to the idea of managing an application that delivers as much capability as this product does through the same interface we already employ for managing users.
## PhoneFactor

PhoneFactor provides the addition of second-factor authentication using something everyone has. This product uses a phone as a token. With this solution, users can enlist their phone to provide a second factor of authentication through a call, text message or even voice recognition. This also provides full, out of band security and can be used both inside and outside of the enterprise. For inside the organization, PhoneFactor can be used to authenticate to custom-sensitive applications, as well as many already existing applications, using RADIUS, Microsoft IIS and Windows-based authentication. For outside, it can be used to integrate with web-based applications, such as online banking and other account management applications for customers. This provides strong authentication at no extra cost to the user.

This tool consists of two major components: The first is the PhoneFactor service. This is hosted by the company in a data center. The second part is the agent. This is installed on the customer site – or as part of the customer’s cloud – and is used as a way to integrate PhoneFactor with applications and user accounts. Once the agent is deployed, it can synchronize with Microsoft Active Directory or LDAP (lightweight directory access protocol), which makes integration into an existing environment quite seamless. There is also a full, web-based portal available as an optional third component. Users can access this portal for self-enrollment and other account management tasks.

From an administration standpoint, this solution offers not only several integration options, but we found it easy to use and manage. While it did take a little bit of experimenting on our part, we found that this product can be quite powerful and can plug into almost any application. The agent itself does not require a high amount of system resources, so it can be deployed easily on almost any available server in the enterprise.

Documentation included implementation and quick-start guides. The quick-start guide provided all the steps to get the agent installed, as well as some brief instructions for configuring the applications to be secured with the product. The implementation guide provides a much more in-depth look at how to integrate and manage the product. PhoneFactor provides customers with standard and extended editions of gold level support as part of the license cost. Gold level support includes 8 a.m. - 6 p.m. phone and email technical support. Customers can purchase platinum level assistance – which includes 24/7 availability – at an extra 10 percent cost of the license. We found minimal help via the website, other than a FAQ section and a few technical resources.

At a price ranging from $10 to $25 per user, we find this to be a good value for the money. PhoneFactor provides solid integration features that are easy to deploy to users through their own phones.

## Entrust IdentityGuard

IdentityGuard from Entrust offers a plethora of multifactor authentication methods that can be used throughout the enterprise, as well as for customer-facing web applications, such as online banking and web-based account management. This product uses three types of authentication that can be combined and mixed and matched for solid multifactor authentication. Methods include the use of tangible devices, such as one-time password tokens, grid cards and digital certificates; knowledge-based authentication, including personal identification numbers; and transparent authentication, which includes IP geolocation and device-based authentication.

Deployment is quite straightforward, but there are several components to be installed and configured. The first module that needs to be loaded is the server itself. The IdentityGuard server can be installed on either a Windows or Linux machine, and the server includes all the necessary components for the server services, as well as the web-based components for management. IdentityGuard also relies on a backend database, which can be either Microsoft SQL Server or PostgreSQL. Once the database is configured and the server is installed, other modules can be employed. These include enrollment, user self-service and a mobile device.

We found overall deployment and management to be easy and intuitive. Management can be done either from a web-based management or application interface. We found both to be equally complete, as well as easy to navigate with intuitive controls. We also found this product to be quite configurable with many integration options. Administrators can use many combinations of factors that allow for stronger authentication to sensitive systems, as well as physical access to rooms or buildings. On the user side, we found the authentication methods to be well integrated and easy to understand.

Documentation is well-organized and includes several PDF manuals for the various components. Each major asset has an installation guide, as well as a user or administrator guide. We found all documentation to not only be well-organized and easy to decipher, but also to include many step-by-step instructions, screen shots, configuration examples and diagrams.

Entrust offers three support programs to customers. These are priced at $8 per user and dropping down to $3 per large volume of users, we find this to be an excellent value for the money. Entrust IdentityGuard provides not only many authentication options for users, but also flexible deployment and easy management.

---

### Ratings

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Price</th>
<th>Features</th>
<th>Ease of use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Value for money</th>
<th>OVERALL RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entrust</td>
<td>$6+ per user</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

### Strengths

Many authentication methods with highly configurable controls.

### Weaknesses

None that we found.

### Verdict

A solid product with a strong pedigree, good pricing and a lot of features. We make IdentityGuard our Best Buy.

---

### Ratings

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Price</th>
<th>Features</th>
<th>Ease of use</th>
<th>Performance</th>
<th>Documentation</th>
<th>Support</th>
<th>Value for money</th>
<th>OVERALL RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhoneFactor</td>
<td>$10 - $25 per user</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

### Strengths

Leverages a user’s phone for strong authentication.

### Weaknesses

Slightly difficult to configure

### Verdict

A novel approach to authentication that is easy to deploy and has a good feature set.
SecureAuth Identity Enforcement Platform (IEP)

The SecureAuth Identity Enforcement Platform, or IEP, is a full featured multifactor authentication appliance. This product leverages an already existing Microsoft Active Directory or LDAP (lightweight directory access protocol) structure to add multifactor authentication to a host of services and applications. IEP uses its Versatile Authentication Solution (VAS) service to integrate single sign-on and identity management services for cloud-based, web-based, virtual private network (VPN), and mobile resources. This product can easily add strong authentication to the enterprise using a combination of certificates; one-time passwords that can be delivered via SMS text, by phone or by email; and personal identification numbers.

This solution can be deployed in several ways. Customers can choose from a physical, virtual or a cloud-based appliance. For our evaluation, we looked at the physical appliance, and we found deployment to be quite straightforward. The device comes preloaded with a copy of Windows Server and all the software needed. After a short setup process, the appliance is up and running. All management can be done on the appliance itself through a shortcut or through the web-based management console. We found this to be easy to navigate thanks to its intuitive and organized layout.

From the user side, this product provides seamless integration with applications. After the administrator has set up a policy, a user can login to a web-based user page, which contains all the various accounts for that user. This page can include web application logins, such as web-based email and SharePoint accounts, as well as SaaS applications, such as online storage accounts. Users can employ this portal to manage their account and reset their password.

Documentation that came with this product included several integration guides, as well as appliance setup guides. The appliance setup guides provided the steps necessary to get the device connected to the network. We found these guides to be clear and concise, but found they lacked depth and screen shots. The integration guides are provided on a documentation portal, and we found them to be well-organized with clear step-by-step instructions and many screen shots and examples. Overall, we found the documentation to be sufficient and easy to understand.

SecureAuth provides phone and email technical support from 6 a.m.-5:30 p.m. PST, Monday through Friday, to all customers as part of the ongoing license cost. Also included is 24/7 support for mission-critical issues. Customers also can access an online portal that provides service status and notices, as well as some useful help tools. Technical documentation also can be found online. However, there is no knowledge base included in the portal.

At prices starting at $2,000 per appliance for the appliance, plus $10 per user per year, this product can be quite costly. With that being said, we find the SecureAuth appliance to be quite feature rich and easy to manage with some very nice integration functionality all combining to be a reasonable value for the money.

Swivel Secure PINsafe

The PINsafe from Swivel Secure takes a user’s fixed personal identification number and randomly generates a one-time login code that is sent to the user to enter as part of a second factor for authentication. This code can be delivered to the user through multiple paths, including a mobile application, text message, voice call or web application. When the user receives their code, they enter that along with their password and are able to login to the specified resource. PINsafe can integrate with a multitude of applications and services, including secure sockets layer virtual private network (SSL VPN), remote access and web platforms, and many cloud services.

This solution can be deployed as a physical or virtual appliance, or as a software-only installation. For our evaluation, we looked at the physical appliance. We found PINsafe to be of average difficulty to install and configure. Much of the management of the tool is done through a web-based management console known as Welmin. We found this tool to be fairly easy to navigate with an intuitive design, but it did take a little bit of getting accustomed to. Integration is a big strong point with this offering. It can be configured to integrate with the already existing Microsoft Active Directory infrastructure for user management, and then further integrate with already existing platforms throughout the enterprise, including SonicWALL, Cisco, Check Point and Citrix SSL VPNs; Microsoft services, including Terminal Services, Exchange and Outlook Web App (OWA) and SharePoint; and many cloud-based services, such as Google applications and Salesforce.com.

From the user standpoint, this product is seamlessly integrated into the applications themselves. In most cases, the user will notice an extra field that has been added to the login page for their one-time code. There is nothing for them to install, and they encounter no real difficult authentication processes. Users can get their one-time code from a variety of sources, including from the obvious text to their mobile phone, voice phone call, and a web application to the not-so-common dedicated application available across multiple mobile phone platforms.

Documentation included a single-page quick-start, a short console user, a console management interface, and several other configuration-specific mini-guides available online. We found all documentation to be easy to understand. Many included screen shots, configuration examples and step-by-step instructions. Also provided was a full reference manual that included many in-depth configuration instructions and procedures.

Swivel Secure provides customers with free unlimited access to a knowledge base and a few other online resources. Customers also can purchase standard, eight-hours-a-day/five-days-a week or full 24/7 phone and email technical support at 8 percent and 40 percent of the license cost, respectively.

With an appliance price of $4,000, plus an additional $1.41 to $110 per user (based on volume), this appliance can become quite pricey for some environments. However, we find it to be a reasonable value for the money based on its solid integration functions and seamless ease of use to licensees.
Vasco Data Security Digipass
Go 7 and Identikey Server

The Digipass Go 7 and Identikey Server from Vasco Data Security work together to provide strong multifactor authentication throughout the enterprise. Digipass is used in tandem with a personal identification number that is configured on the server side to provide multifactor authentication. Digipass itself offers easy, one-button touch functionality to provide a one-time passcode that is entered along with the user’s PIN to authenticate to a number of different programs, including web-based bank applications and various virtual private networks (VPNs), such as those from Cisco, SonicWall and Check Point.

The heart of the system is the Identikey Server, which can be installed on a Microsoft Windows or Linux system in the enterprise. We found the initial installation to be quite easy and straightforward. The deployment of the Identikey server is done by running an installer package, which launches an easy-to-follow wizard. This installs the server, as well as the necessary components, such as the backend database. The wizard also goes through quite a few preconfiguration tasks that, at completion, will put a base configuration in place on the server. Once the installation is done, all management can be performed through the web-based management interface. We found this to have an organized layout with an intuitive navigation structure.

Overall, the server is easy to configure as well, and we also found it easy to plug right into our existing Active Directory environment. With the help of a solid software development kit (SDK), the server offers a lot of flexibility for integration. Administrators and programmers can use this SDK to integrate Digipass strong authentication into almost any web-based application, including custom ones. On the user side, this product integrates quite well into applications. Users also can access a self-management web portal. They can use this portal to easily register for a Digipass token, assign a token to themselves, synchronize static passwords, and run a login test.

Documentation includes PDF-based server manuals. These include getting-started, administrator reference and installation guides, and a few other supplemental manuals. We found all the guides to be well-organized with many screen shots and step-by-step instructions. Vasco offers a wide range of plans for software and server support. Customers can choose from standard technical assistance, which is available during business hours, as well as 24/7 full-support services. Vasco also offers the option for pay per incident and remote assistance. Plans range from seven percent up to a whopping 27 percent of the software cost depending on the type of help purchased. Customers also get no-cost access to a full knowledge base and other online resources.

At a cost starting at around $3,800 for the server license, plus around $4 to $22 per device depending on volume, this offering can result in quite the price tag. However, we find it to be a good value for the money based on its highly flexible ability to be customized to easily meet the needs of even home-grown web apps.

NAC, juiced up

The appliance is about the size of a three-inch thick iPad. But inside the NetClarity NACWall Nano is more than enough power for a full 1U rack-mounted piece of hardware. This is NAC on steroids, sized and priced for small and midsize businesses (SMBs). We connected the network, hooked up a screen and keyboard, and plugged the tool into the wall. We then pushed the blue power button and within seconds got a message on the screen that it was ready to configure. There are 13 steps to this process, according to the excellent quick-start manual, and the last one is, “Congratulations! You have completed the initial operational deployment.”

This little powerhouse sports a lot of useful NAC-ish features: auditing, malware detection, VLAN support, Active Directory integration, smart switch integration and vulnerability management, just to name some of the big ones. Of course, it offers the usual device authentication, as well as machine tracking, so that rogue devices are kept off of the network, and we’re notified if non-compliant devices are found, or they are simply blocked.

Once we had the box up and running – 12 steps really – we adjusted its clock, switched from our DHCP addressing to a static address (and back; just to see if we could), discovered all of the devices on our network, and updated the service pack, anti-malware software and CVE tests. Now, it will update itself about every three to five hours – as long as it is connected to the internet.

We were impressed with its ease of use. Network asset discovery, for example, was a one-click effort. We did change the subnet mask, but that was because we wanted to see if it would try to find what wasn’t there (our test network is only a class C). It didn’t. The Nano is capable of sending alerts just about anywhere one wants. We chose email, and that worked fine. The other thing it can do is fit nicely into a distributed NACWall environment. A NACWall Enterprise device – bigger than the cigar-box-size Nano – can manage a whole group of Nanos. So, that means that even though the first reaction is that the Nano is for SMBs, it also is ideal for branch offices.

The Nano is managed via a web interface – using the protected https://, of course – and it routinely calls back to the mothership for updates. This device is about as easy to administer as it gets. It is just the ticket for the level of business for which it is intended. SMBs and branch offices can manage this tool with limited resources.

The desktop and administration menus are simple, straightforward, comprehensive and clean. There is absolutely no clutter in the menus, screens or logs. Audits are straightforward and build on the years of experience that this device demonstrates as its legacy. A big piece of that legacy is its agentless deployment. For large enterprises with many branches, that is a big plus.

Pricing starts at less than $1,500 and the tool comes in two sizes. We like this product – we have enjoyed its larger siblings for years – and it is clear that this device has a solid place in today’s enterprises, large and small.

— Peter Stephenson
Revolution is in the air

It’s time to rethink the basic approach to protecting our businesses, says Cisco CSO John Stewart.

S ecurity professionals continue their efforts to protect IT infrastructure from those who would disrupt society and business, steal information or do harm. Across our industry, there is a rallying call for revolution – one that re-examines our existing practices and behaviors to course-correct and lead the way to a more assured future.

Our world is quickly evolving, and electrifying new technologies are eating the way. Today, we don’t use technology, we rely on it. Whole societies are running on the technological advancements that continue to change our way of life for the better, yet this progress also creates new challenges. Security professionals have to be persistently more creative, agile and responsive just to keep pace.

While we have moved the needle on improving information security, there is still a ways to go. Albert Einstein defined insanity as “doing the same thing over and over again, and expecting different results.” So why do we continue to rely on traditional practices, such as patching and anti-virus, to protect our critical assets when the rate of technological evolution has rendered these approaches virtually ineffectual?

We have built complexity into our IT systems and have relied on common practices for far too long. The complexities we face are vast and asymmetrical. It’s expensive to do everything we need to protect our assets, yet still far too easy for a miscreant to do harm.

We’re in an unfair fight. To level the playing field, we need to challenge traditional thinking around security and make the penalties for hacking more punitive. In fact, it’s time to rise up, get fighting mad and force an insurgency that will bring revolutionary change to how we protect our information assets.

Let’s get back to basics. Do less… and do it well. Create simple goals and strategies to keep the bad things out while protecting the most critical assets. Gauge for detection to understand what is truly occurring in the infrastructure, and then analyze and validate the data frequently to measure effectiveness. Most importantly, stop building systems and adding security on later. Instead, architect them with security embedded from design to operation.

Don’t do it alone. Apply an “eye-in-the-sky” approach that provides global visibility into the overall condition of the IT infrastructure and threat, and more effectively helps to protect the things that need to be protected. Prepare a contingency plan for when something goes wrong, and then work hard to make sure it doesn’t.

Human curiosity can’t be ignored. Links and attachments want to be clicked, and all the security controls in the world can’t stop ignorant, imaginative and/or malicious users from hurting themselves or the organization. Most employees are unknowledgeable, inexperienced and ill-equipped to contend with increasingly dynamic, risk-prone and open operating environments. And most don’t have a clue about technology security, and don’t want to know. We must boldly educate users about the importance of their role in protecting the organization and themselves. We must also encourage their participation and hold them accountable.

Help is available if we know where to turn and what to ask. Reach out to local law enforcement and international protection agencies, which can help understand, manage and mitigate risk. Find ways to illuminate the problems and ideas publically. Share ideas that work and know where to get answers from others, as, ironically, we’re all facing similar challenges.

Remember: No matter how much you think you know right now, “tomorrow” will surprise you, so be prepared. Your call to action: Join the revolution and help us all move to a more secure future.

John Stewart is vice president, chief security officer at Cisco.

Most [employees] don’t have a clue about... security, and don’t want to know.”

LastWord
World's No. 1
Antivirus and Internet Security

ESET leads the industry in the consecutive number of “VB100” awards from Virus Bulletin testing organization.

Virus Bulletin Awards  Success ratio (%)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>25</th>
<th>50</th>
<th>75</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESET</td>
<td></td>
<td></td>
<td></td>
<td><strong>97</strong></td>
</tr>
<tr>
<td>Symantec</td>
<td></td>
<td></td>
<td></td>
<td>91</td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td></td>
<td></td>
<td>93</td>
</tr>
<tr>
<td>Sophos</td>
<td></td>
<td></td>
<td></td>
<td>79</td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td></td>
<td></td>
<td>76</td>
</tr>
<tr>
<td>GDATA</td>
<td></td>
<td></td>
<td></td>
<td>73</td>
</tr>
<tr>
<td>McAfee</td>
<td></td>
<td></td>
<td></td>
<td>68</td>
</tr>
<tr>
<td>TrendMicro</td>
<td></td>
<td></td>
<td></td>
<td>67</td>
</tr>
</tbody>
</table>

Selected Antivirus Vendors (not a complete list)

And the best keeps getting better—
IT experts everywhere agree.