

Security Trends Report

10/19/07

Can you spot a phish? Play Carnegie Mellon's game and see

Test your knowledge and learn how to tell the URL of a fraudulent site from a legitimate one
Network World staff

September 28, 2007 ([Network World](#)) -- Scientists at [Carnegie Mellon University](#) have developed an online game designed to teach Internet users about the dangers of phishing.

Featuring a cartoon fish named Phil, the game, called Anti-Phishing Phil, has been tested in CMU's Privacy and Security Laboratory. Officials with the lab say users who spent 15 minutes playing the interactive, online game were better able to discern fraudulent Web sites than those who simply read tutorials about the threat.

The game focuses on teaching Internet users how to tell the URL of a fraudulent site from a legitimate one, officials say. It offers tips such as examining URLs for misspellings of popular sites, dissecting a Web address to understand where it's pointing to and using [Google](#) to validate a URL against search results. (This reporter played the game, scoring 8 out of 8 in the first round, 6 out of 8 in the second round and not enough correct answers in the third round to move up.)

The lab has now decided to open up the game for broader testing. Visitors to the [site](#) http://cups.cs.cmu.edu/antiphishing_phil/ who click on "play the game" are given a short quiz, play the game and then take another quiz, officials said. Visitors who submit their e-mail addresses and take a follow-up quiz the next week are entered in a raffle to win a \$100 [Amazon.com](#) gift card.

The game was developed to help raise awareness about phishing attacks, in which spam e-mails that appear to come from a legitimate bank or retail organization try to lure the recipient into entering personal or financial information into a fraudulent Web site, where it can be stolen and used in identity theft.

Users run the risk of falling prey to a phishing attack more than viruses and other malware because these scams rely on social engineering and can't be protected against by technology, according to professors at the lab.

While security experts argue the effectiveness in educating users to be aware of phishing scams, Steve Sheng, the Ph.D. student who developed Anti-Phishing Phil, this summer presented results of a study showing that training improved Internet users' ability to tell a legitimate Web site from a fraudulent one. According to Sheng's research, users in the study improved their accuracy in spotting fake sites from 69% before playing the game to 87% after.

This project is part of a larger CMU antiphishing research initiative funded by the [National Science Foundation](#) and the Army Research Office.

Sep 10, 2007

Criminals Operating Malware Supermarkets

The global market for criminal malware now operates like a supermarket, complete with special offers and volume discounts, a security company has discovered.

According to Panda Software's, latest quarterly report the going rate for a reasonably sophisticated but generic Trojan is between \$175 (US\$350) and \$350, while the email list with which to target victims for the program costs from \$50 per million names. The malware writers even offer specials -- in one case the company discovered a site selling a 'payment capture' Trojan for \$200 to the first 100 customers to sign up, a saving of \$50 off the normal rate.

The company is shy of giving more details of the sites from which such offers were being made, but was willing to say that it considered Russia -- an area with poor anti-malware legislation -- as a prime location for the malware industry.

"In recent months we have witnessed the growing professionalization of digital crime," said Panda Software's lab chief Luis Corrons. "The first step for cyber-crooks was when they started looking for profits from their activity instead of just notoriety. Now they are creating a vast online malware market, where there are even specialized segments. New business models are appearing, as we speak", he said.

According to Corrons, the malware industry now appears to be turning from being just a shop from which malware can be bought, to one where services are offered. For between one and five dollars per executable, malware could be cloaked -- encrypted -- against the anti-virus software programs it was likely to encounter on a for-hire basis. Finally, criminals could rent spam servers for \$250 a time to distribute their assembled malware package, the company said.

Corrons also provides details of the cost of hiring DDoS attacks in his blog.

"This malware market is completely online. All types of creations and crimeware tools can be bought in hundreds of forums. Even though most web pages have been located in Eastern European countries, mafias extend their networks worldwide, he said.

"Although it may look difficult to find web pages where these tools are sold, it is not. All you have to do is search in browsers for forums where hacking services are rented or where Trojans are sold."

If using malware to attack users is so lucrative, why do some criminals choose to sell their expertise rather than exploit the programs themselves? This is a harder question to answer, but could have something to do with risk. Better a low-risk, lower return that is guaranteed than a high-risk, high-return one that is not.

By John E. Dunn, Techworld.com

"Security Breach Severity Worsens, Study Finds" Network World (09/18/07) ; Dubie, Denise

Although the number of reported security breaches has declined, the average severity of breaches has doubled, concludes a new Computing Technology Industry Association study. CompTIA compiled responses from over 1,000 IT professionals, evaluating areas ranging from IT security to IT budgets, training, and costs of breaches. Thirty-four percent of those polled said they experienced a major security breach in 2006, down from 38 percent in 2005, but the average severity of breaches in 2006 ranked a 4.8 on a 1 to 10 scale, up from 2.3 and 2.6 in previous years. Meanwhile, security consumed 20 percent of IT budgets in 2006, up from 15 percent in 2005 and 12 percent in 2004, while the number of organizations designating at least a part of their budgets to training or certification last year also increased to 68 percent, up from 55 percent in 2005. Forty-two percent of respondents attributed human error to breaches, while almost half credited viruses and worms with facilitating breaches. Authorized-users abuse and lack of user awareness were also cited by those polled, and 55 percent of respondents said spyware was a major security threat. The number of organizations that have established IT security policies has increased compared with prior years, while 81 percent of IT professionals said they had security-specific policies in place.

"Data Explosion Shakes Up IT" IDG News Service (09/13/07) ; Kirk, Jeremy

Dubbed the "information explosion" by IT managers, the exponential increase of devices and systems means companies will have to develop strategies for saving and securing data, locating information, and adhering to regulations, predicts IDC's Stephen Minton. Though the majority of such data will stem from consumer activities, such as sending email and surfing online, roughly 60 percent of that data will still be conveyed across corporate networks. Such data is primarily unstructured, and companies are far from having the capacity to study the unstructured data crossing their networks, says Minton. However, technologies are surfacing that can analyze unstructured data to help businesses enhance their operations by determining what is important to consumers. Such business opportunities represent the information explosion's positive side, but security concerns and compliance anxieties represent the negative. In 2005, the number of software vulnerabilities reported swelled to a record high of approximately 6,000 vulnerabilities, according to the U.S. Computer Emergency Response Team. Minton attributes the rise in vulnerabilities to the proliferation of applications and devices. As a result, IT departments now directly influence a company's bottom line, for insecure and unreliable systems put a company's reputation at risk. Indeed, a 2007 IDC survey found that 60 percent of businesses now rank security as their top budget priority.

2007 CSI Computer Crime and Security Survey Shows Average Cyber-Losses Jumping After Five-Year Decline" PR Newswire (09/14/07)

The average annual loss reported by U.S. companies in the Computer Security Institute's 2007 Computer Crime and Security Survey more than doubled, jumping from \$168,000 in 2006 to \$350,424 this year. Financial fraud topped the list of losses, followed by losses attributed to viruses and system penetration by outsiders. Close to one fifth of those polled reported that their losses resulted from targeted attacks, while 46 percent reported incidences of security attacks. Employees' access to the Internet that resulted in virus vulnerabilities, such as email or pirated software, also accounted for a substantial amount of security threats. Survey author and CSI director Robert Richardson says the data supports the fact that cyber threats "are beginning to materialize as mounting losses."

"Assessing and Protecting Your Corporate Network" eWeek (09/11/07) ; Prince, Brian

In order to establish a strong data security framework organizations must first understand what data they care most about, says RSA's Christopher Parkerson. Parkerson says that organizations must then find out where this data resides, determine what policies are needed to protect it, and implement effective enterprise-wide controls for consistent enforcement. But in order to effectively implement proper controls, organizations must first develop a well-executed data identification and classification process--something that many fail to do. According to a recent survey by Forrester Research, 37 percent of organizations admitted to not having a data classification policy. In addition to these steps, security professionals say organizations should establish metrics to measure the effectiveness of their security tools, policies, and procedures. IT security professionals beginning a job at a new company should start by looking at any previous security audits and talking to the heads of the company's business units to see what their policies and concerns are. Overall, organizations should take a holistic approach to security and view technology as just one part. This holistic approach should include education and technology, as well as IT security policies that align with business security policies, says Forrester Research analyst Khalid Kark.

--OMB, NIST, NSA, DoD Formalize Single Federal Desktop Configuration For Agencies Using Windows (21 September)

To formalize the methods to be used in implementing US government policy on buying "security baked in" more than 700 federal executives and business executives gathered at NIST to hear how to make it work. White House Cyber Czar Karen Evans, NSA's Vulnerability Chief Tony Sager, Gartner's Security VP John Pescatore, NIST ITL Director Cita Furlani, Office of the Director of National Intelligence's Security Chief Sherrill Nicely and DoD's top cyber strategist Michelle Iverson, Microsoft's Chase Carpenter and more than 15 commercial tools vendors provided guidance, tools, demonstrations of effectiveness of the new FDCC (Federal Desktop Core Configuration) and S-CAP (Security Content Automation Process) initiatives.

http://www.gcn.com/online/vol1_no1/45074-1.html Where to find complete documentation: [Editor's Note (Paller): Commercial companies like Apple, Intel, CA and HP are also supporting or architecting support into upcoming products (through their systems management platforms) the new S-CAP standard for automating vulnerability discovery and correction.

Every large security company is building in S-CAP compliance (though a few are exaggerating when they say they already have it). Several Fortune 100 companies (and one Asian and two European governments) are finalizing strategies for taking advantage of the rapid patching and massive cost savings enabled by the FDCC. FDCC and SCAP are the best examples to date of the US government leading by example and large organizations are taking note.]

--Connecticut State To Sue Accenture Over Tape With State Data Stolen From Consulting Firm (September 19 & 20, 2007)
The state of Connecticut plans to file a civil complaint against the company it says is responsible for the presence of state agency bank account data on a backup tape stolen in Ohio earlier this year. Connecticut Attorney General Richard Blumenthal said that Accenture Ltd. treated the data "like scrap paper." Accenture has contracted with the state of Connecticut since 2002 to automate the state's human resources and financial data. Apparently an Accenture employee took a tape with Connecticut data on it to Ohio, where the company was helping to set up a similar system. The lawsuit alleges illegal negligence, unauthorized use of state property and breach of contract.

<http://www.bizjournals.com/masshightech/stories/2007/09/17/daily30.html?t=printable>

<http://www.stamfordadvocate.com/news/local/state/hc-19174003.apds.m0122.bc-ct--datasep19.0.4112604.story?coll=hc-headlines-local-wire>

<http://www.informationweek.com/shared/printableArticle.ihtml?articleID=201807932>

"Federal CISOs Seek Security Standards to Prevent Data Breaches" Network World (09/18/07) ; Greene, Tim

The government's efforts to encourage telecommuting among federal employees have not been very successful, in part because of a lack of mobile endpoint security standards. Such standards would govern the security of laptops, which is a primary concern for most federal CISOs. Currently, there is no formal certification of mobile devices to reassure CISOs that the laptops they issue fulfill the mandates of the Federal Information Security Management Act. According to some federal CISOs, the nearest thing to certification is the set of guidelines from the National Institute of Standards and

Technology. NIST suggestions include basics such as using antivirus software, conducting scans for spyware, and developing strict personal firewall rules. NIST also promotes the encryption of laptop data and the capacity to lock down lost or stolen laptops remotely. NIST's advice for securing mobile devices also includes maintaining activity logs, rigorous authentication, and double-wrapping laptops in personal firewalls. CISOs realize that the willingness to telecommute may be hampered by strict security measures, as well as by FISMA-mandated security training for telecommuters. Disaster recovery remains the government's key impetus for promoting telecommuting, and possible disaster scenarios will force CISOs to address new security concerns, such as securely permitting employees onto sensitive servers previously barred from use by telecommuters, says Commerce Department CISO Michael Castagna.

TJX offers settlement deal in wake of massive data breach

It's also offering credit monitoring and a three-day customer appreciation event Jaikumar Vijaya

September 24, 2007 ([Computerworld](#)) -- [The TJX Companies Inc.](#) is offering three years of credit-monitoring services along with identity theft insurance coverage to all consumers whose driver's license or other personal data may have been compromised by the massive data breach disclosed earlier this year by the retail company.

Consumers who had to replace their driver's licenses because of the compromise will also be reimbursed for the actual replacement costs under a proposed consumer class-action settlement announced by the company on Friday.

In addition, individuals whose driver's license or other ID numbers were the same as their Social Security numbers will be reimbursed for "certain losses from identity theft," the company said. Customers who had to change bank and credit card information because of the breach will receive vouchers redeemable in TJX stores in the U.S., Canada and Puerto Rico. As part of its settlement action, sometime next year TJX will hold a one-time, three-day customer appreciation event at which it will offer a 15% discount on all goods.

The settlement is not yet final and is subject to court approval. It is also contingent on an independent evaluation of the information security enhancements implemented by the company in the wake of the breach. TJX did not say how much the proposed settlement would cost. But it noted that [the estimated costs](#) were part of its previously announced fiscal 2008 second-quarter charge of \$118 million and fiscal 2009 noncash costs of \$21 million.

The proposed settlement, which covers all class actions in the U.S., Canada and Puerto Rico, "addresses the different ways customers have told us they have been impacted by the intrusion(s)," TJX CEO Carol Meyrowitz said in a statement. "Importantly, we truly appreciate our customers' continued patronage. TJX has been working diligently to reach a settlement that offers a good resolution for our customers."

The company's statement is available as an "important customer alert" on the [main TJX Web page](#).

TJX is the owner of a number of retail brands, including T.J. Maxx, Marshalls and Bob's Stores. In January, the company announced that someone had illegally accessed one of its payment systems and made off with card data belonging to an unspecified number of customers in the U.S., Canada, Puerto Rico and potentially the U.K. and Ireland. Later, it revealed that the number of cards compromised in the break-in was 45 million, making it the biggest compromise of personal data ever reported.

The proposed settlement is likely to satisfy consumers, who for the most part appear to have been less concerned about the breach than the media has been, said [Khalid Kark](#), an analyst at [Forrester Research Inc.](#) in Cambridge, Mass.

"I think [TJX has] gotten off cheaply" so far, Kark said, noting that neither the company's stock price nor its sales have been affected by the breach. "My overall sense is that people aren't really [as] concerned with these breaches as the media is. It seems like the reaction of the public is, 'It's not such a big deal.' So people may be OK with this settlement."

Kark had earlier this year estimated that costs to TJX from the breach over the next few years could amount to \$1 billion. However, so far TJX's own disclosures have pegged breach-related costs at a much lower \$150 million.

Security experts pitch 'culture of data'

The key to keeping a happy network: Live in your users' reality

Matt Hines

September 26, 2007 ([InfoWorld](#)) -- The companies that are having the most success in advancing their data security efforts today are those that are finding a way to protect sensitive information without getting in the way of business users, industry experts maintain.

In crafting their data-handling policies and selecting from the multitude of security technologies at their fingertips, those businesses that can foster both ready access to information, along with strong defenses for end-users and IT systems, are making progress the fastest, claim leading vendors and service providers.

After years of "throwing technologies" at the data security problem while juggling complex business demands along with external threats and regulatory compliance audits, some businesses are finally discovering that they can simplify the entire process by taking a more comprehensive approach to tailoring their programs to the manner in which their users access, handle, and share information.

Even within IT giants like [IBM](#), the struggle to balance security issues with emerging business demands to work with information in new ways hasn't always been approached in this manner, said Julie Donahue, vice president of the security and privacy service in the company's Global Technology Services group.

Only through experience and ongoing efforts to constantly rationalize security policies with business demands has the massive firm been able to get a grip on its own data-handling needs, she said.

"Customers need to step back and see what their own culture wants. If we locked down everything within IBM, it would be so difficult to manage that we would have a serious management problem, so you have to ask questions around culture before you begin thinking of enforcement," said Donahue.

"You have to assess the risk environment and think of this as a holistic problem in terms of how you place bets and need to manage pools of risk, even though that for most CIOs it often feels like you have to spend your time going day-to-day dealing with the crisis of the moment," she said. "You really need to look at where to make the right investments, where to do enforcement, and where to monitor to have a truly strategic view."

Donahue said that when IBM was building its security practice roughly 16 months ago, it found that customers were spending as much as 10 percent of their IT budgets dealing with the maintenance and complexity of their data security systems.

The only way to reduce the data security management headache is to design an internal framework for managing infrastructure to ensure that investments are being made wisely, she said.

In many cases, those companies that are succeeding in that regard are treating their data assets just as they would treat cold, hard cash, the expert maintains.

"Companies need to protect their vast ecosystem of data like it is a monetary system, they really have to think about it that way," said Donahue. "It can't be the data center's problem or the network administrator's responsibility alone to protect its security; it has to be everyone's responsibility throughout the entire company."

IBM learns about security leaks the hard way

As evidence of the types of things that can happen to undermine even a comprehensive security game plan, Donahue pointed to IBM's loss of two backup tapes that contained sensitive information about former employees earlier this year.

While the incident was actually related to IBM's provider of backup storage services, the company was forced to pay out roughly US\$22 million in remediation costs related to informing those people who had been affected and providing credit monitoring services and the like for those individuals, she said.

In that sense, companies must also require the highest security standards from their business partners, said the expert. IBM has since written stronger backup-tape handling policies into its contract with its partner as a result of the incident, and Donahue encouraged others to do the same.

Phillip Dunkelberger, chief executive at encryption software specialists PGP, said that companies are spending too much time trying to react to data incidents and the individual mandates of compliance regulations while overlooking opportunities to improve data security through smarter process control.

Many companies are still too concerned with protecting various endpoint devices and network assets when a more data-driven approach would save them both time and money, he said.

"It has to be about the data. Data is very much the currency that people are transacting with, and employees need to be able to get their jobs done, even if that means taking information outside the network," said Dunkelberger.

"As complexity grows, things happen -- executives buy [iPhones](#) that are essentially 60GB storage devices that run on Open BSD and allow third-party applications," he said. "Defending the device is going to be a losing war, and even if you try to do that, people will inevitably add to the device or change its configuration."

While it unsurprising that Dunkelberger advocates the use of encryption as an intelligent way to overcome the complexity of changing IT infrastructure and business demands of defending data, he said that problems are most often related to faulty policies, not the types of technologies used for information protection.

The heightened information security atmosphere of today isn't as much a result of the rapid growth of mobile computing or shared infrastructure between companies, but rather an issue of poor data architecture from the top down, he said.

"Unless we start having a comprehensive discussion about the defense of data, the problem will only continue to persist, and not just in relation to hackers or compliance," Dunkelberger said.

"Everyone has policies, but it is interesting how much intellectual property is being targeted and stolen despite that; more of these attacks are coming, and that will only increase costs and complexity if handled improperly because these are the crown jewels of the organizations that are being targeted," he said.

VA puts new IT internal affairs unit on fast growth track

Agency's IT oversight group has grown from seven to 128 employees since February
Patrick Thibodeau

September 26, 2007 ([Computerworld](#)) -- WASHINGTON -- The laptop theft that roiled the [U.S. Department of Veteran Affairs](#) last year prompted a data security overhaul and an ongoing centralization of the agency's IT operations. And it led to the creation of a fast-growing unit that is charged with keeping an eye on IT at the VA.

The Office of IT Oversight and Compliance, known as ITOC, was formed early this year with just seven employees. It now has a staff of 128 workers and is expected to increase that to 165 employees by 2009.

In a memo last February ([download PDF](#)), [VA Secretary R. James Nicholson](#) gave the ITOC a broad mandate to inspect the agency's IT operations and determine whether they are in compliance with laws and regulations. The ITOC will also act as a first responder within the agency to IT security incidents that require review of privacy and security processes.

Arnaldo Claudio, the ITOC's executive director, offered some insight into his organization on Wednesday in [testimony](#) before the House Committee on Veterans' Affairs. Claudio was one of more than a half-dozen witnesses who testified at the [hearing](#), which was held to review the progress of the VA's IT reorganization.

Claudio said the ITOC's goal is to provide "independent, objective and quality oversight and compliance assessment services." The unit's rapid growth in head count "is in itself a success story," he said. "Most government programs take years before they can be stood up and become fully operational."

The ITOC has hired workers from within the private sector as well as the government, according to Claudio. It reports to top IT officials at the VA, including [CIO Robert Howard](#), who also testified at the House hearing.

Prior to the creation of the ITOC, a group called the Review Inspection Division (RID) was tasked with doing reviews and inspections of IT services within the agency. But it was staffed by only five VA employees plus "a handful of contractors," Claudio said. With a total of 12,000 VA sites to inspect, the RID "was given an impossible task to perform," he added.

Claudio told the committee that the idea for the ITOC was suggested, in part, by [Eugene Spafford](#), a professor at Purdue University and executive director of the school's Center for Education and Research in Information Assurance and Security.

Spafford testified before the House Committee on Veterans' Affairs in June 2006 -- one month after the laptop and a hard drive containing the personal data of 26.5 million veterans and active-duty military personnel [were stolen](#) from a VA employee's home in Maryland. In his testimony ([download PDF](#)), Spafford pointed out that the VA lacked a centralized point of authority "to ensure that rules, procedures and good practices are instituted and observed."

The [U.S. Government Accountability Office](#) said last week that the VA has made some progress on improving its IT security processes since the theft of the laptop and hard drive, which were [recovered](#) about a month and a half after they were taken.

But in a report ([download PDF](#)) that was released publicly last week in connection with an [IT oversight](#) hearing held by the Senate Committee on Veterans' Affairs, the GAO added that the VA has yet to [fully implement](#) two of the federal watchdog's four security recommendations and 20 of 22 suggestions from the agency's own inspector general.

The GAO issued another report on Wednesday to coincide with the House hearing. In this week's report ([download PDF](#)), the GAO said the VA hasn't kept to scheduled timelines for implementing new management processes that are the foundation of its IT realignment. The GAO added that if the VA doesn't dedicate a team of employees to oversee the implementation of the realignment plan, the agency could miss its July 2008 target date for completing the internal changes.

Howard told the House panel that the VA has already adopted some of the GAO's recommended actions, such as implementing an IT governance plan and accelerating the development of performance metrics for tracking the progress of the realignment work. The GAO, he acknowledged, had "correctly identified that there is more work to be done to have a successful transition from a decentralized to a centralized organization."

Connecticut sues Accenture over stolen backup tape

There's no indication that the stolen data has as yet been used

Tim Greene

September 26, 2007 ([Network World](#)) -- Accenture Ltd. is in hot water with the state of Connecticut for putting sensitive data about hundreds of state bank accounts and purchasing cards as well as 58 taxpayers on a backup tape that was later stolen.

So far, there is no indication that the data has been used to withdraw money from the accounts or make improper charges against the cards, according to the state attorney general's office.

The tape was lost in June, and Accenture notified Connecticut on Sept. 4, the attorney general said.

The comptroller's office hired Accenture to create a financial data system and transferred some of the data to a tape that was taken to Ohio, where the company was working on a similar project, according to a published report in *The Hartford Courant*. The tape was stolen.

Connecticut is seeking reimbursement for resources expended to secure the data and an order that Accenture return some of the money the state has already paid it.

Accenture says an employee violated company policy in taking the data out of state, according to the *Courant*.

The suit may be prompted by political wrangling between the state's Republican governor and its Democrat attorney general and comptroller. The governor's office said it thought the Democrats hadn't reacted strongly enough to the breach, and three days later, the attorney general filed suit.

The tape was stolen in June from the car of a student intern for the state of Ohio, the *Courant* said.

The attorney general said 298 active purchasing-card numbers were stolen, along with 456 inactive ones.

The Fifth Annual Global State of Information Security

Five years ago, when *CIO* and PricewaterhouseCoopers collaborated on the first "Global State of Information Security" survey, very few people knew how bad the problem was. Now everyone knows. They just don't know how to fix it.

By [Scott Berinato](#)

August 28, 2007 — [CIO](#) —

Awareness of the problematic nature of information security is approaching an all-time high. Out of every IT dollar spent, 15 cents goes to security. Security staff is being hired at an increasing rate. Surprisingly, however, enterprise security isn't improving.

For the fifth straight year, CIO, CSO and [PricewaterhouseCoopers \(PWC\)](#) present select results and analysis from the "Global State of Information Security" survey, the world's largest, most comprehensive annual information security survey.

And the first question to ask is, Are you feeling anxious?

Are you feeling the disquiet that comes from knowing there's no reason why your company can't be the next TJX? The angst of knowing that these modern plagues—these spam e-mails, these bots, these rootkits—will keep coming at you no matter how much time and money you spend trying to stop them? The chill that comes from knowing how much you don't know?

Yeah, you're feeling it.

You're feeling it because you're seeing it. According to the 2007 survey, a comprehensive canvassing of 7,200 respondents on six continents, you see the information security problem more clearly than ever before. You're seeing it because you've created tools and systems in order to see it. For example:

- *You've added processes.* Three years ago, only 37 percent of companies reported having an overall security strategy. This year, 57 percent did. Also, nearly four out of five companies conducted enterprise risk assessments, at least periodically.
- *You've deployed technology.* Nine out of 10 respondents said they use firewalls, monitor users and rely on intrusion detection infrastructure, and that number approached 98 percent when responses were limited to larger companies (more than \$1 billion in revenue). Encryption is at an all-time high, with 72 percent reporting some use of it (compared to 48 percent last year).
- *You've hired people.* The number of CISOs and CSOs employed continues to rise. And the mean number of information security workers per company has topped 100, most likely due to more outsourcing and the use of contract employees.

You've crafted an infrastructure for understanding. You're seeing it, and that's why you're feeling it. You're undergoing a shift from a somewhat blissful ignorance of the serious flaws in computer security to a largely depressing knowledge of them.

Awareness may be at an all-time high, but awareness doesn't equal improvement, and awareness doesn't bring happiness. The sad fact is that the strides made to date have not crossed the threshold from seeing to fixing.

PWC BREAKDOWN BY SECTOR

- **Aerospace and Defense**
- **Energy (oil and gas)**

- **Entertainment and Media**
- **Financial Services**
- **Healthcare/provider**
- **Healthcare/payer**
- **Pharmaceuticals**
- **Public Sector**
- **Retail and Consumer**
- **Telecommunications**
- **Utilities**

"That next level of maturity has not been reached," says Mark Lobel, a principal with PWC's advisory services. "We have the technology but still don't have our hands around what's important and what we should be monitoring and protecting. Where's that console that says, 'Hey, credit card numbers are crossing the firewall and this is a PCI issue that has a real business impact?'"

Read on for more on what awareness has led to and other insights from the "Global State of Information Security 2007" survey.

"I See," Said the Blind Man

Five years ago, 36 percent of respondents to the "Global State of Information Security" survey reported that they had suffered zero security incidents. This year, that number was down to 22 percent.

Does this mean there are more incidents? We don't think so. We believe it simply means that more companies are aware of the incidents that they've always suffered but into which, until recently, they had no visibility. Those once inexplicable network outages are now known to be security incidents. Perhaps a spam outbreak wasn't considered a security incident before, but now that it can deliver malware, it is. Awareness is higher, and that's because companies have spent the past five years building an infrastructure that creates visibility into their security posture.

The Infrastructure Is in Place

Baseline deployment of people, process and technology continues to rise steadily, sometimes dramatically. Among those companies that don't have these techniques in place, the priority for adding it is remarkably low, indicating that most people who think they need these things now have them.

	2006	2007	Priority for 2008
People: You have a...			
CSO	21%	28%	13%
CISO	22%	32%	17%
CPO	16%	22%	14%
Processes: You have...			
An overall security strategy	37%	57%	13%
A baseline for customers/partners	25%	42%	10%
Centralized SIM	34%	44%	11%

Technology: You deploy...

Firewalls	77%	93%	15%
Encryption	43%	72%	25%
IDS/A-V/other detection*	57%	90%	28%
Data backup	78%	82%	14%
User security/ID management*	73%	89%	33%
IPS/filters*	44%	83%	22%
Internet security*	31%	70%	14%

* Before 2007, these categories were not consolidated. The percentage listed is the highest percentage given for one of the subcategories now consolidated into the new category.

We've Seen the Enemy; It's You

This year marks the first time "employees" beat out "hackers" as the most likely source of a security incident. Executives in the security field, with the most visibility into incidents, were even more likely to name employees as the source.

Likely Sources of Incidents

Recognition of the insider threat is a sign that awareness is increasing, largely due to the controls that have been put in place over the past five years.

Who attacked us?

	2006	2007	2007 Security Executives Only
Employee/former employee	51%	69%	84%
Hacker	54%	41%	40%

Have employees suddenly turned more malicious? Are inside jobs suddenly more fashionable and productive than they used to be? Probably not. Most security experts will tell you that the insider threat is relatively constant and is usually bigger than its victims suspect. None of us wants to think we've hired an untrustworthy person.

This spike in assigning the blame for breaches and attacks to employees is probably more like the dip in companies that report zero incidents—a reflection of awareness, of managers' ability to recognize what was always there but what they couldn't previously determine.

"What's happening is we're doing a better job with logging and understanding situations," says Ron Woerner, former information security manager at ConAgra Foods, now security engineering consultant at [TD Ameritrade](#). "For a while, I think, ignorance was bliss. Now, with all the technology in place, we're learning that we all have the same problems."

Here's how building a security infrastructure can lead to more employees named as culprits in security incidents: A CISO is hired. He has the tools to investigate internal network anomalies and the authority to ask business unit leaders to provide him with information for an investigation. His deployment of user-monitoring tools helps him identify insider threats. Then he centralizes security information management software that automatically detects anomalous network behavior. Then maybe he adds a periodic risk assessment process (another trend on the rise, according to the survey), and suddenly his office is finding previously unknown vulnerabilities being exploited. Perhaps he adds an anonymous e-mail/hotline function for whistle-blowers. With all of this and more in place, a company has increased its odds of detecting security incidents.

But here's an odd paradox: Despite the massive buildup of people, process and technology during the past five years, and fewer people reporting zero incidents, 40 percent of respondents didn't know how many incidents they've suffered, up from 29 percent last year.

The rate of "Don't know" for the type of incident and the primary method used to attack also spiked.

What You Don't Know...Could Fill Volumes

I Dunno

Increasingly, those involved in information security reply "Don't know" when asked about the number and nature of security incidents.

	2006	2007	2007 CSO/CISO
Number of incidents	29%	40%	29%
Type of attack	26%	45%	32%
Primary method used	26%	33%	20%

It doesn't bode well that after years of buying and installing systems and processes to improve security, close to half of the respondents didn't have a clue as to what was going on in their own enterprises. But when close to a third of CSOs and CISOs, who presumably should have the most insight into security incidents, said they don't know how many incidents they've suffered or how these incidents occurred, that's even worse.

The truth is, systems, processes, tools, hardware and software, and even knowledge and understanding only get you so far. As Woerner puts it, "When you gain visibility, you see that you can't see all the potential problems. You see that maybe you were spending money securing the wrong things. You see that a good employee with good intentions who wants to take work home can become a security incident when he loses his laptop or puts data on his home computer. There's so much out there, it's overwhelming."

Woerner and others believe that the security discipline has so far been skewed toward technology—firewalls, ID management, intrusion detection—instead of risk analysis and proactive intelligence gathering.

If most of the investment has been put into technology, most of the return will come from there too. The tools will do their job. They will tell you what's happening and block the most ham-fisted attacks. But technology is largely reactive. It provides alarms and ex post facto reports of anomalies. Intrusion detection, for example, is not terribly effective at threat intelligence—understanding the nature of vulnerabilities before they affect you. All IDS boxes know is that some preset rule has been broken. Think of a glass break sensor on a window at a museum. That piece of technology is extremely effective at telling you that someone broke the window; it does nothing to explain how and why a painting was stolen, nor can it help you prevent the next window from being broken and the next painting from being snatched.

Furthermore, even a cursory look at security trends demonstrates that adversaries, be they disgruntled employees or hackers, have far more sophisticated tools than the ones that have been put in place to stop them. Antiforensics. Mass distribution of malware through compromised websites. Botnets. Keyloggers. Companies may have spent the past five years building up their security infrastructure, but so have the bad guys. Awareness includes a new level of understanding of how little you know about how the bad guys operate. As arms races go, the bad guys are way ahead.

Why You Have to Change Your Strategy

What can be done about all this? Be strategic. Security investment must shift from the technology-heavy, tactical operation it has been to date to an intelligence-centric, risk analysis and mitigation philosophy.

Information and security executives should, for example, be putting their dollars into industry information sharing. "Collaboration is key," says Woerner. They should invest in security research and technical staff that can capture and dissect malware, and they should troll the Internet underground for the latest trends and leads. Dozens of security companies do just this and provide subscriptions to research services.

"We have to start addressing the human element of information security, not just the technological one," says Woerner. It's only then that companies will stop being punching bags. Only then will they be able to hit back.

IT Strikes Back

Speaking of striking back, the 2007 security survey shows a remarkable (some might say troubling) trend.

The IT department wants to control security again.

In the first year of collaboration [on this survey](#), CIO, CSO and PWC noted that the more confident a company was in its security, the less likely that company's security group reported to IT. Those companies also spent more on security.

The reason CIO and CSO have always advocated for the separation of IT and security is the classic fox-in-the-henhouse problem. To wit, if the CIO controls both a major project dedicated to the innovative use of IT and the security of that project—which might slow down the project and add to its cost—he's got a serious conflict of interest. In the 2003 survey, one CISO said that conflict "is just too much to overcome. Having the CISO report to IT, it's a death blow."

And every year after that, the trend was for the security function to gain increasing autonomy. More security executive positions were created. More decision-making power was shifted to security and away from IT. And more security groups reported to functions outside of IT, including the legal department, the risk department and, most significantly, the CEO. The trend was even more pronounced at large companies.

In 2007, this trend didn't slow down; it flipped. What's more, the reversal was most pronounced in the largest companies. For example, respondents chose from 12 possible functions to which their CISO could report. Those 12 functions were divided into three categories:

1. IT (CIO, CTO)
2. Neutral (board, CEO, CFO, COO, legal)
3. Security (CSO, risk, security committee, CPO, audit)

To allow respondents to select more than one of these answers, we created "shares"—the percentage of respondents with some reporting relationship to one of these three categories. Here are the results.

Reporting to IT

Security has some reporting relationship to the following:

	2006	2007	2007 (>\$1B Revenue)
IT	41%	53%	60%
Neutral	76%	79%	68%
Security	44%	46%	48%

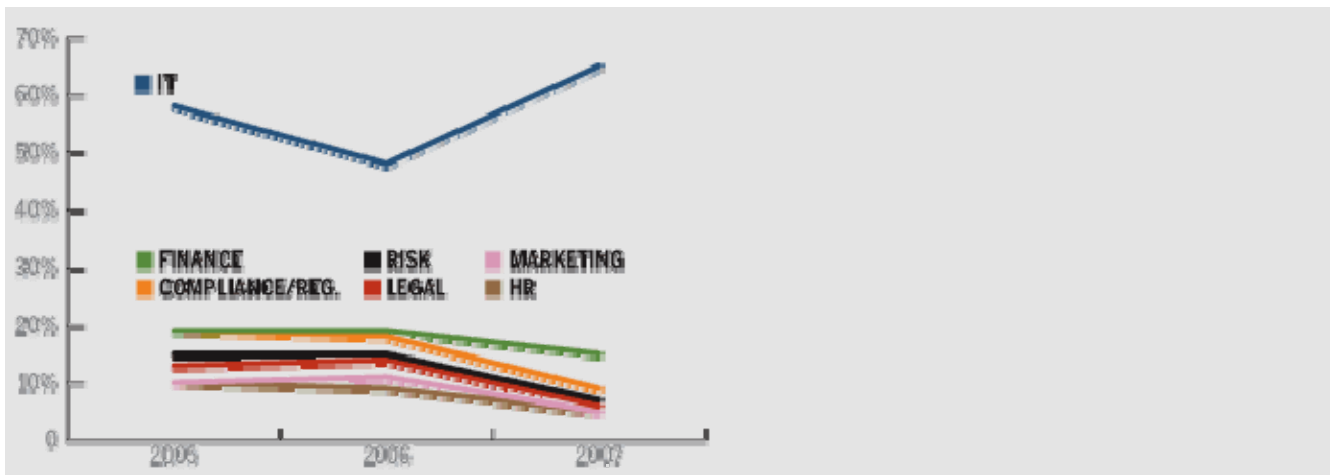
A 12 percent rise in the number of security executives reporting to IT is hugely significant. And when you slice that by large companies, it's a 19 percent rise. Notice, too, that bigger companies show fewer information security executives reporting to neutral functions.

M. Eric Johnson, an economist who specializes in information security issues at Dartmouth College, says, "We actually analyzed the org charts, and the solid-line relationships are going back to IT and the CIO. CISOs have gobs of dotted line relationships, but IT is dominating reporting structures and the budgets."

Indeed, the trend is even more pronounced when you follow the money trail.

Security Dollars Come from IT

Funding for information security comes from (could check more than one)



Another hallmark of an evolved security function is its convergence with physical security, usually under a CSO. This makes sense both for operational efficiency and because threats are becoming more converged. Access control is a classic example of convergence paying dividends. By combining building access and network access in one system, you save money, improve efficiency and create a single view into both physical threats (illegal entry) and digital ones (illegal network access).

And for four years, convergence of physical and IT security steadily increased. Until this year.

And Furthermore...

More data points to ponder from the "Global State of Information Security" Survey.

"Uh, Boss? Can We Talk?"

Are security and IT communicating enough with the CEO? By comparing their answers, one finds some startling disconnects.

What the Boss Thinks; What You Know

CEOs seem to think their enterprises are a lot more secure (and their employees more reliable) than CIOs and security leaders do. Conversely, CIOs and security leaders are a lot more optimistic about their budgets than are their CEOs.

	CEO	CIO	CISO/CSO/ Infosec dir.
We've had fewer than 10 security incidents	74%	65%	53%
We've had an unknown number of incidents	18%	25%	28%
An employee or former employee was the source of the incident	44%	71%	83%
We do not conduct enterprise risk assessments	31%	21%	13%
Security spending will increase in '07	41%	53%	57%
Spending will stay the same	41%	32%	28%

We Need to Be But Are Not in Compliance With

Again, CEOs are far more confident than their CIOs and security execs that their enterprises are compliant. Either the CEOs are clueless, or the people who should know aren't telling.

	CEO	CIO	CISO/CSO/ Infosec dir.
HIPAA	9%	14%	27%
Sarbanes-Oxley	9%	20%	32%
State privacy breach laws	10%	12%	21%

Privacy—Better, But...

Perhaps because of the sheer number of incidents involving privacy breaches, companies have improved their privacy practices. They are increasingly separating privacy from security and also separating security governance (which would take part in setting privacy policy) from tactical security. That means, for example, the people deploying monitoring tools aren't the ones setting the usage policy for those tools. But more work needs to be done. Some of the key steps to ensuring data privacy—encrypting databases, classifying data by risk level—haven't become standard practice. The industry least likely to have adopted privacy practices is technology. A privacy leader? Consumer banking.

Who Wants to Know?

Privacy Best Practices

	Employ CPO	Separate privacy & security	Separate security gov. & ops.	Classify data by risk
Overall	22%	54%	66%	70%
> \$1B	30%	66%	58%	79%

revenue				
Financial services	33%	64%	60%	80%
Consumer financial	41%	69%	55%	90%
Retail	14%	51%	66%	58%
Health insurance	53%	73%	49%	81%
Healthcare provider	49%	72%	65%	64%
Technology	22%	49%	72%	77%

More on Privacy

While 60 percent of survey respondents posted privacy policies internally, only 24 percent posted policies on their external websites. Only 28 percent audited their privacy standards through a third party. Sounds like a cover-your-butts ploy; after all, if you don't have a policy posted, you can't be sued for violating or not living up to it. And if you haven't had your privacy audited, you don't have to fix all the problems an audit would find.

Respondents who do not keep an accurate inventory of user data:	69%
Respondents who do not keep an accurate inventory of where data is stored:	67%

Region of Risk

One of the areas of the world where the focus on information security has intensified is Latin America, specifically Brazil and Mexico. Researchers and law enforcement believe that cultural differences in acceptance of less-secure online transaction methods and fewer controls and regulations on banking activity have made the region the banking center of choice for the Internet criminal underground. Here are some select findings.

	Infosec budget as % of IT budget	Do not conduct risk assessment	Budget will rise more than 10% in '07	> 1 day downtime
Overall	15%	23%	20%	8%
U.S. and Canada	12%	19%	16%	7%
South America	19%	36%	30%	15%
Brazil	16%	43%	29%	21%
Mexico	21%	33%	28%	13%
China	19%	32%	26%	13%
India	21%	17%	33%	9%

Physical and Information Security Converge, Then Diverge

Information and physical security are separate

	Overall Revenue \$1B or more	
2003	71%	NA
2004	50%	NA
2005	47%	NA
2006	25%	36%

2007	46%	55%
Information and physical security report to the same executive leader		

	Overall Revenue \$1B or more	
2003	11%	NA
2004	26%	22%
2005	31%	24%
2006	40%	33%
2007	34%	27%

Respondents that do not integrate physical and information security personnel: 69%
Of those, percent with no plans to integrate personnel: 80%

Who's in Charge?

Signs of IT's control and influence are peppered throughout the survey results. For example, when asked what security guidelines their companies followed, respondents were far more likely—in some cases two or three times more likely—to cite more general IT guidelines like ITIL than security-specific ones like SAS 70 and various ISO security standards.

What's going on here? Johnson has one theory: "Security seems to be following a trajectory similar to the quality movement 20 or 30 years ago, only with security it's happening much faster. During the quality movement, everyone created VPs of quality. They got CEO reporting status. But then in 10 years the position was gone or it was buried."

In the case of the quality movement, Johnson says, that may have been partly because quality became ingrained, a corporate value, and it didn't need a separate executive. But the evidence in the survey suggests that security is neither ingrained nor valued. It's not even clear companies know where to put security, which would explain the "gobs of dotted line" reporting structures.

That brings us to another theory: organizational politics. What if separating security from IT were creating checks on software development (not a bad thing, from a security standpoint)? What if all this security awareness the survey has indicated actually exposed the typical IT department's insecure practices?

One way for IT to respond would be to attempt to defang security. Keep its enemy close. Pull the function back to where it can be better controlled.

SURVEY METHODOLOGY

The "Global State of Information Security 2007" survey, a worldwide study by *CIO*, *CSO* and PricewaterhouseCoopers, was conducted online from March 6 through May 4, 2007. Readers of *CIO* and *CSO* and clients of PricewaterhouseCoopers from around the globe were invited via e-mail to take the survey. The results shown in this report are based on the responses of 7,200 CEOs, CFOs, CIOs, CSOs, VPs and directors of IT and IS, and security and IT professionals from more than 100 countries. Thirty-six percent of the respondents were from North America, followed by Europe (28%), Asia (23%), South America (12%), and the Middle East and South Africa (2%). The margin of error for this study is +/- 1%.

"What I hear from CIOs," says Johnson, "is at the end of the day they're responsible for failures anyway. They're on the line whether security is separate or not." Why wouldn't the CIO want to control something he's ultimately responsible for?

On the other hand, maybe security was never as separate as it seemed. Companies created CISO-type positions but never gave them authority. "I continually see security people put in the position of fall guy," says Woerner of TD Ameritrade. "Maybe some of that separation was, subconsciously, creating a group to take the hit." Woerner also believes that the trend of the security budget folding into the IT department could be a direct result of security auditing that focuses primarily on infrastructure. That is, when auditors look at information security weaknesses, they recommend technological fixes. And IT buys the technology. Why should IT be charged for another department's expenses?

Whatever the reason, the trend is disturbing to some security professionals, especially at a time when they play an ever more central role in corporate crises, and in society in general.

The state of Internet security is eroding quickly. Trust in online transactions is evaporating, and it will require strong security leadership for that trust to be restored. For the Internet to remain the juggernaut of commerce and productivity it has become will require more, not less, input from security.

But right when the best and brightest security minds are needed most, they're being valued less.

[Scott Berinato](#) is executive editor of *CSO*.

Web 2.0, social networking can endanger corporate security, analyst says

Beware the 'perforated perimeter,' warns IDC's Christian Christiansen

Linda Rosencrance

October 02, 2007 ([Computerworld](#)) -- With the Web becoming central to the way companies do business, cybercriminals are taking increasing advantage of Web 2.0 and social networking sites to launch attacks, according to IDC analyst Christian Christiansen.

The Web isn't the benign resource for information that people once saw it as, said Christiansen, who spoke today at [Kaspersky Lab Inc.](#)'s Surviving CyberCrime conference in Waltham, Mass. "One of the things that's happened that's disconcerting -- and it's been growing over the last 10 years -- is the blending of people's private lives with their corporate lives," he said.

Employees' personal lives -- their online shopping habits and interactions with friends and families -- get intermingled with the interactions they have at work with customers, fellow employees, partners and suppliers, he said. "So that creates a perforated perimeter where there isn't a hard, fast separation between the corporate world and the personal world," he said.

The problem is that employees don't always follow their companies' security policies -- probably because they don't know what those policies are, just as they don't know what their companies' acceptable use policies are. The result: employees don't know what's allowed and what they're barred from doing. Sometimes, Christiansen said, the very people who set up the corporate policies don't even follow them.

Problems also occur when an IT department no longer controls the products being connected to the corporate network. That list could include everything from smart phones to new and untested laptop and desktop computers to various application environments, he said.

"We're seeing the realization that the internal security problem is growing -- the threats are coming from inside the network," he said.

The latest threats to network security now are coming from collaboration and Web 2.0 environments -- where employees casually click on links that could lead them to malware. And they're coming from the wide variety of devices that may be accessing private as well as corporate networks, he said.

"We're seeing a change in the threat environment," he said. "Instead of the threats -- the malicious code -- being distributed as e-mail attachments, we're seeing more and more that they're being embedded in Web 2.0 links," he said. "In the past, what you saw was an immediate effect. Now we're seeing much greater levels of subterfuge and much more sophisticated attacks."

To better avoid potential problems, IT departments need to control user behavior, the types of devices being used to access information, the applications being used and content contributions.

"Risk reduction requires policy managements and layered protection -- at the gateway to the Internet as well as at the endpoint [desktops, laptops and servers]," he said. "You need a whole series of checks and balances."

Federal agencies face obstacles in implementing FISMA, says GAO

The 2002 law is designed to help agencies better protect data

Jaikumar Vijayan

October 03, 2007 ([Computerworld](#)) -- Four U.S. agencies -- the departments of Homeland Security, Justice, Defense and State -- are apparently still having trouble complying with some of the requirements of the Federal Information Security Management Act (FISMA) of 2002, according to the [U.S. Government Accountability Office](#) (GAO).

Four years since federal agencies began reporting on their progress in implementing the requirements of FISMA, several are still struggling to meet all of the requirements for a variety of reasons, according to the GAO.

For instance, in a report dated Aug. 31, the GAO found that the U.S. Department of Defense ([DOD](#)) has been particularly challenged in trying to develop a complete inventory of major systems. The problem there has to do with the different definitions the department uses for what constitutes a "system," the GAO report said.

Meanwhile, the [U.S. Department of Homeland Security's](#) (DHS) FISMA problems center on security training issues: The tool DHS uses to report security training activities only counts each course taken by an employee -- not whether an individual has taken any required, specialized courses.

Each of the four agencies also had trouble demonstrating that it had controls in place for monitoring and evaluating the effectiveness of its own security controls.

"The challenges in implementing these requirements arose from various weaknesses, including inadequate tools and gaps or inconsistencies in guidance," the GAO noted. "Until the departments address their challenges and fully implement effective departmentwide information security programs, increased risk exists that they will not be able to effectively protect the confidentiality, integrity and availability of their information and information systems."

The report was based on an investigation of the challenges each of the departments faced in complying with FISMA. Federal agencies affected by the act are required to implement a specific set of information security controls and processes for protecting confidential data. They are supposed to conduct an inventory of all major systems, common security configurations, training measures, testing and evaluation controls and form security certification processes.

Each agency's inspector general is required to provide the [White House Office of Management and Budget](#) with an annual FISMA progress report detailing the steps the department has taken to implement the required controls.

The GAO report appeared to draw a mixed response from each of the departments studied.

In a formal response to the findings, a Defense Department assistant secretary refused to accept the GAO's recommendation that the DOD implement a departmentwide definition for what constitutes a major system. The agency argued that it already had such a definition in place and would continue to use that definition. The department also refused to concur with the GAO's assessment of its overall FISMA compliance.

Similarly, [State Department](#) officials challenged the GAO's characterization that its issues have hindered FISMA implementation. Rather than being obstacles, the issues mentioned in the FISMA report have already been identified as weaknesses that the agency is addressing, the State Department said in a response.

"GTISC Releases Emerging Cyber Threats Forecast" Georgia Institute of Technology (10/02/07)

The Georgia Tech Information Security Center has published its annual forecasting report, the GTISC Emerging Cyber Threats Report for 2008, which describes the five key areas of security risk for enterprise and consumer Internet users. In 2008, cyber security threats are anticipated to grow and evolve in the areas of Web 2.0 and client-side attacks, such as social networking attacks, and targeted messaging attacks, including malware proliferation through video-sharing online and instant messaging attacks. Botnets, particularly the expansion of botnet attacks into peer-to-peer and wireless networks, are another significant area of concern. Threats aimed at mobile convergence, including vishing, smishing, and voice spam, are anticipated to be substantial, as are threats targeting RFID systems. The primary driver behind all five major threat categories in 2008 continues to be financial gain. GTISC recommends improved synchronization among the security industry, the user community, application developers, Internet service providers, and carriers. GTISC director Mustaque Ahamad anticipates that enterprise and consumer technologies will continue to converge in 2008, making it even more essential to protect new Web 2.0-enabled applications and the IP-based platforms they increasingly depend upon.