

## ESO - Security Trends Report

11/09

### ***Corporate Breaches Increase Chances Of Consumer ID Theft, Study Says***

#### **When their data is leaked by a business, individuals are four times more likely to suffer identity theft, Javelin study says**

Nov 04, 2009 | 07:03 PM

**By Tim Wilson**  
***DarkReading***

Consumers who have received data breach notifications within the past year are at a much greater risk for fraud than typical consumers, according to a new study.

According to a report published last week by Javelin Research, individuals whose personal information has been compromised in a corporate breach are four times more likely to suffer identity theft or fraud. This result runs contrary to the common mantra among breached companies, which often say that they have no indication that the compromised data has been used by criminals.

"Data breach notifications are intended to help consumers take protective action," said Mary Monahan, managing partner and research director at Javelin. "Notification is critical because consumers are over four times more likely to encounter actual fraudulent transactions if they receive a data-breach notification."

But the Javelin study also indicates that most consumers don't see a direct relationship between breach notifications and identity theft.

"During each of the past three years, an average of 11 percent of consumers received a breach notification," Javelin said. "Slightly more than 33 percent of breach victims experienced exposure of their Social Security numbers, and 15 percent of breach victims had their ATM PINs compromised. [But] despite 19.5 percent of breach victims suffering some kind of fraud in the past year, only 2 percent attribute their fraud to the breach."

The Javelin report, "Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud," is based on multiple years of data and includes updates on 2009 data breaches. The report also presents a timeline overview of the most recent and egregious data breaches in U.S. history, with recommendations for how individuals and companies can increase safety

### **Judge says TD Ameritrade's proposed security fixes aren't enough**

#### **Court rejects company's proposed class-action settlement for 2007 data breach**

**By Jaikumar Vijayan**

October 27, 2009 02:59 PM ET

Computerworld - A federal judge's rejection of a proposed settlement by TD Ameritrade Inc. in a data breach lawsuit marks the second time in recent months that a court has weighed in on what it considers to be basic security standards for protecting data.

U.S. District Court Judge Vaughn Walker in San Francisco yesterday denied final approval of a settlement that had been proposed by TD Ameritrade in May to [settle claims stemming from a 2007 breach](#) that exposed more than 6 million customer records.

In arriving at his decision, Walker said the court didn't find the proposed settlement to be "fair, reasonable or adequate." Rather than benefiting those directly affected by the breach, Ameritrade's proposed settlement was designed largely to benefit the company, Walker wrote in his 13-page ruling.

In September 2007, Ameritrade announced that the names, addresses, phone numbers and trading information of potentially all of its more than 6 million retail and institutional customers at that time had been compromised by an intrusion into one of its databases. The stolen information was later used to spam those customers.

As part of an effort to settle claims arising from that incident, Ameritrade this May said it would retain an independent security expert to conduct penetration tests of its networks to look for vulnerabilities.

The company also offered to retain the services of an analytics firm to find out whether any of the data that had been compromised in the breach had been used for identity theft purposes. The company also said it would give affected customers a one-year subscription for antivirus and antispyware software.

It was those offers that the judge dismissed as too meager. He described the additional security measures that Ameritrade proposed in the settlement as "routine practices" that any reputable company should be taking anyway.

Penetration tests provide a reliable way for companies to detect the sort of security weaknesses that led to the Ameritrade breach, Walker said. But "as a large company that deals in sensitive personal information, penetration and data breach tests should be routine practices of TD Ameritrade's department that handles information security," he wrote.

The two "very temporary fixes do not convince the court that the company has corrected or will address the security of client data in any serious way, let alone provide discernible benefits," he noted.

A TD Ameritrade spokeswoman expressed disappointment at the ruling, especially considering the amount of time spent working to arrive at the proposed settlement. "We felt it was fair and reasonable and would have provided benefit to members of the class," she said.

Both sides are scheduled to meet in court again in December to try to figure out how to move forward. "There are a number of options available to us," the spokeswoman said, though she declined to elaborate.

The case is the latest to illustrate a growing willingness by courts around the country to consider claims of negligence and breach of contract brought by individuals against companies for failing to protect sensitive data.

In August, the federal court for the Northern District of Illinois [denied a request by Citizens Financial Bank to dismiss a negligence claim](#) brought against it by a couple. The two had claimed that Citizens' failure to implement two-factor user-authentication measures had resulted in the theft of more than \$26,000 from their home equity line of credit.

The judge hearing the case allowed the claim to move forward, saying there was a reasonable basis to show that the bank had not moved as quickly to implement stronger user-authentication measures as it should have.

Such rulings are relatively rare in consumer lawsuits against companies that suffer data breaches involving the potential compromise of credit card data and personal information.

Until recently, courts have tended to reject such lawsuits mainly on the grounds that consumers suffer little financial harm from such breaches. They have also held that consumers can't seek damages for any potential injury that could stem from any future identity theft that might result from such breaches.

A case before the Maine Supreme Court is [testing whether consumers can seek restitution](#) from merchants for the time and effort involved in changing payment cards and bank accounts after a data breach.

# Pandemic Seen Slowing Internet Traffic

## Net Capacity Could be Tested by Temporary Telework

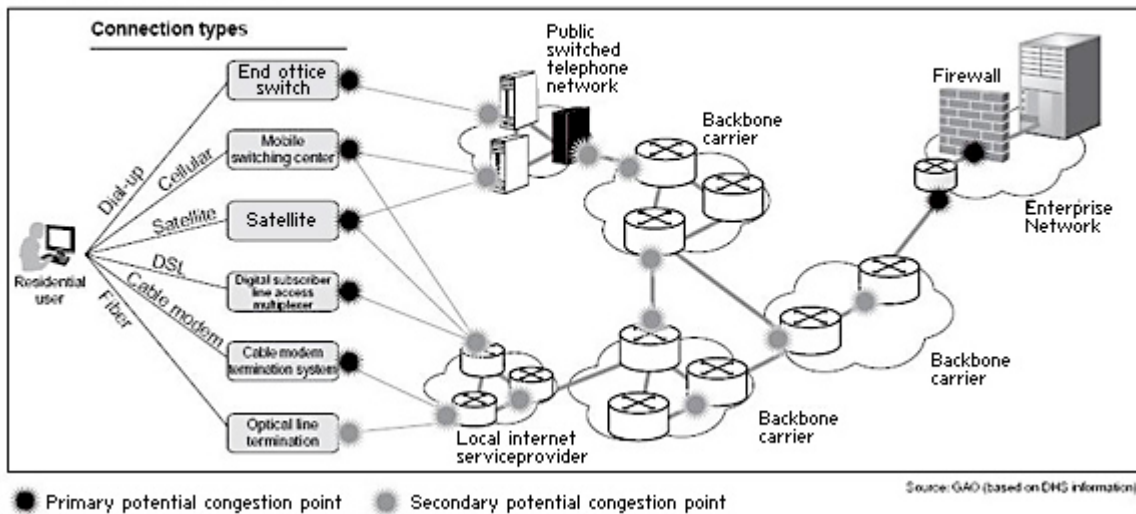
October 26, 2009 - Eric Chabrow, Managing Editor

In the event of a severe pandemic, the Internet might not be able to accommodate increased traffic caused by the increased number of people working from home, the Government Accountability Office said Monday in a report issued.

The report, entitled [Influenza Pandemic: Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet](#), comes just days after President Obama [declared a national emergency](#) because of the spreading H1N1 flu and focuses on the financial services industry, though the impact could be broader to include a wide number of industries.

"Increased demand during a severe pandemic could exceed the capacities of Internet providers' access networks for residential users and interfere with teleworkers in the securities market and other sectors," the GAO study said, citing studies by the Department of Homeland Security, Internet service providers and its own analysis.

Potential Points of Congestion



GAO, Congress' investigative arm, said ISPs have limited ability to prioritize traffic or take other actions that could assist critical teleworkers. The Congressional auditors said some actions, such as reducing customers' transmission speeds or blocking popular Web sites, could negatively impact e-commerce and require government authorization.

According to the GAO, DHS has failed to:

- Develop a strategy to address potential Internet congestion or worked with federal partners to ensure that sufficient authorities to act exist;

- Assess the feasibility of conducting a campaign to obtain public cooperation to reduce nonessential Internet use to relieve congestion; and

- Commence coordinating with other federal and private sector entities to assess other actions that could be taken or determine what authorities may be needed to act.

GAO pointed out that because key securities exchanges and clearing organizations mostly employ proprietary networks that bypass the public Internet, their ability to execute and process trades should not be affected by any congestion. And, these financial services organization have prepared pandemic plans that addressed key

regulatory elements, including hygiene programs to minimize staff illness and continuing operations by spreading staff across geographic areas. However, GAO said, not all of these financial services companies had completed or documented analyses of whether they would have sufficient staff capable of carrying out critical activities if many of their employees were ill. Also, the report said, not all had developed alternatives to teleworking if congestion arises.

GAO said the staff of the Securities and Exchange Commission has regularly examined market organizations' readiness, but could further reduce risk of disruptions by ensuring that these organizations prepare complete staffing analyses and teleworking alternative.

GAO recommended and the SEC concurred that the SEC conduct better reviews of market participants' plans.

But DHS didn't concur with all of GAO's recommendations. Jerald Levine, DHS director of departmental GAO/Office of Inspector General Liaison Officer, wrote to the GAO that DHS will take steps to mitigate the impact of any pandemic-related congestion on the systems that the federal government uses to communicate critical national security/emergency preparedness information. However, he wrote, addressing Internet congestion for other communications, as a general matter, does not fall within DHS's responsibilities, and that DHS does not have the responsibility for developing an Internet congestion strategy separate and apart from assuring national security/emergency preparedness communications.

In response, GAO said a presidential directive, HSPD-7, gives DHS broader authority to safeguard key communications networks, and under that authority, should take the steps to relieve potential congestion during a pandemic.

A number of members of Congress prompted GAO to conduct its study as concerns grew that a more severe pandemic outbreak than this past year's H1N1 flu could cause large numbers of people to stay home, increasing their Internet use and overwhelm ISPs' network capacities. According to GAO, such network congestion could prevent staff from broker-dealers and other securities market participants from teleworking during a pandemic.

## **Gartner joins GAO in raising flu network congestion fears**

**'Last mile' would be the bottleneck, as students vie with workers at home**

**By Matt Hamblen**

October 30, 2009 06:04 AM ET

Computerworld - Could the H1N1 flu virus give networks a bad case of congestion? It could if workers and students are forced to stay home because of the pandemic.

Officials at the U.S. Government Accountability Office [weighed in on the potential for clogged networks](#) Monday in a 71-page report: Gartner Inc. analysts reiterated the GAO's concerns yesterday.

Although the issue has been raised before by various ISPs and network carriers, recent worries have focused on securities firms that depend on third parties to clear trades and process payments over the Internet, according to the GAO. "Internet congestion during a severe pandemic that hampers teleworkers is anticipated, but responsible government agencies have not developed plans to address such congestion and may lack clear authority to act," the GAO warned.

Gartner picked up that GAO theme and offered some technical tips for businesses grappling with the problem. Work-at-home strategies for organization "may be in jeopardy as residential Internet bandwidth supply may not meet demand," Gartner said.

Both Gartner and the GAO, as well as other groups, have consulted with ISPs, carriers and large carrier consortiums on this issue, and have noted that Internet backbone congestion from a pandemic is not a major

concern. The larger problem may be with the network "edge" or "last mile" in the residential portion of the Internet.

The last mile is a generic name often used for the wired connections between homes and carrier switching offices, often a mile or so away from a group of homes.

Al Berman, executive director of the Disaster Recovery Institute in New York, agreed, saying there could be congestion problems for workers who work at home without the right equipment. He urged companies to do stress testing on their private networks.

Gartner said that dozens of residential DSL users could share a single DSLAM connection at the carrier's switching office to reach the backbone, contributing to congestion problems. "Last-mile DSL and cable modem networks are where remote access falls apart," said John Girard, a Gartner analyst. "Backbones will be affected [some], but the network edge will crash."

While the network edge impact would vary by neighborhood, Gartner based its comments on a Centers for Disease Control planning guideline that assumes 40% of the workforce may be out of the workplace for an extended period of time during a pandemic.

In some ways, Gartner went further than the GAO in airing concerns about network readiness, although the focus of Gartner's comments was on businesses -- not how the government should work with businesses.

Gartner analyst Roberta Witty said that current work-at-home strategies being implemented by organizations to deal with pandemic-related network congestion "will likely not work" in a true emergency. She recommended that IT groups work with network service providers to decide in advance which business operations require heavy Internet use. Companies may even need to stagger hours of operation to increase chances of getting needed bandwidth.

Gartner suggested three ways businesses can improve bandwidth for work-at-home employees during a pandemic:

- Consider deploying WAN optimization controller software on every laptop used at home to mitigate bandwidth and latency problems. Such software can reduce the bandwidth needed for many applications by 80% to 90%.
- Install client applets that work with data center application delivery controllers or with WAN optimization controller software to reduce network performance bottlenecks.
- Bypass the wired last mile by switching to a wireless connection such as 3G or Wimax or satellite. Even so, Gartner said to assume that wireless services might also be overused in an emergency.

The GAO's report is far broader, and indicates that service providers could add extra network capacity, install direct lines to businesses, temporarily reduce maximum transmission rates or shut down some Internet sites. But all those methods are limited by technical difficulties and whether the government has the authority to insist on such moves.

The GAO asked several government agencies to comment on its report, and included a response from the Department of Homeland Security (DHS) that went on for several pages. In one portion, DHS urged all Internet users, including financial services, to develop pandemic contingency plans.

"An expectation of unlimited Internet access during a pandemic is not realistic, any more so than an expectation that traffic congestion on hurricane evacuation routes can be completely avoided," the DHS wrote. "All users which rely on the Internet, including the financial services sector, should not expect that Internet congestion problems will be easily solved...."

# Opinion: Stolen fingers: The case against biometric identity theft protection

By George Tillmann

October 27, 2009 10:56 AM ET

Computerworld - According to Winston Churchill, there is no worse mistake in leadership than to hold out false hopes. One area where false hopes have long abounded is information security, and it's happening again.

This time the false hope we're extending is that we can deploy one simple piece of technology that will significantly reduce the problem of [identity theft](#). Of course, identity theft is a huge and growing problem. Each year, the identifying information of millions of Americans is stolen from corporate databases. Companies face billions of dollars in theft, millions of dollars in fines and, perhaps most important, the loss of customer trust.

Worse, identity theft can harm victims through lost savings, rejected loans and denied jobs. CIOs are faced with a security challenge that threatens the viability not only of the IT organization but of the entire corporation as well. To date, the countermeasures that we've deployed -- passwords, PINs and authentication tokens -- have been ineffective. All can be stolen and used by the nefarious.

This has made inexpensive [biometrics](#) look attractive for authenticating employees, customers, citizens, students and any other people we want to recognize. But do the benefits of biometrics outweigh the risks?

[Biometrics](#) rely not on something you *have* (a credit card) or something you *know* (a PIN), but something you *are* (your fingerprints, palm prints or retinas). Those unique biological identifiers are electronically read and converted to a string of ones and zeros and sent to an authenticator. There the information is compared with the string of numbers on file in the authenticator database.

And there is the weakness, for the risk of transmission interception or database theft remains unchanged. If a credit card number can be stolen, then the sequence of numbers that make up a fingerprint can be stolen just as easily. It might take thieves a little time to gear up to this new challenge, but gear up they will. Undoubtedly, in the years to come, news reports about fingerprint, palm print and retinal eye scan thefts will be just as common as credit card number thefts are today.

So, does that mean biometrics will leave us right where we are? No, they will leave us in a worse place. Think about it: If you lose your credit or ATM card, the issuing company can replace it. If your PIN becomes compromised, the bank can give you a new one. Even a Social Security number can be replaced. But what do you do if someone steals your retina scans? Who is going to give you new eyeballs?

What will stop thieves from electronically sending your stolen fingerprints to your bank to confirm that you really do want to clean out your bank account through an ATM in Islamabad? What will you do when your digitized fingerprints wind up on a government No Fly list? If you think it takes forever to board a plane now, wait until every law enforcement agency in the free world has your fingerprints on file as a suspected thief or, worse, a terrorist.

The reality is that biometrics are a feel-good measure designed to give people the false impression that they are more secure than they were before, when in fact they are more at risk. Identity theft victims report that it can take three, five or more years to clean up the financial mess left after a stolen Social Security number. How long will it take to clean up a stolen fingerprint?

Where does this leave the CIO? Not in a very comfortable position. While the threat of information theft is unchanged, the risk of inflicting unnecessary hardship on employees, customers and citizens is very real. In the coming years, we will see how many CIOs stand up to the unenviable task of confronting the uncomfortable facts and how many surrender to spreading false hope to a fearful constituency.

## Latest threat vector: Our mobile devices

October 26, 2009 - 2:43 P.M.

As the "security guy" for my entire adult life, I've gotten a wide variety of security questions from friends, family, colleagues, travel companions and more. I tend to use these questions in the aggregate to spot trends in the wild. Far and away the most frequent questions are now focused on our mobile devices -- specifically how they are being used to spy on their owners and reveal our most intimate of secrets.

In the run up to the last Olympics I had lots of questions from law enforcement and intelligence communities around the world about the risks to corporate executives preparing to travel to the games. At that time, there were several known attack vectors being used to exploit traveler's smart phones, regardless of brand. These were well organized and highly focused attacks against high value targets -- people expected to have significant confidential data stored in their e-mail, contact lists, text messages, photo cache, document store and the deleted files. The information gained through these types of attacks could be used for corporate, political, or personal leverage.

Now, however, I'm getting similar questions from a very different and much wider group of folks. Rather than just the government calling, now corporate executives and regular folks who are going through some sort of breakup -- personal or professional -- are getting hit with very similar attacks, and it's hurting them much more deeply than a simple blue screen of death. Their innermost secrets are being revealed, and used against them in the most personal of ways.

There are three basic types of common attack vectors on smart phones: direct entry, via a download, or through Bluetooth.

A direct entry attack means that someone has physical control of your phone for a few minutes and they load spyware on it (yes, there is a lot of spyware on the market specifically for mobile devices). Think about how often you leave your phone sitting on your desk, your night stand, or a table at the coffee shop. If you start treating that phone more like your Visa card, you're a lot less likely to be attacked in this direct way. If you're going through a breakup of some sort, it takes a conscious effort to keep your 'trusted' partner from gaining access while you're at lunch, asleep, or at play. Once installed, mobile spyware can listen in on your calls, copy and transmit your e-mails and texts, and even steal your photos. Most people find out only when others seem to know information they really shouldn't. This is the most common form (other than from well-funded intelligence-gathering agencies) of mobile attack, and is easily spotted (more on how to spot mobile spyware in an upcoming post) and removed with several good commercially available programs -- once you know to look for it.

The next most common form of this attack is through a program download. Blackberry users who are addicted to Brick Breaker should watch out for add-ons (a new Blackberry patch is coming shortly). Similarly, everyone who downloads games should realize they might also carry a spyware payload along with the game. Whenever you download a program to your smart phone from a previously unknown website, email, or text link (and no, a Google hit does not a trusted relationship make), you run the risk of adding spyware to your mobile device. These programs perform basically the same spying functions as found with a direct entry attack, but they are generally not targeted at you specifically, as it's really up to you to find and download the program in the first place. This is a growing form of information harvesting, with corporate data and identity theft being the big targets.

Finally, it is now possible to attack many smart phones simply by standing within a few feet of them for a minute or two. That's how long it takes for programs to guess their way into your 4 digit Bluetooth key (even faster if you left it set to 0000 like most of the human population). Once in, the most common attack is to load a new 'blank' record into your contact list along with some code that can remotely activate your microphone. With that in place, you can be eavesdropped on whenever and wherever -- even when you don't think you're using the phone. This attack is the hardest to accomplish, and still the least common, but it has now spread beyond the foreign intelligence and organized crime world into regular, old fashioned corporate and personal espionage. If you use a Bluetooth earpiece, you're susceptible to this attack.

We now rely on our smart phones for all aspects of our lives. They contain most of our secrets, yet we still don't take them seriously when it comes to security. Everything that happens on our desktops is quickly moving to our smartphones, and that includes the bad with the good. Judging from the calls I've been getting, it's time to protect our smart phones as well as or

better than the rest of our computers.

## **Gartner: IT already has its head in the cloud**

October 20, 2009 - 12:20 P.M.

All the world's a cloud, it seems, at Gartner's IT Expo this week - and attendees at the show, who arrived in strength this week, are listening. More than 5,000 people are here, everyone's focused on business, not the economy, and cloud computing is clearly on the radar.

This morning Gartner released its list of most strategic technologies for IT in 2010. Number one: Cloud computing, which everyone agrees is still far from mature. Cloud's impact is infused into discussions in sessions on many topics, and several focus explicitly on private and public cloud architectures.

Gartner defines cloud computing broadly as "A style of computing where scalable and elastic IT-related capabilities are provided 'as a service' to customers using Internet Technologies." In other words, on demand compute services, delivered from shared system infrastructure (storage, processor), application infrastructure (databases, middleware) or full blown applications, as a metered service.

Gartner contends that enterprises are unwittingly building the foundations for their own private cloud services as they continue to build out virtual infrastructure. As such in choosing a vendor they're committing themselves to a path that may have unforeseen consequences down the road. Most organizations can't see past the immediate value - consolidation and management efficiencies, and make decisions on that alone, says analyst Tom Bittman. As use models evolve and resources are pooled, tools such as live migration and Distributed Resource Scheduler are providing the substrate on which cloud computing services will be delivered, he says.

His advice: Keep that in mind as you choose virtualization options, since you'll be locked into methodologies and tool sets down the road, when it comes time to consider implementing a private cloud.

Eventually, IT will become a service provider, analyst Carl Claunch. But Gartner's infamous "troth of disillusionment" still looms. According to Gartner's own predictions, mainstream adoption of the technology is still several years away.

## **Report: Employee Holiday Shopping Will Strain Security**

### ***Annual survey from ISACA finds productivity losses, information security risks are at stake when employees use work devices for shopping***

By [Joan Goodchild](#), Senior Editor

October 21, 2009 — [CSO](#) —

Despite a lagging economy, many workers will shop online while at work this coming holiday season, according to a survey conducted on behalf of ISACA, a nonprofit association of information technology (IT) professionals. The second annual "Shopping on the Job: Online Holiday Shopping and Workplace Internet Safety" survey found that fully half of those surveyed plan to use their company's computer to shop, putting a strain on employers' systems and potentially compromising an organizations sensitive information and security.

Among those polled, the mean amount of time employees planned to spend shopping online was 14.4 hours, nearly two full working days. One in 10 plans to spend at least 30 hours shopping online at work. Most planned to do their shopping in early to mid-December.

"The potential danger of shopping online is that it can open the door to viruses, spam and phishing attacks that invade the workplace and cost enterprises thousands per employee in lost productivity and potentially millions in destruction or compromise of corporate data," ISACA officials said in a statement on the findings.

ISACA also noted that employees who shop online using a work computer are also likely to engage in other high-risk behaviors. Survey participants also bank online (51 percent), click on e-mail links redirecting them to shopping sites (40 percent) and click on links from social network sites (15 percent). Yet nearly one in five says they are not concerned that their online shopping habits may affect the safety of their organization's IT infrastructure.

The survey also found that more than one in 10 Americans who use a mobile work device such as a BlackBerry or iPhone plan to use it for holiday shopping, further opening the door for additional security issues and exposure to data loss for a company, according to ISACA.

ISACA officials also found there is a large reality gap between employees and the IT department. A separate ISACA survey of more than 1,500 IT professionals who are ISACA members conducted during the same time period revealed close to half (48 percent) of those in IT believe employees will spend just over one work day, or nine hours, shopping online from a work computer. One in four IT professionals estimated that their company will lose US \$15,000 or more per employee in productivity during this year's holiday season.

## Companies Seek Social Networking's promise, Find Peril Instead

***Seventh Annual Global Information Security Survey: Social networking sites such as Twitter, Facebook and LinkedIn enhance collaboration but also make it easier than ever for your employees to share customer data and company secrets with outsiders.***

By [Bill Brenner](#), Senior Editor

October 26, 2009 — [CSO](#) —

Social networking sites such as [Twitter, Facebook and LinkedIn](#) enhance collaboration and help your company connect with customers, but they also make it [easier than ever for your employees to share customer data and company secrets](#) with outsiders.

That's one of the big takeaways from the seventh-annual Global Information Security survey, which CSO and CIO magazines conducted with PricewaterhouseCoopers earlier this year. Some 7,200 business and technology executives worldwide responded from a variety of industries, including government, health care, financial services and retail.

### **A hazardous way of life**

In less than two years, social networking has gone from an abstract curiosity to a way of life for many people. When someone updates their status on Twitter, Facebook or LinkedIn, they might do it at work by day or on company-owned laptops from home at night.

What gives IT executives heartburn is the ease with which users could share customer data or sensitive company activities while they're telling you what they're having for lunch. Cyberoutlaws know this and [use social networks to launch phishing scams](#). In one popular attack, they send their victims messages that appear to be coming from a Facebook friend. The "friend" may send along a URL they insist you check out. It may be pitched as a news story about Michael Jackson's death or a list of stock tips. In reality, the link takes the victim to a shady website that automatically drops malware onto the computer. The malware goes off in search of any valuable data stored on the computer or wider company network, be it customer credit card numbers or the secret recipe for a new cancer-fighting drug.

It's no surprise, then, that every IT leader surveyed admitted they fear social-engineering-based attacks. Forty-five percent specifically fear the phishing [attacks against Web 2.0 applications](#).

Nevertheless, for many company executives, [blocking social networking is out of the question](#) because of its potential business benefits. Companies now clamor to get their messages out through these sites, so the challenge for CSOs is to find the right balance between security and usability.

"People are still incredibly naïve about how much they should share with others, and we have to do a better job educating them about what is and isn't appropriate to share," says H. Frank Cervone, vice chancellor of information services with Purdue University Calumet. "We have to do a better job of enhancing our understanding of what internal organization information should not be shared."

But in a university setting, it's critical to engage people through social media, Cervone adds. Even in the commercial sector, he doesn't see how organizations can avoid it.

And yet this year -- the first in which we asked respondents about social media, only 23 percent said their security efforts now include provisions to defend Web 2.0 technologies and control what can be posted on social networking sites.

### **Security dangers on the radar**

One positive sign: Every year, more companies dedicate staff to monitoring how employees use online assets -- 57 percent this year compared to 50 percent last year and 40 percent in 2006. Thirty-six percent of respondents monitor what employees are posting to external blogs and social networking sites.

To prevent sensitive information from escaping, 65 percent of companies use Web content filters to keep data behind the firewall, and 62 percent make sure they are using the most secure version of whichever browser they choose. Forty percent said that when they evaluate security products, support and compatibility for Web 2.0 is essential.

Unfortunately, social networking insecurity isn't something one can fix with just technology, says Mark Lobel, a partner in the security practice at PricewaterhouseCoopers.

"The problems are cultural, not technological. How do you educate people to use these sites intelligently?" he asks. "Historically, security people have come up from the tech path, not the sociologist path. So we have a long way to go in finding the right security balance."

Guy Pace, security administrator with the Washington State Board for Community and Technical Colleges, says his organization takes many of the precautions described above. But he agrees with Lobel that the true battleground is one of office culture, not technology. "The most effective mitigation here is user education and creative, effective security awareness programs," he says.

## **4 Tips for Writing a Great Social Media Security Policy**

***Think creating policies to deal with Facebook and Twitter are a security headache? Security researchers at IANS think these policies actually provide security departments with a great opportunity.***

By [Joan Goodchild](#), Senior Editor

October 21, 2009 — [CSO](#) —

Facebook now claims 300 million active users. And Twitter, the micro-blogging site that was almost unheard of at the beginning of 2008, is now one of the internet's 50 most popular sites, according to Alexa Internet Inc.'s web traffic statistics.

Naturally, social media growth has also been seen in the workplace, both with regard to employee use as well as functioning as a communication and/or marketing tool for some companies. And according to a survey recently conducted by IANS, a Boston-based research company that focuses on information security, regulatory compliance and IT risk management, the number of enterprises with a social media policy in place has jumped dramatically, too, in just twelve months.

Jack Phillips, IANS co-founder and CEO, said when IANS conducted the same survey in 2008, the majority of respondents did not have a social media policy.

"They really hadn't done the hard thinking," said Phillips. "But then jumping forward to 2009 we saw about a third of the audience now has something in place and another large percentage is considering these kinds of policies."

Specifically, just under ten percent of respondent enterprises said their social media policy was fully implemented and communicated in 2008. That jumped to 34 percent in 2009, with another third responding that they had either created or implemented a policy for social media use. The take away, according to Phillips, is that social media is front and center now in organizations and the discussion is taking place not only among the security team, but within marketing, sales, human resources and even executives.

Phillips believes this is an opportunity for security folks to raise their profile and take part in an important issue from its inception. He shared with CSO four things he thinks organizations should consider when putting together policies and practices for use of Facebook, Twitter, Linked In and other social media within an organization.

### **1. Don't start from scratch**

The media landscape is so dynamic that if you create policy for today's hot technology, tomorrow it will be obscure. Instead, said Phillips, use this as an opportunity to draw attention to existing policies.

"Most purists will say: This stuff isn't really new. It should be part of our HR and acceptable use policies," said Phillips. "The same sort of norms apply to this new world that has applied to the world before today."

Phillips noted most of the organizations IANS polled with a social media policy already in place said they had not named specific medias because of changing pace of new media.

"It's Twitter today, but it may be something else tomorrow," he said.

### **2. Use social media policies to raise security awareness**

"This issue is an opportunity for info sec leaders to refocus attention on information security and risk management, said Phillips.

IANS is dispelling what Phillips says is age-old advice for enterprises when it comes to adapting to change. For instance, when compliance regulations came into play, savvy security teams were able to create new policies to comply, while also letting employees know why they were important. Same holds true this time around, said Phillips.

"We are finding some innovative awareness tactics that focus on these technologies because they are front and center. A Twitter campaign, or a Facebook campaign, a Linked In campaign, can all have real impact in terms of receptivity. The percentages are so low in terms of success of awareness campaigns, this is an opportunity to jump in."

### **3. Use social media access to raise security's positive profile within the organization**

While the initial security reaction to new media is often to block, Phillips said most organization now need to consider that not only may allowing access be necessary, but also useful from an info sec perspective.

"The advice we have given is, instead of just knee-jerk blocking everything, we find that this as an opportunity to record usage and activity among the employee base," said Phillips. "When the original data-loss-protection technologies were introduced, they were not in blocking mode, but in monitoring mode."

Phillips believes the new technology of social media gives information security what he calls "an interesting opportunity" to see how critical these technologies are to the enterprise.

"That kind of information is quite useful to other functions of the enterprise," he said "Sales, marketing, HR are all going to be interested and that raises information security's profile among management."

#### **4. Be prepared for the next phase**

As social media platforms come and go, some will ultimately become commonplace and integral to an enterprise. While creating entire new policies around social media doesn't make sense right now, at some point, said Phillips, it will become necessary for policies to be more specific. As it stands now, he said, he finds his clients are more comfortable with some mediums and with others; not so much. Most organizations find Linked In to be the most controllable and with the least potential for damage. But Facebook, with its security vulnerabilities, and the nature of its content, still makes many uncomfortable. Particularly, said Phillips, because many employees are not respecting that line between personal and enterprise.

"Because these technologies are so different, it is at some point we expect policies are going to have to get granular," he said. "Our sense is high-performing teams will have to create unique Facebook, Twitter, Linked In and Google Docs policies. And they are going to have to get that granular about what is appropriate and inappropriate with each tool.

"We will end up with an open environment, but we will end up with some asterisks that say, it's open, but not 100 percent open. For example, some might say: 'It is not appropriate to use the company's name on your Facebook profile.'

## **Opinion: Twitter, Facebook security depends on vigilant developers, sensible users**

**By John Viega**

October 19, 2009 06:00 AM ET

Computerworld - There's been a lot of fuss in the press recently about Web 2.0 security. In the past year, [Facebook](#) and Twitter both have had serious problems that have made some waves among the technically savvy.

People are starting to wonder if we, as an industry, just don't know anything about securing Web 2.0 applications. There's a bit of truth to that, but mostly the software development industry is just plain bad at creating secure software of any kind.

Part of the problem is that developers generally aren't security experts. Even in organizations where all developers receive software security training, it's rare for them to remember anything significant. Developers and development organizations are thinking about features, first and foremost. When it comes to security, they just go through the motions. The ability to log in with a password is a feature. SSL support is a feature. It's unusual for anybody to pay attention to doing things right -- until they get bitten publicly a few times.

Take Twitter, for example. The site has had a litany of security glitches over the past year, including cross-site scripting problems. Until it got burned, it wasn't so much that Twitter thought it didn't have to worry about security. It was more that it thought its people were smart enough to address the problem as a matter of course.

After a couple incidents proved that the company didn't actually have it together, the Twitter guys wanted to do the right thing. They didn't want a bad reputation for security. As a result, they've brought in outside consultants to look for security flaws in their code. And they've been trying hard to recruit a full-time person to take ownership of product security. I expect that Twitter, like many other companies, is finding that it's extremely difficult to find high-caliber software security talent.

But if you take a closer look at Twitter, a lot of its problems aren't necessarily problems in the software platform (although some of them definitely are). For example, it isn't uncommon for bad guys to [hack into a celebrity's](#)

[Twitter account](#) and make fake posts or [hack into the accounts of Twitter employees](#). Sure, the software platform can try to address those threats, but a big part of the problem is the operational security.

Twitter's employees need to make sure they are [selecting strong passwords](#). And they should be doing as much as possible to encourage their users to do the same.

To some degree, Twitter is already doing these things. But even if the company makes a big effort to encourage responsible behavior among its employees and customers, people are still going to get hacked.

Some people may use the same password everywhere, including on hacked sites. Others may try hard but still choose passwords that can't withstand guessing attacks. And still others may be victimized by phishing scams, tricked into typing their credentials into a phony Web form. This has been a big concern with Twitter, where there are lots of add-on services that ask for your credentials, including Bit.ly, Mr. Tweet and so on.

The truth is, most security breaches require the end user to take -- or fail to take -- some kind of action.

There are certainly issues with AJAX and cloud-centric application models that leave Web 2.0 applications open to attack. That's to be expected -- security always lags a bit behind innovation. But at the end of the day, those issues pale in comparison to the threat users pose to themselves. People are largely very trusting, and bad guys are always going to be able to take advantage of that trust. That will be true even if the day comes when our software has no holes in it and our software vendors are perfect citizens.

## Baited and duped on Facebook

### How smart companies are protecting employees from scammers and creating usage policies that work

**By Mary Brandel**

October 19, 2009 06:00 AM ET

Computerworld - When [CIO Will Weider](#) encouraged employees at [Ministry Health Care and Affinity Health System](#) in Wisconsin to use Facebook to spread the word about new programs and successful projects, he was surprised at the result: Few did so.

"I went in there thinking, 'We've turned these people loose; we'll have 10,000 marketers out there,' " Weider says. But the Ministry Health workforce, it turned out, had been well trained to protect sensitive data, and without explicit guidance on what they could say, their first reaction was to share nothing.

"We've stressed the importance of data security with our employees, particularly when it comes to patient privacy, and it's kept them from sharing all the great things about work on Facebook," Weider says.

That's a good problem to have. Many fear that the popularity of social networking -- among individuals as well as organizations -- will precipitate an increase in social engineering attacks that could result in security breaches that expose corporate data or damage a company's reputation.

Indeed, social media such as Facebook, LinkedIn, Twitter, online forums and blogs create a perfect opportunity for an attacker, mixing the anonymity of the Web, easy and direct access to hundreds of millions of people, and an unprecedented amount of personal information.

Consider that before social networking existed, criminals had to make a real effort to engage victims, says Adriel Desautels, chief technology officer at Netragard LLC, a security service provider that performs vulnerability assessments and penetration tests for clients. Often, the payoff wasn't worth it. But with social media, it's easy to hit a large number of targets quickly and effectively, he says.

"Instead of having to fool that one particular person, they can befriend a whole bunch of people," Desautels says. "They can post a URL on their wall, and one of those people is likely to click on it."

## Approaching Storm

But while executives seem to grasp the potential threats of social networking, only a slim majority of organizations seem to feel the need to do something about it. In an exclusive September 2009 *Computerworld* survey, 53% of the 120 IT professionals polled reported that their organizations have a social media usage policy, while 41% said they don't and 6% said they weren't aware of such a policy.

And in a [July 2009 poll](#) by advertising agency Russell Herder and law firm [Ethos Business Law](#), both based in Minneapolis, 81% of the 438 respondents said they have concerns about social media and its implications for both corporate security and reputation management. However, only one in three said that they have implemented social media guidelines, and only 10% said that they have undertaken related employee training.

A [Deloitte LLP survey](#) echoes those results. Only 15% of 500 executives polled said that the risks of social media are being addressed in the boardroom, although 58% said they agree that it's important to do so. But even those that do have policies may not effectively communicate them. Of 2,008 employees that Deloitte surveyed, 26% said their employers had guidelines regarding what they could say online, 24% said they didn't know if their employers had such a policy, and 11% said that there was a policy but they didn't know what it was.

Not that a policy covers every base, says [Ira Winkler](#), a *Computerworld.com* columnist as well as the author of [Spies Among Us](#) (Wiley, 2005) and president of [Internet Security Advisors Group](#), an IT security firm whose services include espionage simulations. But certainly a hands-off approach is no longer an option, nor is [blocking the use of social sites at work](#).

"Too many companies want to say, 'That's your private life, so I won't bother you,' " he says. "But people's insecure behavior at home proliferates insecurity in the business."

The concern isn't just that employees will divulge sensitive data outright. It's that they'll reveal enough information about themselves or their workplaces -- either in one profile or distributed over several -- to enable an imposter to assess their personalities and gain their trust, figure out responses to their password-reset questions or convincingly pretend to be a co-worker, business partner or customer

"Little pieces of information put together the big picture," Winkler says. Valuable tidbits include birth dates; the names of children, pets and best friends; facts about employers or comments about how projects at work are going; lists of hobbies; updates about vacations or life-changing events; and links to friends. The information is simple to find, either by using reconnaissance tools such as those available at sites like [Maltego.com](#) and [Pipl.com](#) or by simply doing searches on Facebook or LinkedIn.

When Netragard conducts penetration tests, it finds all the people on Facebook who work at a particular company and extracts data from their walls, posts and profiles. It pulls this information into a database and analyzes the results to assess things like the company's culture, whether someone will respond quickly to a request or how seriously security personnel take their jobs. From a simple comment about a Java register misbehaving again, Desautels says, Netragard can create an attack that looks like something the company won't notice or care about.

The bad news, Desautels says, is that there's no sure way to protect your company against social engineering threats. After all, the vulnerability stems from the natural human tendency to trust other people. However, there are measures you can take to reduce the risk that a hacker will succeed. A good place to start is with a [social media policy](#).

Such policies range from strict to very liberal. For instance, [sports broadcaster ESPN Inc.'s guidelines](#) ban employees from setting up personal Web sites and blogs that contain sports content and requires workers to receive permission before engaging in any form of social networking dealing with sports.

Meanwhile, Ministry Health encourages employees to discuss positive work events and even to offer constructive criticism of their employer. However, it also has [guidelines](#) that, for example, prohibit employees from sharing patient information online under any circumstances, Weider says.

One basic but controversial policy question is whether to allow workers to mention their employer by name in their online profiles or in social networking forums. According to Desautels, prohibiting those practices is the best way to defend against social engineering threats.

If you're really concerned, you could consider restricting employees from providing their office e-mail addresses and identifying the geographic region in which they work, says Terry Gudaitis, cyberintelligence director at IT security firm [Cyveillance](#). Even then, it's possible that a friend's comment or other conversations visible on an employee's profile could reveal employer information. In such a situation, it's up to the profile owner to monitor and delete those references, she says.

Similarly, Winkler suggests restricting employees from mentioning business developments on their profiles. What if, for example, a researcher discusses his lack of progress on a project or, perhaps even more revealing, a major breakthrough? Or if a salesperson tweets that she's meeting friends because she just won a big account? Combined with other information, such as names recently added to a salesperson's friend list, such tidbits can reveal quite a bit, Winkler says.

"This stuff used to be under lock and key in a private diary," Gudaitis agrees. "The amount of disclosure on every level -- business dealings, trade secrets, classified information and personal information -- is enormously high." Also alarming, she says, are employees who tweet during meetings about what's happening and even who's in attendance.

Of course, policies banning the mention of employers would take companies out of the [marketing-on-social-media game](#). But Desautels cautions against that type of marketing anyway. "You'd be opening your customers to an entire world of potential hurt via phishing and other types of attacks," he says in his blog.

Weider, on the other hand, says not using social media for marketing is unthinkable. "Why don't we just stop publishing our phone numbers so people can't get into our voice-mail system, or lock our doors so the patients can't get in?" he says.

The way to avoid possible exposure, says Weider, is to establish clear data-security policies and offer employees ongoing training. That training could touch on ways to tighten the security settings on sites like Facebook. According to the Web site [NextAdvisor.com](#), which compares online services, Facebook users should fine-tune who will have access to specific aspects of their profiles and posts using the "My Privacy" section of the site.

### **Not Too 'Friend'-ly**

Companies may also want to advise employees to not accept every friend offer that comes along. "In a lot of cases, people say yes to anyone who pops up," says Gudaitis. "But then they're vulnerable to whoever those people may be." Better to be conservative, she says, and approve only business acquaintances or old college buddies or family members.

To be even more cautious, NextAdvisor says, you should even verify whether a friend request is from the person it appears to be from, by sending him an e-mail or calling him. "It is easy for someone to set up a phony profile under the name of someone you know and trust in order to extract additional information from you," the site says.

Employees should also be aware that just because social networking sites ask them for personal information such as their birth date and phone numbers, it doesn't mean they need to provide it. In a poll of Facebook users that NextAdvisor conducted recently, 27% of respondents said that they listed their full name, date of birth, phone number and e-mail address in their profiles, and another 8% said that they included their street address as well.

"Your real friends and associates will likely already know this information, so including it on your profile will only increase your risk of being victimized by identity thieves," the site says.

Of course, hackers can collect that information even if you don't provide it all in one place. To guard against that, Gudaitis suggests varying your screen name.

Imagine, she says, if a hacker were able to track a specific systems administrator's or help desk technician's every move online, gathering information from message boards and forums, because the victim used the same screen name everywhere. "If I were an adversary, I could start to link all that information and even chat them up to better understand their network and system architecture," she says. "If we looked up every post someone had . . . we could put the puzzle pieces together."

Companies can also look inward at some of their own practices to close social engineering security gaps. In addition to advising employees to choose password-reset challenge questions that can't be answered through research, you could also follow [Google Inc.](#)'s lead and send password information to employees' cell phones instead of their e-mail addresses.

Hiring practices are another area in which security can be tightened. Winkler suggests screening the social networking habits of job candidates not just for stereotypical areas of concern, such as amoral behavior, but also for how active they are in social media and how likely they are to do things like expose personal information and voice extreme political views.

Perhaps most key, says Desautels, is designing your infrastructure and managing your sensitive data with an eye toward minimizing damage in the event of an intrusion. He stresses the importance of using encryption, recording and logging network activity, classifying data and putting your most sensitive data in a zone that can't be reached through the network. With a properly designed infrastructure, "you can keep a successful penetration from being successful in stealing your data," he says. "Just because they break in, they don't have to put you out of business."

In the end, it's really about finding a balanced way to leverage social media while minimizing risk, Weider says. For him, social engineering threats are certainly among his top 10 concerns, but they're nowhere near No. 1. "It's something I take seriously," he says, "but I do think there's a balance between reasonable risk and the likelihood of these various things taking place."

## Facial-recognition system can guess your age

**By Ellen Messmer**

October 21, 2009 01:11 PM ET

*Network World* - ORLANDO -- Those advertising in public places would like to know the age and gender of those viewing their ads to see if they're hitting the right demographic. An experimental facial-recognition system developed by NEC does a pretty good job of delivering that information.

The NEC Next Generation Digital Signage Solution, on display on the exhibit floor at the Gartner Symposium ITExpo this week, is a facial-recognition system with a camera that watches individuals, zeroing in on their faces to instantly determine age and gender.

It doesn't store the image of a person, but gathers age and gender data. The goal, says Takeshi Yamamoto, vice president of strategic alliances in the NEC IT Solutions Group, is to be able to give advertisers in public venues, such as airports or shopping places, what they really crave to know.

"Companies running digital ads have no idea of what people are around it, you'd have to have someone there physically counting them today," Yamamoto says. The NEC facial-recognition system focuses in on passers-by, guessing age and gender with surprising accuracy. Age might be expressed as falling within a 10-year range, for example (and in the case of this reporter, it was accurate, though it missed the mark by a couple of years of another passer-by checking it out).

According to an NEC engineer, the longer you stay in front of the camera, the more accurate it gets, and you can see the data about you floating above the image of your head like a virtual halo.

Yamamoto says the age/gender data about those viewing advertising could be stored and retrieved later or sent electronically, adding the NEC facial-recognition is being tested in Japan by Fuji TV.

# U.S. gov't cybersecurity spending to grow significantly, study says

By Grant Gross

October 23, 2009 01:59 PM ET

IDG News Service - U.S. government spending on cybersecurity will grow at a compound rate of 8.1 percent a year between 2009 and 2014, outpacing general IT spending, according to the government analyst firm Input.

Spending on vendor-supplied information security products and services will increase from \$7.9 billion in 2009 to \$11.7 billion in 2014, Input predicted. General IT spending by the U.S. government will increase by 3.5% a year during the same time frame, said Kevin Plexico, Input's senior vice president of research and analysis.

Even if those increases happen, there will be questions about whether the U.S. government is doing enough, he said. "The challenge is, how good is good enough?" Plexico added. "There's no authority or organization that can tell you when you've done enough and are 'secure.'"

A number of factors will drive information security spending, Plexico said. First, President Obama and lawmakers have paid significant attention to cybersecurity this year, with several bills focused on improving cybersecurity in the U.S. government or private organizations.

In addition, cyberattacks on the federal government have increased substantially in recent years, and attacks are becoming more sophisticated, according to many cybersecurity experts.

"It's a recognition across parties and the administration and Congress that more needs to be done within the federal government," Plexico said. "With that comes broad support for extraordinary levels of funding."

Plexico expects a "higher bar" to be set for federal cybersecurity when Obama appoints his long-awaited cybersecurity coordinator. In May, Obama announced a new direction for federal cybersecurity efforts and promised to appoint a cybersecurity coordinator in the White House.

Vendors that want to market their information security products to federal agencies should be aware of some key trends, Plexico said. The U.S. government is moving toward consolidation of cybersecurity efforts, with a few larger agencies taking over the information security roles at smaller agencies, he said,

"You need to be paying attention to where those consolidation and centralization centers are," he said.

In addition, much of the federal government's cybersecurity focus will be real-time monitoring and control of computer networks, Plexico predicted. He sees less emphasis in the future on audits to identify breaches after they happen.

"Agencies are really investing in technology that helps them identify threats as soon as they happen, and even anticipate where those threats are going to come from," he said.

[Input](#) bases its predictions on economic forecasts, historical analysis of government spending, past budgets, Obama's 2010 budget request and other information.

# IT Security Outsourcing in Decline; Companies Do More In-house

***Seventh Annual Global Information Security Survey: Companies that once outsourced many IT security controls have opted to do more in-house. A look at what caused the shift.***

By [Bill Brenner](#), Senior Editor

October 28, 2009 — [CSO](#) —

The worst economic recession in decades has compelled more companies to spend less on outsourced security services and do more in-house, according to the seventh-annual Global Information Security survey, which CSO and CIO magazines conducted with PricewaterhouseCoopers earlier this year.

Some 7,200 business and technology executives worldwide responded from a variety of industries, including government, health care, financial services and retail.

A few years ago, technology analysts were predicting unlimited growth for [managed security service providers \(MSSPs\)](#). Many companies then viewed security as a foreign concept, but laws such as [Sarbanes-Oxley](#), the [Health Insurance Portability and Accountability Act \(HIPAA\)](#) and the Gramm-Leach-Bliley Act (affecting financial services) were forcing them to address intrusion defense, patch management, encryption and log management. Convinced they couldn't do it on their own, companies chose outsourcers to do it for them. Gartner estimated the MSSP market in North America alone would reach \$900 million in 2004 and that it would grow another 18 percent by 2008.

Then came the [economic tsunami, which appears to have cast a shadow over outsourcing plans](#) even though security budgets are holding steady. Although 31 percent of respondents this year are relying on outsiders to help them manage day-to-day security functions, only 18 percent said they plan to make security outsourcing a priority in the next 12 months.

When it comes to specific functions, the shift has already begun. Last year, 30 percent of respondents said they were outsourcing management of application firewalls, compared to 16 percent today. Respondents cited similar reductions in outsourcing of network and end-user firewalls. Companies have also cut back on outsourcing encryption management and patch management.

At the same time, more companies are spending money on these and other security functions. Sixty-nine percent said they're budgeting for application firewalls, up slightly compared to the past two years. Meanwhile, more than half of respondents said they are investing in encryption for laptops and other computing devices.

The results surprise Mark Lobel, a partner in the security practice at PricewaterhouseCoopers. "When you think about it logically, some IT organizations have the resources and maturity to manage their operating systems and patches, but many don't," he observes. "Hopefully, the numbers simply mean IT shops have grown more mature in their security understanding."

Miguel Lopez, a Los Angeles-based IT security practitioner who has worked for such companies as MSC Software and Stamps.com, observed a stark trend toward less outsourcing while at MSC (he left the company earlier this year).

"The company was doing less and less outsourcing. It was mostly due to the economic conditions more than anything else," he says. "They were certainly looking to see where cost could be reduced or eliminated. I also hear from a few of my friends in other companies that the trend is toward doing more with internal staff."

Peter Hillier, director of IT security for CMA Holdings in Ottawa, believes there are three things driving the move toward more in-house security:

1. Organizations have become more adept at do-it-yourself security since first outsourcing, though, Hillier says, "they should have done that prior to outsourcing security the first time."

2. SIM/SIEM growth has been as good for the insourcer as it is for the outsourcer. "If you can do more with less, then why pay someone else to do it?" he asks.

3. Economy is a driver, as others have noted.

Charles Beard, SVP and chief information officer for Science Applications International Corp. (SAIC), says that no matter what drives security spending decisions, companies should understand their specific security strategies and where managed security providers can offer unique value. Smart business executives understand that they must maintain control of the big picture at all times, even if a third party is managing many of the levers. Keeping an eye on security service providers and the risks they are encountering is essential. "CIOs and security officers may outsource certain functions to various degrees, but they should never outsource their responsibility," Beard advises.

## The Curse of Cloud Security

***Seventh Annual Global Information Security Survey: Companies are clamoring for services in the cloud. But the biggest problem from a security perspective is that few understand what they're dealing with.***

By [Bill Brenner](#), Senior Editor

October 27, 2009 — [CSO](#) —

Virtualization and cloud computing let you simplify your physical IT infrastructure and cut overhead costs, but you've only just begun to see the security risks involved.

Putting more of your infrastructure in the cloud has left you vulnerable to hackers who have redoubled efforts to launch denial-of-service attacks against the likes of Google, Yahoo and other Internet-based service providers. A [massive Google outage](#) earlier this year illustrates the kind of disruptions cloud-dependent businesses can suffer.

That's one of the big takeaways from the seventh-annual Global Information Security survey, which CSO and CIO magazines conducted with PricewaterhouseCoopers earlier this year. Some 7,200 business and technology executives worldwide responded from a variety of industries, including government, health care, financial services and retail.

### **Jumping in, sans parachute**

Given the expense to maintain a physical IT infrastructure, the thought of replacing server rooms and haphazardly configured appliances with cloud services is simply too hard for many companies to resist. But rushing into the cloud without a security strategy is a recipe for risk. According to the survey, 43 percent of respondents are using cloud services such as software as a service or infrastructure as a service. Even more are investing in the virtualization technology that helps to enable cloud computing. Sixty-seven percent of respondents say they now use server, storage and other forms of IT asset virtualization. Among them, 48 percent actually believe their information security has improved, while 42 percent say their security is at about the same level. Only 10 percent say virtualization has created more security holes.

Security may well have improved for some, but experts like Chris Hoff, director of cloud and virtualization solutions at Cisco Systems, believe that both consumers and providers need to ensure they understand the risks associated with the technical, operational and organizational changes these technologies bring to bear.

"When you look at how people think of virtualization and what it means, the definition of virtualization is either very narrow -- that it's about server consolidation, virtualizing your applications and operating systems, and consolidating everything down to fewer physical boxes -- or it's about any number of other elements: client-side desktops, storage, networks, security," he says. "Then you add to the confusion with the concept of cloud computing, which is being pushed by Microsoft and a number of smaller, emerging companies. You're left scratching your head wondering what this means to you as a company. How does it impact your infrastructure?"

Fortunately, there's some evidence of companies proceeding with caution.

One example is Atmos Energy, which is using Salesforce.com to speed its response time to customers and help the marketing department manage a growing pool of clients, according to CIO Rich Gius. The endeavor is successful thus far, so Gius is investigating the viability of running company e-mail in the cloud. "It would help us address the growing challenge where e-mail-enabled mobile devices like BlackBerrys are proliferating widely among the workforce," he says. But he's not ready to take such a big step because the risks, including security, remain hard to pin down. One example of the disruption that cloud-dependent companies can experience came in May, when search giant Google—whose content accounts for 5 percent of all Internet traffic—suffered a massive outage. When it went down, many companies that have come to rely on its cloud-based business applications (such as e-mail) were dead in the water.

The outage wasn't caused by hackers, but there are signs that cybercriminals are exploring ways to exploit the cloud for malicious purposes. On the heels of the outage, attackers added insult to injury by flooding Google search results with malicious links, prompting the U.S. Computer Emergency Response Team (U.S. CERT) to issue a warning about potential dangers to cloud-based service sites.

The attack poisoned several thousand legitimate websites by exploiting known flaws in Adobe software to install a malicious program on victims' machines, U.S. CERT says. The program would then steal FTP login credentials from victims and use the information to spread itself further. It also hijacked the victim's browser, replacing Google search results with links chosen by the attackers. Although the victimized sites were not specifically those offering cloud-based services, similar schemes could be directed at cloud services providers.

IT organizations often make an attacker's job easier by configuring physical and cloud-based IT assets so poorly that easy-to-find-and-exploit flaws are left behind. Asked about the potential vulnerabilities in their virtualized environments, 36 percent cited misconfiguration and poor implementation, and 51 percent cited a lack of adequately trained IT staff (whose lack of knowledge leads to configuration glitches). In fact, 22 percent of respondents cited inadequate training, along with insufficient auditing (to uncover vulnerabilities) to be the greatest security risk to their company's cloud computing strategy.

It's this awareness that makes Atmos Energy's Gius proceed with caution. "We have no CSO. If we were a financial services firm it might be a different story, or if we had a huge head count," Gius says. "But we are a small-to-medium-sized company, and the staff limitations make these kinds of implementations more difficult."

Even with the right resources, security in the cloud is a matter of managing a variety of risks across multiple platforms. There's no single cloud. Rather, "there are many clouds, they're not federated, they don't natively interoperate at the application layer and they're all mostly proprietary in their platform and operation," Hoff says. "The notion that we're all running out to put our content and apps in some common [and secure] repository on someone else's infrastructure is unrealistic."

Mark Lobel, a partner in the security practice at PricewaterhouseCoopers, says perfect security is not possible. "You have to actively focus on the security controls while you are leaping to these services," he says. It's difficult for companies to turn back once they have let their data and applications loose because they are often quick to rid themselves of the hardware and skills they would need to bring the services back in-house.

"If you dive down a well without a rope, you may find the water you wanted, but you're not going to get out of the well without the rope," he says. "What if you have a breach and you need to leave the cloud? Can you get out if you have to?"

# Targeted attacks possible in the cloud, researchers warn

## Study shows how attackers can search, locate and attack specific targets in a cloud infrastructure

By Jaikumar Vijayan

October 28, 2009 11:43 AM ET

Computerworld - The use of virtualization by cloud service providers to host virtual machines belonging to multiple customers on a shared physical infrastructure is opening up fresh data leak risks, a research report warns.

The [report by four researchers](#) at MIT and the University of California at San Diego shows how vulnerabilities in cloud infrastructures could allow attackers to locate and eavesdrop on targeted virtual machines (VMs) anywhere in the cloud.

The attack described in the report was conducted against Amazon's Elastic Computer Cloud (EC2) service. But the vulnerabilities that enable it are generic and would likely affect other cloud providers, said Eran Tromer, a post-doctoral researcher at MIT's Computer Science and Artificial Intelligence Laboratory and one of the authors of the report. The report is scheduled to be presented at the Association for Computing Machinery (ACM) Conference on Computer and Communications Security next month.

The research raises questions about a fundamental assumption about cloud computing which says that data hosted in a cloud is relatively safe from targeted attacks because it's hard to know where in the cloud the data is located. The research also comes at a time when [concerns are high](#) about security and privacy issues related to cloud computing.

According to Tromer, the research shows that it is possible for attackers to identify the physical server on which a targeted virtual machine is hosted in the cloud. The attackers can then establish a rogue virtual machine on the same machine to go after the victim. A virtual machine is an operating environment created within another larger environment. A VM acts as a self-contained computer within a larger server, with virtual boundaries separating each VM from the other. Multiple VMs can run within one physical server.

The multi-stage attack starts with mapping the internal cloud infrastructure to locate the physical server hosting a target VM. Much of the information needed to glean the location of a target VM hosted in a cloud is contained in the IP address and domain name for that particular machine, Tromer said.

In the case of Amazon's EC2 infrastructure, for instance, analyzing the IP address of a VM can reveal details such as geographic region, as well as the availability zones or specific infrastructure segment it is on, he said.

The IP address also specifies an instance type, indicating the amount of computational power, memory and persistent storage that is available to the virtual machine. In addition, VMs located on the same physical server also tend to have IP addresses that are close to each other and are assigned at the same time.

The data gives attackers an idea of the parameters needed to establish a rogue VM on the same physical server as the target VM. They can then proceed to do this by instantiating new VMs until one is placed "co-resident with the target server," Tromer said.

Attackers can significantly boost their chances of achieving "co-residency" by launching a denial-of-service-attack against the target server and forcing it to expand capacity by adding new VMs. If the hackers simultaneously request new VMs of their own, their chances of getting one on the same physical machine as the target, is significantly increased.

According to Tromer, once an attacker gains access to the same physical server as the target VM, the attacker can monitor shared resources on the server to make highly educated inferences about the target VM.

For instance, by monitoring CPU and memory cache utilization on the shared server, an attacker could determine periods of high activity on the target servers, estimate high-traffic rates and even launch keystroke timing attacks to gather passwords and other data from the target server, Tromer said. These "side-channel

attacks" have proved highly successful in non-cloud contexts so there's no reason why they shouldn't work in a cloud environment, he said.

"The basic vulnerabilities, such as architectural side-channels, are inherent to virtualization technology used by all infrastructure-as-a-service cloud providers," Tromer said.

What the research shows is that until cloud providers can guarantee impermeable partitions between virtual machines on a single server, customers should try as much as possible to avoid sharing physical servers with others in the cloud, he added.

Amazon did not respond to requests for comment. But in comments made to the [MIT Technology Review](#), a spokesman said that Amazon has already rolled out safeguards to protect against the mapping techniques described in the research paper.

The company also refuted the notion that side-channel methods could be used to steal information from a VM on a shared physical server. In comments to the MIT Review, the Amazon spokesman said the researchers had tested such attacks in a "carefully controlled lab configuration that do not match the Amazon EC2 environment."

## **FBI: National data-breach law would help fight cybercrime**

### **Information-sharing by businesses could help the agency link attacks**

**By Grant Gross**

October 28, 2009 02:26 PM ET

IDG News Service - A federal law that would require businesses to report data breaches to potential victims could help law enforcement agencies fight the growth of cybercrime, a FBI official said Wednesday.

If U.S. businesses were required to share information about their data breaches, law enforcement agencies could link those attacks to others and potentially stop similar attacks at other organizations, said Jeffrey Troy, chief of the FBI's Cyber Criminal Section.

A data-breach notification bill "would help us tremendously, particularly in terms of efficiency in conducting investigations," Troy said during a cybersecurity discussion in Washington.

Companies need to think beyond their walls when dealing with cybersecurity issues, Troy said. "They have to recognize that the Internet has become a global platform for commerce," he said. "The people that are stealing information from you ... are going after the money."

Attacks used against one company will likely be used against other organizations, Troy said. "We're really looking forward to getting all this data," he said.

Some members of Congress have pushed for several years to pass data breach notification bills, without success. Although about 45 states have passed their own data-breach notification bills, Congress has yet to pass a federal law.

Data-breach notification will be part of a comprehensive cybersecurity bill that the Senate Judiciary Committee will try to move to the Senate floor this year, said Lydia Griggsby, the committee's chief counsel for privacy and information policy. The [Personal Data Privacy and Security Act](#), sponsored by Sen. Patrick Leahy (D-Vt.) would also limit how data brokers can use personal information and would establish data security rules for interstate businesses that collect personal data.

Leahy, chairman of the Judiciary Committee, will hold hearings on the bill later this year, Griggsby said.

A national data-breach notification law is a top legislative priority for cybersecurity products vendor Symantec, said David Thompson, the company's CIO. It's difficult for companies to comply with 45 different state laws, he said.

# Agency Infosec Spend a Mystery to OMB

## Carper: \$40 Billion Spent on FISMA Since 2002

October 29, 2009 - Eric Chabrow, Managing Editor

The White House Office of Management and Budget does not know how much its departments and agencies specifically spend on IT security, Federal CIO Vivek Kundra told a Senate panel Thursday.

Kundra said he was shocked to learn that the OMB never collected from agencies specific IT security expenditures, just aggregate data, when he took over earlier this year as the OMB's administrator for e-government and IT, his statutory title.

Without such information, Kundra said, OMB cannot effectively assess how one agency compares against another in securing IT assets as well as the ability of the government to gain a deeper understanding the value its cybersecurity investments furnish. He said OMB has begun collecting that information for the past fiscal year.

Kundra testified before Senate Homeland Security and Governmental Affairs Committee's Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security, whose chairman, Sen. Tom Carper, found it disconcerting that OMB employs few if any cybersecurity experts and that specific agency spending on IT security is unknown.

Carper said that just the certification and accreditation process required by the Federal Information Security Management Act costs \$1.3 billion annually, and estimates another \$1 billion is spent each year for agency inspectors general to audit FISMA compliance. In total, Carper said, the government has spent \$40 billion related to FISMA since its enactment in 2002.

### 'Simply Unacceptable'

"And even more troubling," Carper said, "agencies may be constrained from implementing the most basic of cybersecurity best practices because of inflexible requirements. Allow me to put that into perspective: federal agencies have spent more on cybersecurity than the entire gross domestic product of North Korea, who some have speculated is to be involved with some of these cyber attacks. That is simply unacceptable."

Much of the hearing focused on new ways to assess the security of federal government IT systems and data, with agreement from all the witnesses and Carper that the current process in which departments and agencies demonstrate how they comply with FISMA and OMB information security directives must be replaced with a system that validates in real-time the security of IT systems. The Delaware Democrat introduced a bill in April, the [United States Information and Communications Act](#), to create a new process to verify IT security safeguards in the federal government. Similar [House legislation](#) is being written.

Gregory Wilshusen, Government Accountability Office director of information security issues, presented a [GAO report](#) encouraging OMB to require agencies to adopt key attributes of successful information security measures promoted by experts from nationally known organizations, academia and state agencies that offer four attributes: they're quantifiable, meaningful, clearly defined and linked to practices used to make decisions. "To the extent that agencies do not measure the effectiveness and impact of their information security activities," Wilshusen said, "they may be unable to determine whether their information security programs are meeting their goals."

Another witness, John Streufert, deputy CIO for information security at the State Department, told the subcommittee about an initiative in which departmental computers around the world are continuously scanned to identify weak security configurations as compared with FISMA, which provides a snapshot once every three years. "Since mid-July," Streufert said, "overall risk on the department's key, unclassified network measured by

the risk-scoring program has been reduced by nearly 90 percent in overseas sites and 89 percent in domestic sites."

Former Rep. Tom Davis, the Virginia Republican who authored FISMA, told the panel "it is time to take FISMA to the next level." But he noted that in the early 2000s, the government had no coordinated policies to address the threat of cyber attacks, and FISMA provided important first steps in protecting the government's critical IT infrastructure. "FISMA has undoubtedly served to elevate the importance of information management and information security in government," Davis said. "That said, there is room for updates and improvements."

## **Nearly 6 Million Infected Web Pages Across 640K Compromised Sites**

October 27, 2009 ([InformationWeek](#))

Startup founded by ex-Google engineers tallies major jump in Website compromises and breadth of the infections.

More Websites are compromised today than ever, and about one-fifth of the pages on each newly compromised Website were infected as of this year's third quarter, according to new data gathered from real-time Web malware monitoring service provider Dasient.

Dasient, a startup whose co-founders include two former Google engineers, found 5.8 million individual Web pages infected across 640,000 compromised Websites. That represents a major increase from Microsoft's report in April of some 3 million infected pages, according to Dasient, which runs a behavioral-based service to diagnose infected Websites.

Ameet Ranadive, one of Dasient's co-founders and a former strategy consultant at McKinsey, says his company also detected more than 52,000 unique types of Web malware in the quarter. "Hackers are starting to see success here with Web-based attacks, so they are investing more in them," he says. "Websites are becoming more complex, and you have more Websites matching content, sourcing, and [banner] ads...creating opportunities to inject malicious content."

Among newly compromised Websites of 10 pages or more, nearly 20 percent of their pages were infected. The bad guys have been infecting more pages as a way to score more victims. "The more parts of a site that have been infected, the more difficult and challenging that it is to remediate and detect it," Ranadive says.

Reinfection of Websites is becoming a big problem, too: Of all the sites infected during the quarter, 39.6 percent were reinfected again during that period. That may be in part due to increasingly more complex and obfuscated malware that's hard to kill. "If a site is not [fully] clean...they are not only at risk, but at risk multiple times," Ranadive says.

Nearly 55 percent of Web-based malware was JavaScript-based, 37.1 percent was iFrame-based, and 8.1 was miscellaneous, according to Dasient. And vulnerable Web apps are only part of the problem, says Dasient co-founder Neil Daswani, formerly of Google. "The Website's code could be secure. But if it's using counters or ads or other functions from other sites, that code could be vulnerable" and then infect the site, he says.

Dasient also announced today it will open up its Web malware infection library via its Website and will list the top 10 Web-based malware threats each week, as well as other attack trends. Dasient has gathered data on more than 70,000 different Web-based malware infections since it first launched a few months ago.

## Latest threat vector: Our mobile devices

October 26, 2009 ([ComputerWorld](#)) -

As the "security guy" for my entire adult life, I've gotten a wide variety of security questions from friends, family, colleagues, travel companions and more. I tend to use these questions in the aggregate to spot trends in the wild. Far and away the most frequent questions are now focused on our mobile devices -- specifically how they are being used to spy on their owners and reveal our most intimate of secrets.

In the run up to the last Olympics I had lots of questions from law enforcement and intelligence communities around the world about the risks to corporate executives preparing to travel to the games. At that time, there were several known attack vectors being used to exploit traveler's smart phones, regardless of brand. These were well organized and highly focused attacks against high value targets -- people expected to have significant confidential data stored in their e-mail, contact lists, text messages, photo cache, document store and the deleted files. The information gained through these types of attacks could be used for corporate, political, or personal leverage.

Now, however, I'm getting similar questions from a very different and much wider group of folks. Rather than just the government calling, now corporate executives and regular folks who are going through some sort of breakup -- personal or professional -- are getting hit with very similar attacks, and it's hurting them much more deeply than a simple blue screen of death. Their innermost secrets are being revealed, and used against them in the most personal of ways.

There are three basic types of common attack vectors on smart phones: direct entry, via a download, or through Bluetooth.

A direct entry attack means that someone has physical control of your phone for a few minutes and they load spyware on it (yes, there is a lot of spyware on the market specifically for mobile devices). Think about how often you leave your phone sitting on your desk, your night stand, or a table at the coffee shop. If you start treating that phone more like your Visa card, you're a lot less likely to be attacked in this direct way. If you're going through a breakup of some sort, it takes a conscious effort to keep your 'trusted' partner from gaining access while you're at lunch, asleep, or at play. Once installed, mobile spyware can listen in on your calls, copy and transmit your e-mails and texts, and even steal your photos. Most people find out only when others seem to know information they really shouldn't. This is the most common form (other than from well-funded intelligence-gathering agencies) of mobile attack, and is easily spotted (more on how to spot mobile spyware in an upcoming post) and removed with several good commercially available programs -- once you know to look for it.

The next most common form of this attack is through a program download. Blackberry users who are addicted to Brick Breaker should watch out for add-ons (a new Blackberry patch is coming shortly). Similarly, everyone who downloads games should realize they might also carry a spyware payload along with the game. Whenever you download a program to your smart phone from a previously unknown website, email, or text link (and no, a Google hit does not a trusted relationship make), you run the risk of adding spyware to your mobile device. These programs perform basically the same spying functions as found with a direct entry attack, but they are generally not targeted at you specifically, as it's really up to you to find and download the program in the first place. This is a growing form of information harvesting, with corporate data and identity theft being the big targets.

Finally, it is now possible to attack many smart phones simply by standing within a few feet of them for a minute or two. That's how long it takes for programs to guess their way into your 4 digit Bluetooth key (even faster if you left it set to 0000 like most of the human population). Once in, the most common attack is to load a new 'blank' record into your contact list along with some code that can remotely activate your microphone. With that in place, you can be eavesdropped on whenever and wherever -- even when you don't think you're using the phone. This attack is the hardest to accomplish, and still the least common, but it has now spread beyond the foreign intelligence and organized crime world into regular, old fashioned corporate and personal espionage. If you use a Bluetooth earpiece, you're susceptible to this attack.

We now rely on our smart phones for all aspects of our lives. They contain most of our secrets, yet we still don't take them seriously when it comes to security. Everything that happens on our desktops is quickly moving to our smartphones, and that includes the bad with the good. Judging from the calls I've been getting, it's time to protect our smart phones as well as or better than the rest of our computers.

## After one year, Conficker infects 7M computers

By Robert McMillan

October 30, 2009 04:25 PM ET

IDG News Service - The Conficker worm has passed a dubious milestone. It has now infected more than 7 million computers, security experts estimate.

On Thursday, researchers at the volunteer-run Shadowserver Foundation [logged computers from more than 7 million unique IP addresses](#), all infected by the known variants of Conficker. They have been able to keep track of Conficker infections by cracking the algorithm the worm uses to look for instructions on the Internet and placing their own "sinkhole" servers on the Internet domains it is programmed to visit. Conficker has several ways of receiving instructions, so the bad guys have still been able to control PCs, but the sinkhole servers give researchers a good idea how many machines are infected.

Although Conficker is probably the computer worm most known about, PCs continue to get infected by it, said Andre DiMino, co-founder of The Shadowserver Foundation. "The trend is definitely increasing and breaking 7 million is pretty much of a landmark event," he said.

Conficker first caught the attention of security experts in November 2008 and received widespread media attention in early 2009. It has proved remarkably resilient and adept at re-infecting systems even after being removed.

The worm is very common in, for instance, China and Brazil. Members of the Conficker Working Group, an industry coalition set up last year to deal with the worm, suspect that many of the infected PCs are running bootlegged copies of Microsoft Windows, and are therefore unable to download the patches or Microsoft's Malicious Software Removal Tool, which could remove the infection.

Despite its size, Conficker has rarely been used by the criminals who control it. Why it hasn't been used more is a bit of a mystery. Some members of the Conficker Working Group believe that Conficker's author may be reluctant to attract more attention, given the worm's overwhelming success at infecting computers.

"The only thing I can guess at is the person who created this is scared," said Eric Sites, chief technology officer with Sunbelt Software and a member of the working group. "This thing has cost so many companies and people money to get fixed, if they ever find the guys who did this, they're going away for a long time."

IT staffers often discover a Conficker infection when a user is suddenly unable to log into a computer. That happens because infected machines try to connect to other computers on the network and guess their passwords, trying so many times that they are eventually locked out of the network.

But the cost of the worm would be even greater if Conficker were to be used for a distributed denial of service attack, for instance.

"This is certainly a botnet that could be weaponized," DeMinno said. "When you have a net of this magnitude, the sky's the limit in terms of what could be done."

# How To Boost Security Awareness Among Your Users

**October 30, 2009**

SMBs should skip the 'Wall of Shame' and instead try promotional events and penetration testing. There's a general misconception about user awareness that the IT industry has fostered for years: the belief that end users are dumb, and awareness is a waste of time. This mind set seems to affect the information security field more than any other area of IT. We even have t-shirts that say things like, "Social Engineering Specialist: Because There Are No Patches For Human Stupidity."

There's obviously no "IT smarts patch" or 12-step program to help users better recognize phishing scams or make them think twice before clicking on a link from Facebook. It's the job of IT and the company to develop an information security awareness program that's interesting, innovative, and won't bore users to tears. And that's where the breakdown occurs -- a breakdown that feeds the negative attitude about user awareness.

So what is user security awareness? The National Institute of Standards and Technology (NIST) in March released a draft of NIST Special Publication 800-16, "Information Security Training Requirements: A Role- and Performance-Based Model." In Section 2.2.1, NIST states:

*"Awareness is not training. Security awareness is a blended solution of activities that promote security, establish accountability, and inform the workforce of security news. Awareness seeks to focus an individual's attention on an issue or a set of issues. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize information security concerns and respond accordingly."*

In other words, a security awareness program needs to inform users of security issues, the policies surrounding them, and why they are important. Trouble is, the "why" is left out, so users consider security policies a boring nuisance they have to listen to once or twice a year, but take no ownership in. And even though PCI DSS Requirement 12.6 is yet another reason to have an awareness program, compliance with PCI doesn't mean anything to users if they don't understand the consequences of noncompliance.

Getting users to take ownership in security is critical to the success of any awareness program. For users to truly believe they are the first line of defense, they need to take ownership of the problems caused by their lack of understanding of security issues and the consequences of their actions. Are they aware of data breach disclosure laws in your state? Do they know what attackers are after these days? Have they seen real-world examples of attacks against other users?

Penetration testing is one method being used more often to help companies realize the deficiencies in their security awareness programs. Enterprises that have previously left users out of the scope of pen tests are now contracting for full-scope pen testing that includes social engineering, simulated phishing e-mail messages, and attacks against client-side applications. The lessons learned from a pen test can be leveraged to show your users how important their role is in protecting sensitive corporate data.

But avoid negative practices, such as a "wall of shame." Calling out users publicly for their security gaffes can be a very effective tool at curbing risky behavior (i.e., surfing porn and social networking sites) in the short term, but employees often end up embarrassed and resentful of information security, which can backfire, leading to carelessness and apathy toward their responsibilities to help protect company data.

Plenty of resources are available to help you develop effective security awareness programs. NIST SP 800-16 and related NIST SSP 800-50 (PDF) are excellent guidelines. Microsoft also has developed a guidance document and sample materials, which are available [here](#).

In addition, here are some activities and materials suggested by NIST in SP 800-16:

- host an information security day;
- conduct briefings on current issues, like the dangers of social networking;
- distribute promotional items with motivational slogans (think coffee mugs, mouse pads);

- provide login banners serving as security reminders;
- show awareness videos (Computer Security Awareness Poster & Video Contest 2009); and
- distribute posters and flyers.

Information security awareness programs can work, but only if you implement them with the right motivations -- and not just to meet compliance requirements. Numerous resources are available to help companies create effective programs to promote secure computing practices resulting in a safer environment for both users and the company's sensitive data.

## The Struggle With DLP

### ***DLP has gone mainstream; CSO Publisher Bob Bragdon says only careful planning can make it pay off***

By [Bob Bragdon, Publisher, CSO](#)

October 30, 2009 — [CSO](#) —

Few security technologies have received as much attention over the past few years as Data Leakage Prevention (DLP) solutions have. The concept behind them is exciting, offering the ability to scan traffic on your network and in your systems, and assign rules-based protections to the data that you want to protect. Someone e-mailing out a copy of customer records with SSNs? The DLP system will block it or encrypt it on the fly. Someone trying to copy IP to a USB drive? Alert management and block the action. It can be a great way to protect your most critical information assets, but as many have found, it is not an end-all, be-all solution to your data leakage problems.

This summer, CSO partnered with GTB Technologies to examine the experiences and expectations of DLP solutions. What we discovered is very consistent with what I have been hearing from CSOs around North America: DLP can be very good, but be prepared for hidden costs and lots of management effort, including internal staffing demands.

As I mentioned above, DLP does work, but the hidden challenges can be pretty big if you don't know what you're getting into. Consistent with what we have seen in other surveys we have conducted, 53 percent of respondents already have a DLP solution in place.

What was very interesting to see was that nearly half of those with a solution in place are planning to replace that solution within the next 12 months. This speaks to the frustration I hear with many businesses feeling that they were sold a "bill of goods" that just wasn't real. But my observations have been that many of these businesses fall down on the implementation, not because they were sold vaporware.

The primary reasons businesses adopt DLP is to protect company reputation (96 percent), avoid litigation (83 percent), meet regulatory obligations (77 percent), protect IP (66 percent) and the vast majority of respondents are very confident that their solution actually helps them to meet these objectives. But there appears to be some confusion regarding the capabilities of DLP. I believe much of that confusion has been driven by the "me too" mentality that has been adopted by some vendors who claim they offer DLP solutions when, in fact, their solutions only address individual silos of a true DLP solution.

Cost and management are also a large issue. When you add implementation and monthly management costs, businesses are spending, on average, \$240 per user over a two-year period for their DLP solution. One-third of respondents found that the solution cost was higher than expected and one-quarter pay more than they planned for internal management, as they have to refine the solution to eliminate false positives and increase effectiveness.

At the end of the day, does it work? Yes. But the message here is that you need to plan accordingly going into the project so that it doesn't become a budget buster in terms of both hard dollars and internal resources.

## Software shields online banking on infected PCs

By **Jeremy Kirk**

November 3, 2009 11:49 AM ET

IDG News Service - A U.K. security company is giving to banks, for free, security software that it says can block malicious software from manipulating online banking transactions or stealing data, even if the computer is infected.

The product, called [SafeOnline](#), comes from Prevx, a security company in Derby, England.

The module is designed to offer an additional layer of security for secure browsing sessions conducted with SSL (Secure Sockets Layer) technology, indicated by the "https" in the URL (Uniform Resource Locator).

Cybercriminals are developing increasingly sophisticated software that, in what is known as man-in-the-middle or man-in-the-browser attacks, can intercept online banking transactions while in progress and transfer funds with the user believing nothing is awry.

SafeOnline installs its own kernel-level driver on Windows PCs. During a secure browsing session, all information from the keyboard is routed through that driver, which defeats attempts to record keystrokes or other interference, said Mel Morris, Prevx's CEO and CTO.

SafeOnline has been tested by Immunity, a company that specializes in evaluating security technology. SafeOnline was tested against some of the most sophisticated banking malware, including Zeus, SilentBanker and Mebroot/Sinowal/Torpig.

SafeOnline has other components, such as an antiphishing feature that prevents authentication information from being entered into a suspicious Web site. It also verifies DNS (Domain Name System) lookups against other trusted DNS servers, which helps prevent pharming, where a correct domain name leads to bogus Web site.

Banks that decide to use SafeOnline with their customers will also get an antimalware component that is in Prevx's other self-titled security product, Prevx 3.0.5.

Prevx is a small company in a brutally competitive security market, dominated by big players such as Symantec, McAfee and Trend Micro. Banks don't want to pay for security software, so Prevx decided to give it to those that want it for free, Morris said.

"I suppose to an extent you can argue from their perspective that had security vendors done their job there wouldn't be a need for such a product," Morris said.

So far, six banking organizations have expressed interest, he said. The banks have special requirements that Prevx is able to meet. Banks don't want to modify their Web sites to accommodate a security technology, they want something that is easy for users and is compatible with other security products their customers may be running, Morris said.

Prevx's software can run alongside other security suites. It was purposely created that way as a way for Prevx to get into the market against entrenched competitors, Morris said.

SafeOnline will detect and halt malware, but if a customer wants to remove the malware, they will have to pay a subscription fee, which is how Prevx will generate revenue. SafeOnline with the malware removal component will cost £15.95 (US\$26) annually. SafeOnline is also a module in Prevx 3.0.5, which costs £24.95 a year.

Morris is hoping that customers see that Prevx outperforms other security suites by detecting more malware and then drop their subscriptions in favor of Prevx.

## Three-year-old Office patch stymies most attacks

Microsoft adds to the problem by not offering Office patches through the popular Windows Update service, expert says

By Gregg Keizer

November 4, 2009 02:21 PM ET

Computerworld - Users running Microsoft Office can stump nearly three-fourths of all known attacks targeting the suite by applying just one three-year-old patch, according to recently published data.

Almost three-out-of-four attacks -- 71% of all those spotted in the first half of 2009 -- exploited a vulnerability in Word that was patched in June 2006, Microsoft said in its bi-annual security intelligence report, released Monday. The flaw was fixed in the [MS06-027](#) security update issued.

The second-most popular exploit, with a 13% share, aimed at a bug that was quashed in March 2008, Microsoft said. The flaw was one of seven patched by the [MS08-014](#) update.

The 2006 update patched Word 2000, Word 2002 and Word 2003, while the 2008 fix affected Excel 2000, Excel 2002, Excel 2003 and Excel 2007.

Microsoft made the point that patching Office was as important as keeping Windows up-to-date with security fixes. "The majority of Office attacks observed in [the first half of 2009], 55.5%, affected Office program installations that had last been updated between July 2003 and June 2004," the company said in its report. "Most of these attacks affected Office 2003 users who had not applied a single service pack or other security update since the original release of Office 2003 in October 2003."

Unfortunately, users are far less likely to update Office than they are to patch Windows. According to Microsoft's data, the median amount of time since the last Office update was an amazing 5.6 years, compared to just 1.2 years since the last Windows update.

"Users can keep Windows rigorously up to date and still face increased risk from exploits unless they also update their other programs regularly," Microsoft warned.

Wolfgang Kandek, the chief technology officer at security vendor Qualys, echoed Microsoft's take on Office patching patterns. "We see the same in our data," Kandek said. "People just don't patch Office, and when they do, they patch it much slower than Windows."

That especially holds true in the enterprise. "This is a major security hole in the enterprise," Kandek said. "IT admins are not focusing on Office as they are on Windows. They do what's required of them," he continued, hinting that they often do little more than that. "Windows' security has a high profile, and so they're patching Windows. I don't think they're looking at Office, to tell you the truth."

Qualys obtains its data from PCs that it manages for its clients, most of which are companies.

One way to stay up-to-date without patching every month is to apply the infrequent service packs that Microsoft issues for Office. "If the Office 2003 RTM users in the sample had installed SP3 [Service Pack 3] and no other security updates, they would have been protected against 98% of observed attacks," Microsoft said. "Likewise, Office 2007 RTM users would have been protected from 99% of attacks by installing SP2."

[Microsoft delivered Office 2003 SP3](#) in September 2007, fixing more than 450 bugs in the application suite, and adding other security measures, including file blocking of older formats, a [move that confused users](#) well into the following year.

[Office 2007 SP2](#) hit the street in April 2009.

Nine out of 10 Office exploits in the first half of 2009 involved a Trojan downloader, or backdoor malware. "These kinds of threats allow attackers to access compromised systems later to install more malware," Microsoft said.

Microsoft urged Office customers to use the [Microsoft Update](#) service, a superset of the better-known Windows Update that pushes patches for Windows *and* Office.

Here, too, Kandek was stumped by Microsoft's practice of offering two separate update services.

"I'm not sure why that's the way they do it," he said, speaking of Microsoft's providing Office updates to consumers and small businesses only through Microsoft Update. "I don't see why they simply can't replace Windows Update with Microsoft Update, and patch everything."

Microsoft offers Office, as well as Windows patches, to businesses that use its Windows Server Update Services (WSUS) patch management system.

Office was last patched Oct. 13 when [Microsoft unveiled a record number](#) of security updates and fixed flaws.

The [security intelligence report](#) can be downloaded from Microsoft's site in PDF or XPS document formats.

## Six Steps to Pull App Security Back to the Future

**By Bill Brenner**

November 5, 2009 03:55 PM ET

CSO - Talk to members of the Open Web Application Security Project (OWASP) and all will agree that app security is half a decade behind where it should be, especially at the government level. The organization routinely holds events designed to turn the trend around, including the 2009 OWASP Application Security Conference (AppSec DC) in the nation's capital Nov. 10-13. In advance of the conference, CSOnline touched base with OWASP member Matt Fisher, CEO and AppSec contractor at Piscis Security, about some of the key problems with app security today and six ways to turn things around. We begin with some questions and answers on the current state of affairs, then move to the six steps.

CSO: Where are organizations most out of sync in terms of how they use Web 2.0 apps and what the greatest security risks are as a result?

Matt Fisher: Well, the term "web 2.0" is a bit like "cloud computing." One of the challenges there is defining it. "Web 2.0" can refer to the programming technologies and certainly the increase in browser plug-ins and client-side techs used for rich internet apps has seen their share of vulnerabilities. It can also refer to collaboration and awareness applications such as internal wikis and blogs. The risk there -- particularly on a wiki -- is that you don't have any control over the content being supplied. If that wiki is open to the entire organization then you're subject to anyone in your organization posting confidential or inappropriate content. Now, if by "web 2.0" one means social networking applications, then the risk goes up tremendously. They make good marketing platforms in that they're opt-in, and let you generate direct impressions without the cost of an e-mail campaign, and they can even be used for inbound information gathering. It's important to realize though that many of these applications have a long history of insecurity and are subject to worms and worse, all of which have the potential to damage your online brand.

Some OWASP members have described the government's app security as being about half a decade behind where it should be. Talk about why it's important for the Feds in particular to be more on top of their Web 2.0 security, in terms of its unique risks, compared to the private sector. Fisher: I think one of the most important areas to understand is that messages from the government have to be trusted, and that just because a novel Web application becomes trendy doesn't necessarily mean it's an appropriate medium for all government use. From a cybersecurity perspective, the completely off-hosted nature of these apps present a real challenge, too. They're being used to communicate department or agency information, yet there's no ability to apply your normal security process to them; you have no independent validation, can't perform a test and evaluation and have no artifacts or documentation to judge their security by. You control absolutely no aspect of the system other than your password, and frankly you don't even know if that password is being stored properly. You don't house the

datacenter and have absolutely no control over the operating system security, the application security, the network defense, you can't pull an incident response on them, you can't perform any forensics. There is zero control.

Of course, theoretically the risk is very low because it's all public communication anyhow. I recently read an analysis of the subject and at one point when discussing risk it said something to the effect that integrity mattered less because it was a public system, but I don't quite agree with that. If you're using one of these sites to communicate as the United States Government, then the integrity of those messages is paramount. It's completely feasible that an adversary could find a vulnerability in one of these applications, and wait until an opportune time to use it for a misinformation or psyops campaign. Imagine all the people getting regular messages from various agencies to their cell phone. Now imagine all of them suddenly becoming subtly bogus during a national disaster.

Let's link this back to the private sector. One thing that comes to mind is that while government security holes can have a negative impact on private enterprise, the reverse can also be the case. Give one or two examples of this in the Web 2.0 universe. Fisher: The government has a huge contracting industry supporting it that is often very interwoven with the departments and agencies they are supporting and there are many historical cases of breaches in a contractor security exposing their customer to risk. Certainly this can exist in the Web 2.0 universe as well as outside it.

Now that we've outlined the problems, give five or more examples of steps the public and private sectors can take to improve app security. Fisher: Here are six:

1. Build a community. Large enterprises like the Federal government are particularly prone to the silo effect; a simple intranet site that's well managed can work wonders to leverage the expertise throughout an entire Department.
2. Spread the expertise. Right now the majority of what application security knowledge exists within security groups. This is a good start but ultimately the programs build and fix the applications; staff them with experts, too.
3. Think beyond tools. While tools can automate certain assessment tasks, realize that they only assist with a portion of your assessments. Even then, assessments are just one portion of an assurance program.
4. Provide guidance. Developers want to build secure, compliant software; they just don't always know how. Make standards, requirements and reference models available to your programs.
5. Don't wait to test. Late-cycle testing under release pressure is stressful on the program and testers alike. Start testing earlier in the cycles and involve your assessment team in the scheduling.
6. Zoom-in your continuous monitoring. A "minor" application change can fly through change control but create huge vulnerabilities. Scrutinize changes to applications carefully, particularly Internet-facing or other high-risk systems.

