

# ESO - Security Trends Report

12/08

## Feds urged to provide cybersecurity incentives

A voluntary approach doesn't work, says the Internet Security Alliance

By Grant Gross

November 19, 2008 (IDG News Service) [President-elect Barack Obama](#) needs to take a new approach to cybersecurity, with the government providing incentives for private businesses to adopt security measures, a cybersecurity group said.

The Internet Security Alliance (ISA), a cybersecurity advocacy group, called on Obama to abandon the voluntary approach advocated by [President George W. Bush's](#) administration during the past eight years. "The voluntary partnership model of the Bush administration did not work adequately," said [Larry Clinton](#), the ISA's president. "However, a centralized set of regulatory mandates will not meet this international and quickly evolving problem and might even be counterproductive."

The Bush administration's 2002 National Strategy to Secure Cyber Space and later efforts contained "no serious attempt" to address incentives needed [for private business to invest in cybersecurity](#), the report said.

Half of all senior executives do not know how much money their companies have lost from cyberattacks, the ISA said. One third of companies in a recent survey don't use firewalls, and nearly half didn't use encryption, the group said.

A new ISA report, "The Cyber Security Social Contract" released Tuesday, recommends that the U.S. government establish incentives -- tax breaks, small-business loans or lawsuit protection -- for private companies to invest in cybersecurity.

"We are now past the time when government can hope that industry will simply fulfill the role of fully funding cyberinfrastructure security," the report said.

It's unclear how much the ISA's recommendations would cost.

The report calls on the government to set up a comprehensive and "aggressive" cybersecurity education program targeted at senior executives at businesses. And it calls for an extensive program to improve the U.S. government's own cybersecurity efforts, targeted at fixing problems at many agencies receiving poor grades on annual Federal Information Security Management Act (FISMA) reports.

The report also lays out the cybersecurity challenges for several U.S. industries, including banking, communications and manufacturing. It asks representatives of those industries to detail what they'd tell Obama about cybersecurity needs.

For example, an unnamed representative of the banking industry said that U.S. cybersecurity "cannot be successfully defended or mitigated against using our current paradigm of thinking."

Instead, companies need better software quality and assurance, protection from lawsuits, a robust cyberinsurance program and better education programs, the banking representative said.

ISA officials said they're confident the Obama administration will be open to the recommendations.

"The good news is that we actually do know a great deal about how to secure our cybersystems," Clinton said. "Independent research and anecdotal reports from information security officials both indicate that as much as 80% to 90% of our current problem could be successfully addressed if we simply get people to adopt the security practices that have been demonstrated to work."

## **Data Destruction a Major Cyber Threat**

**Federal Computer Week (11/18/08)**

National Intelligence director Mike McConnell warns that hackers tampering with and destroying data--particularly data related to financial transactions, transportation systems, and electric power facilities--are the biggest cyberthreat the country faces. Although other types of cyberattacks--such as Website defacing or denial-of-service attacks launched by other countries--also are serious, McConnell says that data destruction and data-scrambling attacks on certain sectors could undermine the nation's stability. For instance, a data-scrambling attack on a bank could have a negative impact on the economy as a whole, he says. However, he says this threat could be addressed by expanding the country's defenses to protect banking, finance, and transportation systems from cyberattacks, including operations at the network level. Doing so would allow companies to quickly identify attacks and take steps to protect themselves.

## **IT Security's Next Big Threat: Young People**

**Dark Reading (11/19/08) ; Wilson, Tim**

Several recent studies have found that Generation Y, people under the age of 28, are one of the biggest cybersecurity threats to organizations. One of those studies, which was published by Accenture in early November, found that 60 percent of students and employees between the ages of 14 and 27 are either unaware of their companies' IT security policies or simply choose not to follow them. The study also found that students and employees between the ages of 18 and 22 use technologies that are not supported by their employers for work-related tasks, including social networking sites, open source technology, and online applications. Another study from Intel and Penn Schoen & Berland Associates found that half of IT professionals believe Generation Y employees are a serious security concern because of their tendency to use non-sanctioned applications and social media tools while at work. Finally, a recent ISACA survey found that 40 percent of Generation Y employees plan to spend up to five hours doing holiday shopping from their work computers this holiday season. This represents a security threat to organizations because many employees will give their workplace email addresses to online retailers, which opens up the organization's network to a variety of threats, ISACA said. In addition, many of the employees ISACA surveyed said they do not check or do not know how to check the security of an online retailer's site before making a purchase.

## **Most Data Security Risks Internal, Cisco Study Finds**

**Network World (11/12/08) ; Duffy, Jim**

Most IT security leaders are more afraid of the risks posed by their own employees than by outsiders, concludes InsightExpress' data-leakage study of more than 2,000 workers and IT administrators in 10 countries. Ten percent of the employees surveyed in the Cisco-sponsored study said they had stolen--and sold for a profit--company-owned information or devices, or were aware of an employee who had. Thirty-three percent of the IT leaders said their largest security concern was theft of portable hard drives, followed by email (25 percent), lost or misplaced devices (19 percent), and talking about sensitive information with non-employees (8 percent). Roughly 10 percent of the employees surveyed had lost or had a device stolen within the prior 12 months, Cisco says. Those who confessed to keeping company devices after they left the job did so for a variety of reasons, including revenge, personal gain, and belief that the device would not be missed.

## **Cyberthieves Mine for Corporate Data Nuggets**

**USA Today (11/12/08) P. 1B ; Acohido, Byron**

The past year has seen an increase in cybertheft, with more and more criminals targeting corporations whose employees use free Web tools such as AOL instant messaging, Gmail, and MySpace. Some of the desired information includes email address books, PowerPoint presentations, engineering drawings, and bid proposals. Most companies do not recognize the need to limit the use of free online programs, or to address the security issues they present. Security firm Finjan reports that data thieves in the past nine months harvested large amounts of data without a specific buyer in mind, searching through it later to find information valuable enough to sell. IBM's Gunter Ollmann says stolen data is sometimes used to access deeper levels of information, such

as company databases. For example, in 2000, stolen information from Super Vision Lighting was purchased by Chinese entrepreneur Samson Wu and used to imitate the company's manufacturing facility. Last month, data thieves found a security flaw in Windows XP and Windows Server PCs that allowed them to copy all personal data stored on the PC's Web browser and registry. Palo Alto Networks' Chris King says that few companies pay for more secure alternatives to free Web programs, such as company-supplied instant messaging. Customized business applications are usually created with function in mind over security, says the National Cyber Security Division's Joe Jarzombek. Experts say that with few companies applying enough protection to their information, there is little reason for cyberthieves to be discouraged from harvesting confidential information.

## **Redundancies, Grudges and Huge Security Risks**

**Financial Times Digital Business (11/05/08) P. 3 ; Munro, Ken**

A recent survey by Cyber-Ark illustrates the risks posed by disgruntled IT professionals. According to that study, 88 percent of redundant IT administrators said they would steal valuable and sensitive information from their company if they were fired. Angry employees who suspect their jobs are in jeopardy can also inflict damage on their organization's network. For example, a systems administrator for San Francisco's Department of Technology allegedly created a password that locked officials out of the city's network when he began to fear losing his job earlier this year. Unfortunately, there are few ways organizations can protect themselves from the threat posed by disgruntled employees, writes Ken Munro, the director of the penetration testing and IT security specialist at NCC Group SecureTest. However, Munro notes that organizations can mitigate the risk posed by these threats by implementing a robust procedure for monitoring activity on their networks, closing accounts when employees quit or are fired, and recovering devices such as BlackBerrys from former employees.

## **Internet Attacks Grow More Potent**

**New York Times (11/10/08) P. B8 ; Markoff, John**

The number of distributed denial of service (DDOS) attacks--in which botnets spray random packets of data in large streams over the Internet in an effort to shut down Web sites and corporate networks--is on the rise, concludes an Arbor Networks survey. The survey also found that individual DDOS attacks are growing more powerful and sophisticated. According to the 70 Internet operators in North America, South America, Europe, and Asia who participated in the survey, the largest DDOS attacks have grown in size from less than half a megabit to 40 gigabits over the past seven years. As a result, the most powerful DDOS attacks today are more than capable of overwhelming today's largest network connections, which carry 10 gigabits of data. Despite the growth in the size of DDOS attacks, Internet operators say they are increasingly able to respond to the attacks thanks to improved collaboration among service providers. "Most enterprises are connected to the Internet with a one-gigabit connection or less," says Arbor Networks' Danny McPherson. "Even a two-gigabit DDOS attack will take them offline."

## **Why Traditional Security Doesn't Work for SOA**

**IDG News Service (11/06/08) ; Clark, Chris**

Many organizations are adopting service-oriented architecture (SOA) because it promises to increase the flexibility of applications, make the process of integration more manageable, reduce development costs, and better align technology systems with business processes. However, there are a number of security risks associated with the use of SOA. For example, many SOA architectures allow each service to possess a method for clients to query and retrieve contracts in order to make the collection and discovery of new contracts easier. This method for retrieving contracts is typically standardized either by the application framework vendor or by SOA practitioners. Although this approach makes it easier for developers to build new services and reuse existing services across the enterprise, it also allows hackers to easily collect contracts and map out the location of high-value services within an organization. Fortunately, SOA practitioners can address such security vulnerabilities by taking certain steps when implementing the technology. For example, practitioners can make it more difficult for hackers to create maps of the location of high-value services by disabling anonymous exposure of service contracts and using authenticated or offline distribution instead.

# Symantec Sees Rise in USB-Based Malware as Reports of U.S. Army Ban Surface

By [Brian Prince](#)  
2008-11-20

A reported ban by the U.S. Army on USB devices underscores the growing prevalence of USB-based malware. Researchers at Symantec say they have observed an increase in USB security threats going back at least a year.

[Researchers at Symantec](#) are noting an uptick in USB-based malware as reports surface of a U.S. Army ban on USB devices and portable media.

According to [reports on Wired](#), the U.S. Army has banned the use of USB sticks, flash media cards, CDs and other removable storage due to security concerns and the proliferation of the [Agent.btz worm](#) a variant of [SillyFDC](#) that spreads by copying itself to thumb drives or other removable media.

News of the Army ban comes as attackers are increasingly turning to USB-based malware. In [Symantec's Global Internet Security Threat Report Vol. XIII](#), the security vendor noted that executable file sharing was the most common means of malware propagation in the second half of 2007. This was done by viruses and worms copying themselves to removable media, according to the report.

The trend has continued in October and November, with each of the five most active pieces of malware that use the USB attack vector increasing in prevalence. For example, VBS.Runatuo went from roughly 2 percent of sampled malware on Oct. 1 to about four percent Nov. 12.

"The jump in this particular type is mainly a result of malware authors being opportunistic," said Marc Fossi, manager of development for Security Technology and Response at [Symantec](#). "We've found in the past that as a technology becomes more widespread and used by more users that malware authors become more likely to take advantage of that technology."

There doesn't seem to be a particular group behind the increase, according to Anthony Roe, threat analysis engineer on Symantec's Security Intelligence Analysis Team. More likely, Roe said, it is a concept that has been incorporated into more malicious code because of the growth in USB use and the method's viability.

"We don't have any specific numbers on USB device usage, but many people are using these devices to share large files that would take too long to transfer over the network or are too large for e-mail," Fossi said. "Also, in regions where Internet cafes and booths are heavily used or more popular, users may store all their personal documents on a thumb drive and plug it into the public terminal to upload or download a file ... It's similar to the way many of the old floppy disk viruses used to spread."

In a blog post, Symantec advised users to disable the AutoRun functionality for removable media. In addition, businesses can set policies that keep USB storage devices from being used, Symantec officials said.

## Who's been reading my cell phone records?

Experts say there have been few reported cases, but no protections are in place

By **Stephen Lawson**

November 25, 2008 (IDG News Service) If [Verizon Wireless](#) employees could snoop into then-[Sen. Barack Obama](#)'s cell-phone records, as the carrier acknowledged last week, then mobile subscribers may worry how well protected they are. They should, according to some industry analysts and privacy lawyers.

Verizon Wireless found that some employees viewed information from an Obama cell-phone account that has been discontinued for several months, the company disclosed last week.

Verizon was investigating employees who saw the information, with and without authorization, and put them on paid leave. Later reports said some had been fired.

Verizon declined to comment for this story.

Information that is saved by mobile operators -- and that might be available to unauthorized or unscrupulous employees -- includes whom you talked to, when you called them or they called you, and for how long you talked, as well as text messages and voice mail, according to [Ari Schwartz](#), vice president and chief operating officer of the [Center for Democracy and Technology](#) (CDT).

### **What info is saved?**

The information can also include your locations when you started and ended the call, as determined by cell towers or other techniques, CDT Senior Counsel John Morris said. The risk is greater with current accounts than with closed ones such as the Obama record that was snooped, Schwartz said, because some types of data are kept longer than others.

There have been few cases of internal snooping on mobile records, at least ones that have seen the light of day, according to attorneys and analysts in this area. But neither are there clear protections, they charge.

"It is very easy to obtain wireless phone records of another person," said Chris Hoofnagle, director of the information privacy program at the Center for Law & Technology at the University of California, Berkeley. "How can you tell when your [authorized] employee is looking at records in an inappropriate context? That's the challenge that the phone companies have to deal with."

Phone-company employees snooping for fun would be one thing, but the danger seems to go beyond that to include information being passed to outsiders, such as private investigators, he said.

### **Personal information for sale**

"There is at least some evidence ... there is a little bit of a market in which employees are improperly selling access to private information," said [Kurt Opsahl](#), a staff attorney at the Electronic Frontier Foundation (EFF).

According to the Electronic Privacy Information Center (EPIC), online data brokers openly advertise on the Internet that for about \$100, they can provide information on all the calls made on a particular cell phone. Such information isn't interesting solely to celebrity-chasers, observers said. It could put average people in danger from stalkers or ex-spouses, for example.

Under standard procedures, no one at a mobile operator looks at an individual's call data record -- the combination of personal identity, dialed numbers, call times and financial details -- without the customer's permission, according to Tad Neeley, chairman of mobile operator Telscape International Inc. If a customer-service representative needs to see the record to solve a problem over the phone, he'll ask the subscriber before opening it up. But the information typically is accessible to many people along the line, including those in administrative positions, Neeley said.

Information on incoming and outgoing calls is collected in a database as the month goes on, but the call data record doesn't exist until someone initiates a query to bring that data together with the customer's name, address and account information, Neeley said. Then the bill goes out on paper or as an e-mail message for the customer's eyes only.

Carriers also need to be able to generate a call data record in response to a subpoena or a police search with a warrant, Neeley said.

But that doesn't mean that no one inside a mobile operator can, technically, create a call data record for his own curiosity, Neeley said. Even if the data is encrypted, some administrators and other employees will have passwords to view it.

Comverse Technology Inc., which provides billing software to mobile operators around the world, offers many tools for carriers to both secure their subscriber records from unauthorized users and keep records on what authorized users do with them, said senior vice president Kurt Silverman.

"In our systems, we'll know what you've done, if you did anything interesting," Silverman said. Verizon does not use Comverse's software, he said.

The legality of viewing cell-phone records isn't always as cut and dried as relying on a subpoena, warrant or customer permission, privacy experts said.

Improperly viewing phone records, whether for land-line or mobile phones, should fall under federal wiretapping laws, Berkeley's Hoofnagle said. But the statutes specifically addressing phone-record privacy are complicated and aren't always as strong for cell phones as for land lines, he said. A recent bill in the California legislature aimed to protect cellular information as tightly as land-line phone bills.

"California tried to strengthen its phone-records protections, and there was a very strong lobbying effort from the phone companies to prevent expansion," Hoofnagle said.

The federal government has cracked down on improper access to cell records with the Telephone Records and Privacy Protection Act. It was enacted last year in part to prevent "pretexting," in which unauthorized people call a carrier and pretend to make legitimate requests for information. Following the Obama records incident, Sen. Patrick Leahy (D-Vt.), chairman of the Senate Judiciary Committee, earlier this week asked the U.S. Department of Justice whether that law had been effective in protecting consumers' privacy. But whether the pretexting law covers this kind of internal breach will be a matter of interpretation, the CDT's Schwartz said.

There isn't much a consumer can do to prevent phone-company employees delving into bill records, but Schwartz recommends that anyone concerned about it ask carriers about their privacy policies before signing up.

If a mobile operator promised its subscribers certain privacy protections and didn't deliver them, that could be grounds for a breach-of-contract suit or even an action by the U.S. Federal Trade Commission against deceptive practices, Schwartz said.

The fact that Verizon found out about these breaches and acted on them is actually a good sign that the industry may be moving in the right direction, Schwartz said.

Opsahl of the EFF, which has clashed with the Bush administration over alleged illegal federal wiretapping in the case of *Hepting v. AT&T*, sees another possible silver lining.

The question of call-record privacy is key to *Hepting v. AT&T*, where the government is alleged to have monitored who called whom on some carriers' wired networks. Voting as a senator earlier this year, Obama approved a law that in part granted some immunity to carriers in such cases. Opsahl said this case may contain a lesson.

"It might help Obama understand the invasiveness of the warrantless surveillance program," Opsahl said.

## UK Information Commissioner Seeks Authority to Impose Increased Fines

(November 18, 2008) The UK Information Commissioner's Office (ICO) wants the authority to fine companies up to 10 percent of their revenue for violations of the Data Protection Act, which would match the maximum penalty that can be imposed by the Financial Services Authority on companies that do not comply with financial regulations. Presently, the maximum fine the ICO may impose is GBP 5,000 (US \$7,366).

<http://www.growthbusiness.co.uk/news/business-news/814242/fines-likely-for-data-breaches.shtml>

[Editor's Note (Schultz): The level of ICO's current authority is ostensibly not nearly sufficient to deal with cases of negligence in data protection. Increasing this office's level of authority to levy much more substantial fines would thus constitute a step forward in helping combat data security breaches as well as identity theft.

(Dick): I agree with Eugene's comment. I recently learned from executives in the electrical power industry one of the primary driving forces in addressing cyber security issues was the fear of significant fines and penalties from Federal and State regulatory agencies. In short, the power companies could not be allowed to pass on the fines and penalties in their rates. If they pay for it, the business case for investment in improved security becomes easier.]

## Healthcare Workers in UK and US Not Taking Adequate Security Precautions with Data

(November 20, 2008) A survey of 1,000 healthcare workers in the UK and the US found that more than one-third store sensitive patient data on portable data storage devices, including laptop computers, Blackberrys and USB sticks.

One-fifth of respondents said they stored data on their personal devices to transport the information. One-third of those responding said they use passwords as the only form of data protection. Six percent of UK respondents said they use no data protection at all; in the US, that figure is 18 percent. Of the UK workers, 56 percent use strong data protection methods, including encryption, two-factor authentication, biometrics and smart cards. Among US respondents, just 23 percent use strong data protection methods.

## Security Audit Guidelines Will Call on Agencies to Focus Attention on Frequently Exploited Flaws

(November 21, 2008) The Consensus Audit Guidelines (CAG) will enable federal agencies to focus their security expenditures on fixing the vulnerabilities that are most frequently exploited, before addressing those that are more hypothetical, and to enable agency inspectors general to verify that the most important problems are fixed first. Concentrating resources on known security flaws will improve the value of the current certification and accreditation process mandated by the Federal Information Security Management Act (FISMA) by ensuring the right things are being measured.

The group developing the CAG, led by John Gilligan, who served as CIO of both the Department of Energy and the US Air Force, is composed of experts from the key federal agencies involved in computer network attack and cyber intrusion investigations as well as their counterparts in the commercial world who do penetration testing and incident response for banks and other victims. The idea behind the initiative - one that also led to the Federal Desktop Core Configuration - is that "defense should be informed by offense."

[http://www.nextgov.com/nextgov/ng\\_20081121\\_8289.php](http://www.nextgov.com/nextgov/ng_20081121_8289.php)

[Editor's Note (Skoudis): Focusing defenses on the most widely used attack vectors is a good idea, one that can allow organizations with resource constraints to focus their energies on the most salient attack vectors. Of course, eventually the bad guys will innovate and use other vectors, but such guidelines can be updated as the attacks evolve.

(Paller): As Tom Donahue, the CIA's top cyber security threat analyst, is fond of saying "you have to manage the known bads." This is the first time government experts have worked together, across agency line, with the private sector, to define those "known bads," so they \*can \*be managed. The federal CIOs who know about this initiative expressed confidence that the CAG would allow them to more rationally allocate their security expenditures. One of them said it clearest, "It's just common sense."]

## NASA Internal Memo Addresses Removable Media Security Policy

(November 21 & 24, 2008) NASA Chief Information Officer Jonathan Pettus last week issued a memo clarifying agency policy on the use of removable media. The memo instructs employees not to use personally owned USB drives or other removable media on government computer systems; not to use government-owned removable media devices on personal machines or machines that do not belong to the agency, department or organization; not to put unknown devices into any systems; and to ensure that systems are fully patched and anti-virus software is updated. The directive is not as sweeping as that imposed by the US Defense Department, which temporarily forbids the use of USB drives and other removable media devices of all types. The DoD instruction was issued to mitigate the spread of detected malware.

[http://www.nextgov.com/nextgov/ng\\_20081124\\_5509.php](http://www.nextgov.com/nextgov/ng_20081124_5509.php)

<http://www.spaceref.com/news/viewsr.html?pid=29884>

[Editor's Note (Skoudis): I'm surprised it has taken this long for some organizations to act on this attack vector. Windows ships with autorun for CDs enabled, and USBs with U3 technology look just like a CD to a Windows box, making compromise trivial. Enterprises should address this threat with clear policy and instructions for employees, shored up with technical implementations that turn off autorun via Group Policy.

Microsoft describes how to do the latter here:

<http://support.microsoft.com/kb/953252>]

# Hands-off hackers: Crooks try surgical strikes

## *Cyber-underworld shows patience and restraint in stalking their victims*

By Jordan Robertson



updated 8:02 a.m. PT, Mon., Nov. 24, 2008

SAN JOSE, Calif. - Internet criminals have been getting more "professional" for years, trying to run their businesses like Big Business to get better and more profitable at selling stolen data online. Now the bad guys of the cyber-underworld are exhibiting other unexpected traits: remarkable patience and restraint in stalking their victims.

A new report by antivirus software vendor [Symantec](#) Corp. details a startling trend that highlights the inventive ways criminals are figuring out ways to make money online.

Hackers are sometimes breaking into [online businesses](#) and not stealing anything. Gone are the bull-in-the-China-shop days of plundering everything in sight once they've found a sliver of a security hole.

Instead of swiping all the [customer data](#) they can get their hands on, a small subset of hackers have concerned themselves with stealing only a very specific thing from the vendors they breach — they want access to the compromised companies' payment-processing systems, and nothing else, according to the "Symantec Report on the Underground Economy," slated for release Monday.

Those systems allow the bad guys to check whether credit card numbers being hawked on underground chat rooms are valid, the same way the store verifies whether to accept a card payment or not.

It's a service the crooks sell to other fraudsters who don't trust that the stolen card numbers they're buying from someone else will actually work, and it's good business.

The bad guys hardly touch anything. The customer data for that store's clientele remains intact. They don't install malicious software that turns the compromised machines into spam-spewing robots.

Think of it like taking a used car to a mechanic for an inspection before buying. Only in this case the mechanic's a squatter who's holed up illegally in some other guy's shop and using his tools when no one's around at night. And he cleans up spotlessly once he's done.

"They treat these things fairly pristinely so they can maintain access," Alfred Huger, vice president for Symantec Security Response, said in an interview.

According to Symantec, in the company's yearlong look at 135 so-called "underground economy servers" — all public servers hosting mostly legitimate chat channels, with a few bad ones catering to cyber crooks —

researchers determined that criminals have latched on to this tactic as a way to make money and self-police the underground.

Symantec said it didn't find out which vendors had been compromised. The company says it didn't get inside the compromised servers that carry even more secretive back-channel conversations, because doing so would have broken the law.

The Cupertino-based company's researchers were only able to determine the trend is happening by looking at thousands of credit card numbers being checked every day — and either accepted or rejected — by shadowy groups online promoting that service and charging a fee. That fee is about \$10 per card checked. Considering they're typically checked in batches of 10 or more, the revenue can add up fast.

Researchers said that the high number of cards the groups were checking each day suggests that they either had long-term access to a few compromised vendors, or had a lot of compromised vendors under their control and would shift the credit-card-checking chores to different ones to avoid being detected.

Huger said the reason the criminals don't raid the victim companies' databases is it's much lower risk to just check the card numbers on someone else's computers, rather than to start taking stuff out, which gets noticed.

Plenty of bad guys are still looting everything in sight, according to Symantec's study. Researchers spotted \$7 billion worth of stolen credit cards and bank accounts being sold during the yearlong project. That figure assumes the cards and accounts were completely drained by the crooks.

The actual price for those cards and accounts could command on the black market was far less, however, because of the risk the buyer takes on in trying to extract money or make fraudulent purchases. Symantec estimated that the total value of the goods advertised for sale was more than \$276 million during the time they were watching the servers from July 2007 to June 2008.

The report mostly underscores the trend that online criminals are adding more touches of professionalism to their businesses, like bundling packages of exploits together and selling them, or offering up programmers — like a company would hire a consultant — to write malicious code for other people.

Huger said the report just touched on the "low end" of the underground economy. The report emphasized that the potential bounty for hackers on the underground economy will only go up as "matures and operates more like a traditional business model."

## **IT Security: Survey Says It's Better**

**Government Computer News (11/20/08) ; Jackson, William**

Confidence about federal government IT security has grown for the third straight year, reveals a recent Cisco-sponsored survey of 223 IT officials in more than 40 civilian and defense agencies. The survey found that 60

percent of respondents said they were more confident with their agency's IT security than they were a year ago. Last year, 51 percent of respondents said their confidence had increased since the previous year. In addition, the survey found that 64 percent of respondents are spending more time on complying with mandated requirements such as the Federal Information Security Management Act and the president's Comprehensive National Cyber Security Initiative. Finally, the survey found that security breaches, poorly trained or unconcerned users, and the impact security breaches have on operations are the security issues that IT officials are most concerned with. However, the survey found that more of the threats IT officials are concerned about are coming from interactive Web 2.0 services. One in five respondents said they were involved in securing Web 2.0 services--which include peer-to-peer communications and social networking--in their agencies.

## **Survey: Employee Data More Vulnerable Than Constituent Data**

**Government Technology (11/14/08) ; Collins, Hilton**

Federal workers--not constituents--are the ones left most vulnerable by a government security breach, concludes a recent PricewaterhouseCoopers (PwC) survey of more than 7,000 CEOs, CFOs, CIOs, chief security officers, and other top executives from 119 countries. The survey found that most governments are uncertain about where their sensitive data is kept. The survey found that roughly two-thirds or more of the respondents in the public sector do not know where their organization collects and stores data, and do not have an inventory of every third-party vendor who might have viewed constituent information. "The organization, first and foremost, needs to perform a risk assessment around this data to determine which data is considered sensitive, or, in some cases, personally identifiable information," says PwC's Jack Johnson. He says agencies are generally more conscientious about protecting constituent data and pay less attention to protecting the data of their own employees, which could make federal workers an easy target. Johnson suggests that government agencies regularly rank information and data assets in accordance with risk level increase employee data protections, encourage employee adherence to federal security guidelines, and draft an incident response strategy in case a breach does occur.

## **Experts Predict Rise in 'Virtual' Malware**

**VNUNet (11/25/08) ; Muncaster, Phil**

Attackers are likely to script some especially complicated forms of malware in 2009 in an attempt to regain ground after a few major botnet seizures and shutdowns made headlines this year, according to forecasts from MessageLabs. The firm predicted that some of the more sophisticated hackers will try to write malware as its own layer of virtualization that runs on the hardware and cannot be detected by the operating system. "The operating system does not know it's there, and the malware will be intercepting low-level operating system calls," says MessageLabs analyst Paul Wood. The main challenge with this type of malware will be identifying it and cleaning it up without having to reinstall all the hardware on a machine, he notes. MessageLabs predicts that hackers will begin creating more attacks especially for mobile devices. While computer-oriented viruses are created with the intention of establishing botnets, the security provider believes attackers will try to earn money by pirating phones and making them call premium phone numbers operated by the attackers.

## **Report: Nearly all computer users running insecure programs**

Angela Moscaritolo  
December 04, 2008

Only two per cent of computer users are fully patched and the other 98 per cent are running at least one insecure, unpatched program, security firm Secunia said this week.

Secunia gathered data from 20,000 new computer users based on a first scan of its recently updated, free consumer vulnerability-scanning tool.

Researchers found that 30.3 per cent of PCs had one to five insecure programs, 25 per cent had six to 10, and 45.8 per cent had 11 or more. These statistics have got slightly worse since January 2008, the last time Secunia posted similar statistics about the state of programs installed on PCs.

In the January results, Secunia found that 95.5 per cent of users had at least one insecure application, 27.8 per cent of computers had one to five, 25.7 per cent had six to 10, and 42 per cent had 11 or more.

"All results presented here are considered to be 'best case' scenarios," Secunia analysts wrote in a blog post. "The real numbers are likely to be worse."

That is, real figures of unpatched users/PCs should be higher because the users who scanned their systems with the tool are likely to be more security minded than all other internet users, the blog said.

"The results are shocking and prove, as well as emphasize, the need for a patching solution for private users," Mikkel Winther, Secunia's PSI partner manager, said.

Reports of exploits to patched systems continue to crop up. Last month, the SANS Internet Storm Center reported new exploits against Adobe Reader that surfaced two weeks after the program was patched. In addition, exploits to Microsoft's patched Microsoft Windows Server Service (MWSS) vulnerability have continually surfaced since the patch was issued on October 23.

## Vulnerable Windows Machines? Shocking!

### ***Vulnerability clearinghouse Secunia releases new research suggesting nearly all Windows PCs are at risk. Didn't we know that already?***

By [Bill Brenner](#), Senior Editor

December 04, 2008 — [CSO](#) —

Vulnerability clearinghouse [Secunia](#) just released a study that will surely send Windows users -- just about everyone -- running to the corner to assume the fetal position. Or not.

You see, the Copenhagen-based security company is telling us something we more or less knew already -- that [more than 98 percent of Windows computers have at least one unpatched application](#) and nearly half have 11 or more attack-prone programs.

The company reached that conclusion after running its Personal Software Inspector (PSI) utility on machines in the past week and finding one or more applications in need of available security updates. PSI scans Windows boxes for installed applications, then compares their version numbers to the most up-to-date versions, Computerworld scribe Gregg Keizer explained in his report on the matter. If they're different, it makes a record of it and spits back a link to the security update. [Secunia CTO Thomas Kristensen](#) says more than 120,000 people have downloaded PSI in the past week, and the company randomly selected 20,000 of those installations to use as lab rats.

"Most people keep Windows up to date because it's so easy to use Windows Update," Kristensen told Keizer. "[Adobe](#) Reader and Flash and Apple QuickTime are like that, too, as are browsers. But a lot of third-party [browser] plug-ins don't have any [update mechanism] and so people don't keep them updated."

Let me clarify: This isn't a swipe at Secunia for the conclusions it reached. It's a warning that vulnerability management vendors will probably start using this research to hound potential customers. They're just doing their jobs, but busy IT security practitioners may start getting e-mails about this and lose time worrying about whether or not this is a new problem.

To any Windows-based IT shop, the findings shouldn't come as a surprise.

We've reported before that many exploits target flaws for which a fix has long been available. A [recent estimate from Verizon](#), for example, suggested 90 percent of successful exploits these days involve vulnerabilities for which a patch has been available for six months or longer.

"For the overwhelming majority of attacks exploiting known vulnerabilities, the patch had been available for months prior to the breach," [Verizon](#) says on page 15 of its 2008 Data Breach Investigations Report. "Also worthy of mention is that no breaches were caused by exploits of vulnerabilities patched within a month or less of the attack." The lesson was that a patch-deployment strategy focusing on coverage and consistency is far better at preventing data breaches than "fire drills" attempting to patch particular systems as soon as patches are released, the report noted.

[Kaspersky Lab](#) Security Evangelist Ryan Naraine made the point that enterprises continue to struggle with the patching upkeep.

Companies are getting better at deploying security updates for their operating systems and Web browsers. But as Naraine noted, admins and users consistently overlook available patches for the third-party media players and .PDF readers everyone is using.

So while the Secunia research is good food for thought, nobody should be stunned.

The advice from security experts remains the same: It pays to take a regular inventory of all the systems on the network and have a process to track, install and manage patches. There's no one-size-fits-all

## How to Improve Cybersecurity: Ask Hackers

**Federal Times (12/01/08) Vol. 44, No. 40, P. 10 ; Carlstrom, Gregg**

A team of forensics experts and officials from the National Security Agency, the U.S. Air Force, the U.S. Computer Emergency Readiness Team (US-CERT), and the Defense Department Cyber Crime Center are working on a plan that would change the federal government's approach to cybersecurity. Under the plan, which will be open to comments from the public within the next several months, the White House would be encouraged to work more closely with hackers and computer forensics experts to learn about security gaps in federal computer systems. Federal agencies would then be given security recommendations that could override the thousands of pages of current guidelines from the National Institute of Standards and Technology (NIST). The SANS Institute's Alan Paller says the plan will take federal agencies' focus off of compliance with NIST guidelines--most of which do not actually improve security anyway--and put it back on securing systems. In addition, the plan will help address application security, which is generally not dealt with in the NIST guidelines. A final version of the plan could be given to the CIOs of federal agencies after the public comment period is over, says former Air Force CIO John Gilligan. If the CIOs like the plan, they could then present it to the Office of Management and Budget, Paller says.

## Laptops Now Meet State Security Standards

**Charlotte Observer (NC) (11/29/08) ; Bonner, Lynn**

The North Carolina Department of Health and Human Services (DHHS) has retrofitted nearly 4,000 of its portable computers with data encryption software to protect employees and consumers in the event of a theft, say agency officials. The agency is responding to an incident in October in which a laptop containing the Social Security numbers of state residents was stolen, potentially exposing the residents to identity theft. The 3,829 laptops in use by employees now contain security software that makes sensitive data indecipherable for unapproved users, says DHHS CIO Karen Tomczak in a letter to state CISO Ann Garrett. The agency paid more than \$101,000 to encrypt the computers and bring them in line with state security standards, though it did not put encryption software on 273 unused laptops because they contain no data, Tomczak said.

## You're Leaving a Digital Trail. What About Privacy?

**The New York Times (11/30/08) P. BU1 ; Markoff, John**

About 100 Massachusetts Institute of Technology (MIT) students have accepted free smartphones that track their every move as part of a research project, and these and other technologies are enabling collective intelligence, which promises to open up new social services and benefits. But collective intelligence also has the potential for misuse, such as allowing the government to identify members of a protest group by tracking social

networks. "Some have argued that with new technology there is a diminished expectation of privacy," says Electronic Privacy Information Center executive director Marc Rotenberg. "But the opposite may also be true. New techniques may require us to expand our understanding of privacy and to address the impact that data collection has on groups of individuals and not simply a single person." Cornell University sociologist Michael Macy observes that people and organizations are increasingly electing to interact with one another via digital technologies that record traces of those interactions, which enables scientists to analyze those interactions in ways that were deemed impossible five years ago. The MIT Media Lab's Alex Pentland says the surveillance-society traps that lurk in collective intelligence technologies can be evaded, and he has proposed precepts to ensure that people have ownership rights to their behavioral data. The principles dictate that people are entitled to possess their own data, that they control the data that is collected about them, and that they may redeploy, remove, or destroy their data as they see fit.

## **Carnegie Mellon CyLab Survey Unveils Major Gap in the Way U.S. Boards and CEOs Manage Cyber Risks**

**Carnegie Mellon News (12/02/08) ; Swaney, Chriss**

Carnegie Mellon University's CyLab has surveyed 703 corporate board directors and found that only 36 percent of the respondents said their board was directly involved in overseeing the management of information security. The boards were involved about 31 percent of the time in assessing risk related to IT or personal data. Only 8 percent said their boards had a risk committee that is separate from the audit committee, and 12 percent have established functional separation of privacy and security. Cybersecurity should be viewed as an enterprise risk management issue rather than an IT problem, say Carnegie Mellon researchers. "There is a clear duty to protect the assets of a company, and today, most corporate assets are digital," says CyLab's Jody Westby, lead author of the survey. The researchers offer recommendations for improving the corporate governance of privacy and security, such as establishing a board risk committee that is separate from the audit committee, reviewing existing top-level policies, and embracing security and privacy issues. "Without the right organizational structure and interest from top officials, enterprise security can't be effective no matter how much money an organization throws at it," says report co-author Richard Power.

## **Think tank panel recommends that feds make major cybersecurity changes**

Commission calls for new regulations on businesses, shift of responsibility from DHS

**By Grant Gross**

December 8, 2008 (IDG News Service) The U.S. government should overhaul its approach to cybersecurity by imposing sweeping new regulations on businesses and creating a centralized cybersecurity office in the White House, an outside group of experts recommended today.

The White House office is needed because the [Department of Homeland Security](#) isn't equipped to protect the federal government against cyberattacks, according to [a report issued by a cybersecurity commission that was set up last year by the Center for Strategic and International Studies](#) (CSIS). Many members of the Commission on Cyber Security for the 44th Presidency "felt that leaving any cyber function at DHS would doom that function to failure," according to the report.

The 96-page report — which was presaged in September when some commission members [testified at a congressional hearing](#) — also calls for new government regulations focused on protecting computer networks in the U.S. Many of those regulations would focus on refining government efforts to protect its own cyber infrastructure, but regulations on private industry are needed as well, the report said.

In addition, the report rejected the market-driven approach to cybersecurity advanced by [President Bush](#). "The strategy essentially abandoned cyber defense to ad hoc market forces," the report said. "In no other area of national security do we depend on private, voluntary efforts. We believe that cyberspace cannot be secured without regulation."

New regulations are needed for the IT, finance and energy industries — including the use of identity authentication credentials — and for supervisory control and data acquisition, or SCADA, systems, the report said. The commission also called on the government to change its own acquisition rules for IT products to focus more on cybersecurity.

Furthermore, the report recommended that federal officials should allow U.S. residents to use government-issued cyber credentials for their online activities.

"Cybersecurity is among the most serious economic and national security challenges we will face in the 21st century," wrote [James Lewis](#), director of the Technology and Public Policy Program at the [CSIS](#). "Our research and interviews for this report made it clear that we face a long-term challenge in cyberspace from foreign intelligence agencies and militaries, criminals, and others, and that this struggle will wreak serious damage on the economic health and national security of the U.S. unless we respond vigorously."

The DHS, which has been the lead agency focused on cybersecurity, can be strengthened, according to the CSIS commission. But "the nature of our opponents, the attacks we face in cyberspace, and the growing risk to national and economic security mean that comprehensive cybersecurity falls outside the scope of DHS's competencies," the report said. "DHS is not the agency to lead in a conflict with foreign intelligence agencies or militaries or even well-organized international cyber criminals."

Cybersecurity is no longer a homeland security or critical infrastructure problem, the report added. "This is far too narrow a scope," it said. "Cybersecurity is no longer (if it ever was) a domestic issue. It is an issue of international security in which the primary actors are the intelligence and military forces of other nations."

The report recommends that the DHS retain responsibility for the U.S. Computer Emergency Readiness Team and related functions, but it envisions a new White House National Office of Cyberspace that would coordinate and oversee cybersecurity efforts governmentwide. Currently, the government has hundreds of people working on cybersecurity issues, and this "too often resembles a large fleet of well-meaning bumper cars," the report said.

A DHS spokesman didn't immediately respond to a request for comment on the CSIS report. In September, after the congressional testimony by commission members, the agency dismissed their suggestions as "political posturing" and said their call to reassess cybersecurity responsibilities was "a classic 'inside the Beltway' gambit."

Members of the commission said in their testimony that the current approach isn't working. "We are under attack, and we are taking damage," Lewis told a House of Representatives subcommittee then. "The U.S is disorganized and lacks a coherent national [cybersecurity] strategy."

Other outside observers have also said that improving cybersecurity needs to be [a higher priority](#) for the next administration. Despite a variety of initiatives that were launched during the Bush administration, the cybersecurity effort is still seen as [a work in progress](#).

The CSIS, a nonpartisan think tank in Washington, launched the cybersecurity commission in August 2007 in an effort to make recommendations to the next U.S. president. More than 40 people, including employees of IBM, Oracle, Sun Microsystems, EMC and AT&T, have been serving on the commission.

The group's report also recommends that:

- The government develop a new national cybersecurity strategy that includes diplomacy, military action, changes in policy and the involvement of intelligence and law enforcement officials in the U.S.
- President-elect Barack Obama put a new emphasis on having the government work with the private sector, with clearly defined responsibilities and a focus on building trust with the business community.
- Congress increase spending on cybersecurity research and create a scholarship program to encourage more college students to obtain cybersecurity degrees.

"We are in a long-term struggle with criminals, foreign intelligence agencies, militaries, and others with whom we are intimately and unavoidably connected through a global digital network," the report said. "This struggle does more real damage every day to the economic health and national security of the United States than any other threat."

## Security Fed's Achilles Heel: Need Baked-in Security

(December 3, 2008) Speaking at a conference last week, US Air Force chief information officer (CIO) Lt. Gen. Michael Peterson called cyber security the US government's "Achilles heel" and said that best practices need to become ubiquitous for government agencies to be adequately protected from cyber threats. Peterson added that he believes that in the future, conflict will not become solely computer based, but that cyber attacks will be one strategy among many used by adversaries. Peterson said cyber security needs to be implemented in agency operations, not added on as an afterthought.

[http://www.nextgov.com/nextgov/ng\\_20081203\\_1212.php](http://www.nextgov.com/nextgov/ng_20081203_1212.php)

[Editor's Note (Pescatore): One good way the DoD could accelerate "baking in security" (vs. trying to sprinkle it on at the end) is to accelerate efforts to change the certification and accreditation process for IT systems from a paper-driven exercise to something that has more focus both on early design review for inclusion of security capabilities

\*and\* on actually detecting vulnerabilities in software before approving systems.

(Northcutt): You have to give the government some credit for moving in the direction of best practice, but they need to go further - to begin to shift the focus to be more on detection so they are ready when the inevitable compromises occur. We need to get better at detecting collected information being taken and "beamed to the mothership" and also detecting malware on systems themselves.

(Paller): Few security problems are more challenging than finding the "persistent presence" of attackers who have burrowed into systems and networks. The US government has prioritized solving that problem as one of the 12 key projects of the multi-billion-dollar Comprehensive National Cyber Initiative (CNCI).]

## Vulnerabilities play only a minor role in malware spread, says researcher

About two-thirds of all computer infections are due to duped users

**By Gregg Keizer**

December 8, 2008 (Computerworld) Computer users are their own worst enemies, a security company warned today, as it released data that shows software bugs were the source of just 5% of the past year's infections.

The majority of the attacks carried out by 2008's top 100 pieces of malware were caused by users surfing to malicious sites and then accepting some kind of download, [Trend Micro Inc.](#) researchers said today.

From Jan. 1 to Nov. 25, the top 100 attack programs infected 53% of their victims by duping them into downloading something from the Internet. An additional 12% of the infections tracked globally were caused by users opening e-mail attachments.

Just 5% of the infections were related to an exploit of a software vulnerability, according to Trend Micro's analysis.

"This is what we've been seeing all year," said [Paul Ferguson](#), network architect at Trend Micro. "This illustrates that social engineering seems to be playing a larger role than we thought. The problem isn't due to software vulnerabilities in, say, the browser."

Even so, Ferguson wasn't ready to completely dismiss the role that vulnerabilities play. "Because of the sheer overall volume [of malware], we're still talking about some staggering numbers of infections here," he said. Trend Micro and other security vendors have claimed that the number of individual pieces of malware jumped dramatically in the last year.

The numbers in North America were stacked even more against bugs as the cause of infections. While 63% of the infections from the top 100 pieces of malware in the region were caused by downloading something from the Web -- and 3% came from opening e-mailed attachments -- just 1.7% were related to security vulnerabilities.

"That's something we can't engineer against," said Ferguson. It's also why Trend Micro and other security vendors have stepped away from a pure antivirus detection and deletion model and instead have been bringing in other protective features, such as domain reputation ranking and URL filtering, to their products.

"We still have quite a way to go to get users to educate themselves about risks," said Ferguson. "They still manage to get duped into situations that put them at risk." As proof, Ferguson cited what he called "a new wave" of spam posing as shipping notices from UPS and [Wal-Mart](#). The messages have an attached file that they claim is a shipping invoice; when users open it to view or print it, their PCs are infected with a Trojan horse.

"The same [hacker] methodology still works," said Ferguson. "There's still enough low-hanging fruit that they don't even have to try very hard."

## **IT Security Outlook: Ominous**

**Government Computer News (12/04/08) ; Leffall, Jabulani**

The number of malicious applications in circulation has surpassed the number of legitimate applications, concludes a new Symantec report. The report also noted some of the security trends that were seen this year. For instance, the report said that botnet bugs, which allow hackers to control computers from a remote location, were increasingly prevalent during the last quarter of 2008. In addition, the report said that there was a significant number of data security breaches at companies of all sizes this year. The report notes that these breaches used a variety of different attack vectors and victimized a number of different organizations, including Walter Reed military hospital in Washington, D.C. The report also makes several predictions for security trends in 2009. For example, the report projects that users will likely see more spam and possible security issues with virtual machines and social-networking sites next year. Finally, the report includes some recommendations for security administrators and CIOs, including adopting security measures based on the individual needs and assessed risks at their organization.

## **Network Security: San Francisco Incident Raises Questions for CIOs**

**Government Technology (12/03/08) ; Collins, Hilton**

There are a number of steps organizations can take to protect themselves from insider attacks, such as the one launched by a network engineer for the San Francisco city-county government last summer that prevented officials from accessing the city's FiberWAN (wide area network). NASCIO executive director Doug Robinson says CIOs should pay attention to employees who appear to be stressed out by events in their lives, such as a divorce, foreclosure, or other type of financial instability. In addition, organizations also should pay attention to employees who are disgruntled because they were fired, demoted, or did not get a raise they thought they deserved. CIOs can minimize the risk of an insider wreaking havoc on their organization's network by having several different administrators who can do the same type of work and have access to the passwords, says Bill Schrier, the chief technology officer of Seattle's Department of Information Technology. Members of management also should be given oversight to ensure that job responsibilities are divided and supervised, Schrier says. Taking these steps would ensure that there is more than one way and more than one high-level administrator with top-level authority to access the system. However, distributing network responsibilities among different people can be difficult to do in state and local government because of tight budgets and government personnel policies, notes Gartner analyst John Pescatore.

## **Security Expert Warns of Continuing Threats From the Web**

**Computerworld (12/09/08) ; Rubio, Jenalyn**

The Internet and the proliferation of Web 2.0 applications will continue to be a breeding ground for attacks that affect both businesses and consumers, Sophos warns. Sophos' Jim Dowling says more than 15,000 new pages are infected daily, and 90 percent of these sites are legitimate. Furthermore, one out of every 100 Web searches yields an infected page, making it difficult for consumers to differentiate between a clean and tainted Web site. The security landscape is constantly changing due to the availability of cloud computing, third-party outsourcing of security services, USB drives, and third-party devices, Dowling adds. "In the past, people saw Web security

as a luxury and not a necessity," he says. "Until people start protecting themselves against the Web, it will continue to be one of the, if not the, major source of various security threats." Sophos' Julius Suarez says cybercriminals now understand that they can infect a wider range of victims by hacking into social networking sites and other legitimate pages instead of inviting users to a sham site loaded with malware.

## **Thieves Winning Online War, Maybe Even in Your Computer**

**New York Times (12/06/08) P. A1 ; Markoff, John**

Malware continues to overcome security professionals' efforts to defend against it. "Right now the bad guys are improving more quickly than the good guys," says SRI International's Patrick Lincoln. As businesses and individuals become increasingly involved in online communities, cybercriminals are given more opportunities to infect machines and commit crimes. The Organization for Security and Cooperation in Europe estimates that credit card thefts, bank fraud, and other online scams rob computer users of \$100 billion annually. In late October, the RSA FraudAction Research Lab discovered a cache of 500,000 credit-card numbers and bank account log-ins that were stolen by a network of zombie computers run by an online gang. "Modern worms are stealthier and they are professionally written," says British Telecom chief security technology officer Bruce Schneier. "The criminals have gone upmarket, and they're organized and international because there is real money to be made." Meanwhile, malicious programs are becoming increasingly sophisticated, with some programs searching for the most recent documents on the assumption that they are the most valuable and others stealing log-in and password information for consumer finances. Microsoft researchers recently discovered malware that runs Windows Update after it infects a machine to ensure the machine is protected from other pieces of malware. Purdue University computer scientist Eugene Spafford is concerned that companies will cut back on computer security to save money. "In many respects, we are probably worse off than we were 20 years ago," he says, "because all of the money has been devoted to patching the current problem rather than investing in the redesign of our infrastructure."

## **Survey Finds Database Security Lacking**

**ITPro (12/08/08) ; Knights, Miya**

Although the overwhelming majority of IT decision-makers at large multinational companies say they are confident that most or all of their confidential data is protected, in reality that information is not as secure as they think it is, concludes a survey by the Application Security and Enterprise Strategy Group. Nearly 84 percent of 179 IT decision-makers at multinational companies with at least 1,000 employees report being confident about the protections for their confidential data, though they also note that their organizations have failed major enterprise-wide and industry-specific security audits more than a third of the time. The survey also found that 63 percent of respondents said the security of their organization's database--where customer and employee information is typically held--is solely dependent on manual processes. This dependence on manual processes means organizations are always taking a reactive, not proactive, approach to attacks, says Application Security's Tom Bain. Finally, the survey found that more than 60 percent of respondents said their organization had suffered at least one data breach in the past 12 months. Bain says the survey's results prove that organizations must take pre-emptive action to deal with security threats and have the right people, policies, and processes in place in order to improve cybersecurity.

## **Web 2.0 Security: 3 Key Questions**

**CIO Insight (12/03/08) ; Likens, Scott**

In an effort to cut channel costs and boost sales in this weak economy, companies will increasingly take advantage of Web 2.0 technologies such as widgets, wikis, and blogs, writes consultant Scott Likens. However, cybercriminals also will be able to exploit these technologies by using them for a variety of malicious purposes, such as installing key logging software on Web surfers' machines and directing them to sites that steal their credit card information. Compounding this problem is the fact that Web 2.0 security is not a high priority for many companies, but CIOs and other IT security professionals can protect their organizations from the threat posed by Web 2.0 technologies by answering several questions, Likens says. First, CIOs need to ask themselves whether they need to establish a wide-open social network that all of their organizations' employees can use to

collaborate with one another, or whether they can use something more structured to foster better communications between departments. CIOs also need to ask themselves whether the business case for using Web 2.0 technologies supports the need for additional security measures. Next, CIOs need to determine who is responsible for overseeing consumer-generated information, or wikis, on their organization's site. Finally, CIOs should determine the level of due diligence necessary to assess the risks posed by Web 2.0 technologies.

## Obama administration to inherit a real mess on Real ID

President-elect's position still unclear on controversial law setting national ID standards

By Jaikumar Vijayan

December 11, 2008 (Computerworld) As [President-elect Barack Obama](#) prepares to take the reins in Washington, it remains unclear how his administration will deal with [the controversial Real ID](#) national identification standards put in motion by predecessor [George W. Bush](#).

Thus far, Obama himself has made almost no public comments about the Real ID initiative, which calls for driver's licenses and other state-issued IDs to include digital photos and be machine-readable so the information on them can be captured by scanning devices. And on the one occasion in which Obama had an opportunity to vote on an issue related to the Real ID Act in the Senate, he didn't cast a ballot.

Meanwhile, [Arizona Gov. Janet Napolitano](#), Obama's [choice to be secretary](#) of the [U.S. Department of Homeland Security \(DHS\)](#) — the agency responsible for implementing the Real ID rules — previously signed a bill barring her state from participating in the program. Given that fact, it's uncertain how effective she would be in pushing for adoption of Real ID in her expected new role or if she would even be inclined to do so in the first place.

The Real ID Act was approved by Congress and signed into law by President Bush in 2005 as part of the government's effort to combat terrorism. But the law has evoked widespread [criticism from privacy advocates](#) and civil rights groups, which say it would create a de facto national identity card system that would be hard to manage and even harder to secure. Even a [DHS advisory committee](#) voiced reservations about the Real ID effort last year because of privacy, security and logistical concerns.

Over the past two years, Real ID has also become a bone of contention between the DHS and state governments that see it as an attempt by federal officials to force unwanted ID standards down their throats, while also making the states pay for the program. Several states have joined Arizona in refusing to participate, with the list including Arkansas, Idaho, Maine, Montana, [New Hampshire](#), South Carolina and Washington.

"I don't think anybody in the next administration, including Napolitano, wants to deal with Real ID. It's a real stinking mess," said Jim Harper, director of information policy studies at the Cato Institute, a Washington-based public-policy research organization with libertarian leanings. "Most likely, they will find the quietest way they can to get it off their plates."

Other provisions in the Real ID law require participating states to store digital images of IDs for seven to 10 years and for their driver's license databases to be linked to essentially create a single large system with shared access. There's no mandate that states issue Real ID cards. But under the law, all citizens will eventually need ID cards that comply with the Real ID requirements in order to board planes, enter federal buildings and receive benefits from the federal government.

The outpouring of protests has prompted the DHS to [ease up on the implementation deadlines](#) and modify some of the requirements in an attempt to make Real ID more palatable. For instance, under the final rules set by the agency last January, driver's licenses issued under existing state standards will continue to be accepted as identification by federal agencies until December 2014. And people aged 50 and above won't have to show Real ID cards until December 2017.

In addition, after initially setting a deadline of last March for states to request an extension on meeting an initial set of Real ID requirements that were supposed to be implemented by May, the DHS backed off of threats to begin [enforcing the law's rules](#), even going so far as to [issue extensions](#) to states that didn't actually ask for one.

Those moves weren't just an attempt by the DHS to appease state officials who are opposed to Real ID, Harper said, adding that the agency decided to slow down and pass the baton to the next administration. DHS officials "realized there's just no way they're going to win this" by taking a confrontational approach, he said.

Estimates that the final tab for the Real ID program could exceed \$17 billion also make it a challenge to push forward, according to Harper. Even so, he doesn't expect Obama to seek an outright repeal of the law because that would likely generate criticism that the new president was being soft on terrorism and immigration-control issues.

The extensions to the original May deadline for initial Real ID compliance give states until next December to meet those requirements. At this point, the only reasonable way forward is for the DHS to work more cooperatively with the states on Real ID implementations instead of continuing to "dangle sabers over their heads," said [Chris Dixon](#), an analyst at Input, a government-focused consulting firm in Reston, Va.

"I'm amazed that the Bush administration has allowed this to smolder for so long," Dixon said. "This should have been put to bed long ago."

According to Dixon, the one public comment that Obama has made about Real ID came during a primary campaign debate, when he voiced his opposition to the way the law was being implemented and the burdens it imposed on states. A perusal of Obama's [Senate voting record](#) on the Project Vote Smart Web site shows that as a senator from Illinois, Obama didn't vote on a proposal relating to Real ID funding.

But whatever position the new administration takes, the fact remains that many of the standards required under Real ID are already being implemented by states as part of their own efforts to improve security, Dixon said. As a result, he noted, moving the Real ID program forward may require little more than a willingness on the part of the DHS to see if those efforts are enough to qualify as complying with the law.

Dixon noted that Napolitano's experience as the governor of a state that is fighting against the Real ID initiative should have given her insight into the issues being faced by the other states as well. If she's confirmed to head the DHS, he said, "Napolitano could sit down with the governors and try to find a way out of this impasse."

## **T-Mobile, AT&T banned from saying their mobile voice mail is safe**

The cell phone providers falsely advertised the security of their systems

**By Robert McMillan**

December 11, 2008 (IDG News Service) Mobile service providers AT&T Inc. and [T-Mobile](#) have been banned from saying that their voice-mail systems are safe from sabotage after agreeing to permanent injunctions filed in a Los Angeles court.

The cell phone providers falsely advertised the security of their systems, according to the Los Angeles District Attorney's Office. During an investigation, "cell phones purchased by undercover investigators were easily hacked into, enabling the voice mail to be changed at will," the district attorney said in a statement today.

"Hacking into voice mail allowed messages to be changed or erased. Important information could be removed from the voice mail and phony information could be inserted," the district attorney said. "Imagine the havoc that could result."

Investigators were able to hack into voice-mail accounts using something called a [SpooferCard](#). [SpooferCard's](#) software lets people display any number they want on Caller ID. It has been used to access voice-mail systems that do not require passwords, such as those used by [Cingular](#) (now part of AT&T) and T-Mobile.

Two years ago, SpoofCard suspended [Paris Hilton](#)'s account after gossip sheets linked her to the voice mail hacking of her celebrity rival, Lindsay Lohan. At the time, SpoofCard said it had suspended more than 50 customers for using the service to hack into voice-mail accounts.

In a statement, T-Mobile said that customers who want to add password protection to their voicemail should call voicemail, then press the star key to interrupt the greeting, and then press 5 to be prompted to change their password.

"T-Mobile cooperated with the district attorney and is pleased to have reached resolution on the issue," the company said.

As part of the settlement, AT&T will pay \$59,300 in penalties and T-Mobile will pay \$25,000. The case was heard in the Superior Court of the State of California for the County of Los Angeles.

AT&T and TelTech did not immediately return calls seeking comment.

In a separate civil action, SpoofCard's parent company, TelTech Systems, has agreed not to advertise its product as "legal in 50 states." It is illegal in California and some other states, the district attorney's office said. TelTech will also pay a \$33,000 fine.

## McAfee's Virtual Criminology Report

(December 2008)

McAfee's annual Virtual Criminology Report arrived at three key findings. First, cyber crime is not a priority of governments around the world; the low priority is compounded by other pressing international concerns such as terrorism and the economy. Second, because the cyber world knows no borders, prosecution for cyber crime often proves difficult. Finally, law enforcement organizations lack adequate training in all aspects of cyber crime, from forensics to court proceedings. The report makes a number of recommendations to mitigate the problems it describes: increasing training for law enforcement officers, prosecutors and judges; incentives for Internet service providers (ISPs) to adhere to best practices for network design and operation; mandatory security breach disclosure; legal responsibilities for organizations in both the private and public sectors for Internet-related data breach or loss; consumer education; limited liability for software vendors that do not abide by best practices for security in design and operation; and "the use of government procurement power to demand significantly higher standards of security in software and services."

