

# Security Trends Report

04/08

## Stolen hardware basis for most breaches

SAN FRANCISCO, Calif. -- While the number of unique variants of malicious software more than quadrupled in 2007, lost laptops and storage devices -- not malicious software -- were the most common cause of a data breaches, security firm Symantec said in its latest *Internet Security Threat Report* released on Tuesday.

The [report](#), based on data from more than 40,000 network devices and 120 million systems running Symantec software, found more than 700,000 new threats in the 2007, an increase of 468 percent over 2006. The attacks increasingly focused on stealing confidential information, with 68 percent of the top-50 threats targeting confidential information in the second half of 2007, up from 53 percent during the same period in 2006.

"This is not your mom's malicious code," Steve Trilling, vice president of security technology and response for Symantec, said during a morning keynote session at the RSA Security Conference. Symantec is the parent company of *SecurityFocus*.

Yet, the theft of computers and storage devices, not malicious code, accounted for the majority of lost data. In the latter half of the year, such physical theft accounted for 57 percent of data breaches, up from 46 percent in the first half of 2007, the report stated. While the government had only the second highest number of breaches -- 20 percent of the total compared to 24 percent for the education sector -- those breaches accounted for 60 percent of identity theft, the report stated.

Vulnerabilities in Web sites are increasingly being attacked to compromise trusted sites and use them to host malicious code, the report stated. More than 11,250 site-specific cross-site scripting vulnerabilities were identified in the latter half of 2007, compared to almost 7,000 flaws in the first half of the year, Symantec said. Only about 4 percent of the vulnerabilities had been patched by administrators during the period, the company said.

## State agency moves to plug USB flash drive security gap

Washington child-support unit rolls out 200 new thumb drives with management, security tools - By Brian Fonseca

- March 17, 2008 (Computerworld) Security officials are issuing USB flash drives to workers in the state of Washington's Division of Child Support as part of a new security procedure established to eliminate the use of nonapproved thumb drives by workers collecting and transporting confidential data.  
The state has so far distributed 150 of 200 [SanDisk Corp. Cruzer Enterprise](#) thumb drives to unit supervisors in the division who manage collections teams in 10 field offices, said officials (see also "[Review: 7 secure USB drives](#)").  
Brian Main, the division's data security officer, said the new drives promise to help officials keep better track of mobile data by integrating them with Web-based management software that can centrally monitor, configure and prevent unauthorized access to the miniature storage devices.  
"We do periodic risk analysis of our systems, and one of the things that came up is the use of thumb drives -- they were everywhere," said Main. "We had a hard time telling which were privately owned and which were owned by the state." He also said that officials had difficulty keeping track of what data was stored on the workers' thumb drives.  
Main said the division plans to manage and back up the new drives using SanDisk's Central Management & Control server software, which will soon be installed at the division's headquarters in Olympia. The software, which relies on a Web connection to directly communicate with agents on the tiny flash drives, can also remotely monitor and flush any lost drives, he said.  
Each field office will run a copy of the software to handle localized management needs, he said.  
Officials in the division's training operations will get Cruzer Enterprise devices with 4GB of memory to store large presentations and screenshots. Enforcement personnel will get devices that store 1GB, Main said.

Main said the division first looked at Verbatim America LLC's thumb drives in its effort to improve security but ultimately turned to the SanDisk technology because of its support for [Microsoft Corp.'s Windows Vista operating system](#).

Cruzer Enterprise provides 256-bit AES encryption and requires users to create a password upon activation. The device automatically deletes all of its content once someone has tried 10 times to access it using incorrect passwords. Main said the self-encrypting capability was removes the "human component" from managing confidential data, a key feature for the agency.

The Division of Child Support collects about \$700 million annually in child-support payments from noncustodial parents. The agency, part of the state's Department of Social and Health Services, manages 350,000 active child-support cases annually, noted Main.

Sensitive data transported by off-site workers includes tax documents, employer records, criminal histories and federal passport data of some agency clients, Main said. At the least, he noted, the drives include the names, dates of birth and Social Security numbers of children serviced by the agency.

The state began rolling out the Cruzer drives late last year after recalling the thumb drives used by workers. Most of those had been purchased independently by the employees, causing myriad problems for security personnel, Main said. The new policy requires workers to use the drives supplied by the agency. Main said he eventually plans to destroy all existing thumb drives collected as part of the security policy change.

Most companies are too enamored of the convenience, portability and low cost of USB flash drives to consider their [threat to security](#), said [Larry Ponemon](#), chairman of [Ponemon Institute LLC](#), a Traverse City, Mich.-based research firm.

"I think a lot of organizations are asleep at the switch. They don't see this as a huge problem, and it obviously has the potential to be the mother of all data-protection issues," said Ponemon. "A lot of organizations believe if you have a good [security] policy and you educate people and ask them to be good, that's sufficient. The reality is, thumb drives create a lot of uncertainty because they contain enormous an amount of information."

A December 2007 survey of 691 IT security practitioners by Ponemon Institute asked respondents if they believed most employees would report a lost laptop or memory stick. While 78% said that employees would likely notify IT about a lost laptop, only 25% expected that workers would report a lost USB flash drive.

"The general perception is no one will report a lost USB memory stick because they're so cheap -- and the embarrassment factor. It's hard to even know all the different instances where information [on them] is lost or stolen," remarked Ponemon.

The agency is in talks with [ControlGuard](#) to deploy the security provider's Endpoint Access Manager Server and Endpoint Agents across its network. Access Management Server sends security policy information from a central location to agents installed at specific data points to enforce protection and monitor activities. Main said the technology would allow his office to restrict authentication and control data output access on PCs, hard drives and printers.

## Canadian Firm to Offer Data Breach Insurance (March 13, 2008)

As data security breaches appear more and more frequently in the news, at least one Canadian insurance company is starting to offer a product that would cover costs incurred by companies when they have suffered a data privacy breach. The policy would cover the cost of fixing computer damage as well as costs associated with customer notification and reimbursement and compensation paid to credit card companies for losses from fraud. The coverage is structured to address Canadian data privacy laws.

<http://www.theglobeandmail.com/servlet/story/LAC.20080313.RINSURANCE13/TPStory/Business>

[Editor's Note (Schultz): Insurance against security incidents in general has not caught on all that well in the information security arena for a number of reasons. However, this new type of insurance is likely to fare much better because of the widespread concern about and high likelihood of data security breaches.]

## The top 10 security land mines

Companies can actually worsen their risks by failing to take these commonsense approaches to security

By [Matt Hines](#)

March 17, 2008

Many companies spend a small fortune and deploy a small army to secure themselves from the many security threats lurking these days. But all those efforts can come to naught when making any of these common mistakes. The results can range from embarrassing to devastating, but security experts say that all are easily avoidable.

Here are the 10 most common security land mines that experts say you need to avoid.

### 1. A slip of the finger reveals the company secret

Many of the most prevalent security issues are the result of small technological habits that can easily be avoided.

For instance, imagine how many inadvertent data loss events could be eliminated if more users were instructed to turn off the e-mail address "[autofill](#)" feature in Microsoft Outlook and other messaging systems, said Steve Roop, senior director of marketing and products at Symantec.

"When employees are quickly addressing their e-mails, they inadvertently tab and select the wrong name in haste. The employee thinks he is sending an e-mail internally to Eric Friendly, but autofill instead sent it to Eric Foe," Roop said. "We've all done this. [But] if the e-mail contained sensitive data about a proposed merger or acquisition, then the secret is out."

As much as 90 percent of all information leakage events are tied to inadvertent e-mail foibles, including the autofill accidents and mistakes in handling encryption or misinterpreting usage policies, Roop said. Just the simple act of turning off something like autofill could save businesses a lot of headaches at no extra cost, he said.

### 2. People give away passwords and other secrets without thinking

More often than not, users -- not outside intruders -- are responsible for coughing up the passwords and personal data that allow attackers to break into their computers and their employer's networks to wreak havoc and tarnish their names.

Despite all the education people have been given about phishing, spyware programs, and [hacked Web sites](#), many users are still willing to hand out their data whenever it is requested without checking to ensure that they aren't duped or misled, said Dave Marcus, security research and communications manager at McAfee. "People assume the legitimacy of sites as presented; this is fundamentally incorrect in a Web world," Marcus said. "The easiest way to steal someone's identity online is simply to ask them for it."

### 3. A trusted partner ends up not being so trustworthy with your data

Another common security error is found among users who assume that it is fine to send sensitive information such as human resources data to business partners or outsourcing services providers, Roop said. This land mine is made worse when the messages are sent unencrypted.

"The land mine is making the assumption that the person at the HR outsourcer isn't going to send the spreadsheet anywhere else or store the data improperly on their unsecured laptop," he said. "This land mine is true whenever sensitive data is shared via e-mail as part of a business process with third parties."

### 4. Web-based apps can be portals to leaks and thieves

A common behavior that leads to a lot of security problems includes the use of Webmail or allowing workers to access music-downloading and file-sharing services from the company network, said Marcus.

Such Web-based apps [bypass your security filters](#), as in the case of Webmail, or open a channel to the outside that may carry viruses or worse into your organization.

And if your employees take work home, these risks are magnified. If they use your computers and also do personal activities over the Web, those computers could be compromised, Marcus said. If they bring the data home -- via e-mail or a thumb drive -- they risk it getting lost or stolen.

All of these problems can be avoided fairly easily through enforcement of policies that require the use of secure mail clients over VPNs or encrypted channels (in the case of e-mail), or not allowing users to install apps on their work computer or copy data to removable media (in the case of taking work home). Much of this can be managed through security policies and systems management apps. One difficult channel to block is the use by employees of e-mail to send themselves data, though encryption can help.

#### **5. Hoping the worse doesn't happen only makes it worse**

Nobody wants to have a data breach, but you need to act as if one will, advised Kevin Mandia, chief executive of Mandiant, which specializes in post-breach analysis services and software tools. Every organization [can take steps](#) to lessen the impact of a breach once it happens. Unfortunately, most companies wait until it is too late to test or even create their response strategies, he said.

Every company should record the data flow, from who had access when to what systems used the data. But few do, Mandia said. "There's no question, the most common error we see is failure to document what happened," he said. "People hire us and the first thing we ask for is any related documentation that people already have. Most often, people will hand terabytes of data and no formal documentation. Technicians stink at it, and lawyers don't mandate it. So in almost every incident, we go in and ask them what happened and the response is the sound of crickets chirping."

#### **6. Avoiding or diluting response leadership makes breaches worse**

Companies also seriously inhibit their ability to respond to breaches by failing to appoint a single leader or small team to spearhead efforts to respond to incidents and chase down important details.

In many firms, the process devolves into a game of pass-the-buck, while others involve so many people in the breach response effort that they actually become a hindrance to the related investigation.

"We often respond and no one is in charge, no one wants to be, and as a result, no one knows what dedication of resources to give the incident in terms of money, tools, or technologies, and no one person individually can balance their day job with the amount of resources needed to handle a major incident," Mandia said.

"On the flip side, some companies now bring too many people to the decision-making table while still trying to respond. We show up and we're immediately briefing 12 people -- and 10 don't need to be there," he said.

#### **7. Handling breach details sloppily tips off the perp**

Another common problem is that companies typically fail to establish a "need to know" approach to breaches, which makes it harder to carry out baseline investigations as workers find out about an incident and immediately try to protect their own interests.

If insiders are involved in the problem, they also gain the advantage of knowing that the gig is up and may stop telltale behavior useful to investigators — and often try to cover their tracks, Mandia said.

#### **8. Trusting "silver bullet" technology hides real threats**

As regulatory measures that involve IT and data security interests continue to multiply, businesses have invested a lot in technological solutions to plug the holes. But companies commonly believe that installing a specific technology or meeting some individual aspect of a regulation is a [silver bullet](#) or a quick fix. It's neither.

"The biggest problem I see is people thinking that simple things like deploying anti-virus [software], patching, and running vulnerability scans are actually what it means to be compliant. They're not approaching it from a risk management standpoint — they're just checking the boxes," said Mike Rothman, an analyst with Security Incite.

Companies often compound this fools' paradise by auditing their limited security fixes and taking a passing grade as confirmation that no more work is needed. "People often think that once they have a positive audit, they're done," Rothman said. "Then the bad guys prove to them that they're not."

#### **9. Spending unthinkingly wastes resources you might need for important threats**

Another compliance-related security trap that companies frequently fall into is spending the same effort or expense to protect IT systems with wildly different levels of importance to their organization's security and success, Rothman said.

"Some people make the mistake of treating all security issues equally, and spend the same amount of time and money defending an old application that only five people use that they spend on an online application used by all of their customers," he said.

That approach not only wastes money, but it also can leave more important problems to later consideration — or maybe none at all, once the budget has dried up. "Security people often don't know how to prioritize," Rothman said. "They should look at what happens if something specific breaks and look at how to drive spending from there."

## 10. Don't save the wrong data

In another common scenario that spells disaster for both security and compliance interests, many companies that process credit and debit cards inadvertently leave transaction logging systems on that store account information. This logging can lead to customer data breaches and PCI (Payment Card Industry) audit failures.

"Naturally, they don't realize they are storing the data a hacker or malicious employee would need to create fake plastic credit cards," said Symantec's Roop. "This is the cardinal sin of PCI compliance. We actually saw this example at a [recent] prospect. It is a big land mine that most likely will result in a failed PCI audit."

Even companies not collecting card data need to make sure that they only save the information they actively need to do business, Roop said. Keeping anything on hand that could be misused by attackers without a clear need to store that data is asking for trouble, he advised. And if it must be retained, then be sure to build a protection method for it as well.

## "Botnet Scams Are Exploding"

USA Today (03/17/08) P. 1B ; Acohido, Byron; Swartz, Jon

Botnets send out 91 percent of all emails--most of which are spam--and are responsible for millions of dollars in theft from consumers, Cloudmark reports. Users behind these networks prey on vulnerable systems and users through illegitimate banking Web sites, spam, denial-of-service attacks, and infections. While botnet attacks at one time represented only a fraction of total Internet breaches, security firm Damballa estimates that these networks release more than 20 times as many attacks now than 18 months ago--up to 7.3 million daily, compared to 333,000 daily in August 2006. A Russian collection of botnets known as Zbot recently deluged systems in the United States, the United Kingdom, Italy, and Spain, making off with over \$6 million. "It's like a disease you can't even feel," says Support Intelligence CEO Rick Wesson. "The mechanisms we use to protect our networks simply are not working."

## Analyst: Money will lead to more mobile spying programs

By Jeremy Kirk

March 28, 2008 (IDG News Service) Spying programs for mobile phones are likely to grow in sophistication and stealth as the business of selling spying tools grows, according to a mobile analyst at the Black Hat conference on Friday.

Many of the spy programs on the market are powerful, but aren't very sophisticated code, said Jarno Niemela, a senior antivirus researcher at Finnish security vendor [F-Secure](#), which makes security products for PCs and mobile phones.

But there is increasing evidence that money from selling the tools will create a stronger incentive for more accomplished programmers to get into the game, which could make the programs harder to detect, Niemela said.

Niemela said his prediction follows what has happened with the malware writers in the PC market. Many hackers are now in the business of selling easy-to-use tools to less technical hackers rather than hacking into PCs themselves.

One of the latest tools on the market is Mobile SpySuite, which Niemela believes is the first spy tool generator for mobiles. It sells for \$12,500 (U.S.) and enables a hacker to custom-build a spy tool aimed at several models of [Nokia](#) phones, Niemela said.

The number of mobile spyware programs pales in comparison to the number of such programs available for PCs. However, mobile spying programs are harder to track, since security companies such as F-Secure don't see as many samples circulating on the Internet as they do of malicious software for PCs.

However, anecdotal evidence has emerged that enterprises may be increasingly encountering mobile spyware on their fleets of phones. The clues have come from companies that are relatively cagey when talking about what they have seen.

"There have been certain cases of corporate customers asking very detailed questions about spy tools and not mentioning why they need the information," Niemela said.

Some of the more well-known spy programs are Neo-Call and FlexiSpy. Neo-Call is capable of secretly forwarding SMS (Short Message Service) text messages to another phone, transmitting a list of phone numbers called, and logging

keystrokes. FlexiSpy has a neat, Web-based interface that shows details of call times, numbers and SMS messages, and it can even use a phone's GPS receiver to pinpoint the victim's location.

Hackers usually need to have access to the phone itself to install the software. And OS manufacturers such as [Symbian](#) have enabled security features such as application signing, which is intended to prevent rogue programs from being installed on a phone.

Most rogue spying programs leave traces on the phone, and analysis tools can be used to check a phone's processes and file system to see if something is there that shouldn't be, Niemela said.

But there are ways that less technical users can get a hint they've been hacked. One simple clue is if a colleague of the victim knows something that he shouldn't, Niemela said.

Also, mobile spying programs have to transmit their data. If the spy program sends data over GPRS (General Packet Radio Service), the network operator will demand payment. "As long as it has to use a paid channel, it can't escape the operator's bill," Niemela said.

Another way is to replace the phone's SIM card with one that allows for real-time monitoring. SMS messages can then be sent to the phone, which in many countries are free to receive. If the monitoring reveals outgoing data traffic after SMSes are received, the phone could be hacked. It's also possible to check if the GPRS connection icon lights up after a message is received, Niemela said.

Niemela offered some defenses against mobile spyware: Keep the OS up to date, as manufacturers are usually working to counter new devious software. The use of a mobile antivirus program is also prudent, he said. People should also use password protection to block access if someone gets a hold of the device.

Administrators can also regularly "flash" phones to wipe off malware, as well as ensuring that phones install only signed applications.

And when the phone is out of a person's hands, another option is to put the device in a tamperproof container. But "for most people, this is way too [James Bond](#)," Niemela said.

---

**Mar 26, 2008**

## **[Techworld: Supermarket for Stolen Credit Cards Found](#)**

If you've ever wondered where stolen credit card numbers end up, Finjan might have part of the answer. The security company-cum-cybersleuthing outfit has uncovered a Web site supermarket for stolen card data.

The 'SellCVV2' Web site, as it is called, was found to be trading the card numbers and other data in a number of sophisticated ways. Criminals visiting the site would be able to earn discounts based on volume bought and choose from a range of tiers, starting at the least valuable Classic Visa or MasterCard -- those with the lowest credit limits -- through more valuable Gold, Platinum, and Corporate levels.

According to Finjan, prices ranged from US\$38 for small volumes of premium card numbers, down to \$10 for the equivalent low-limit cards in chunks of 100 at a time. Criminals worried about being stung themselves by non-working cards were being offered "guarantees" as well as trial data sets.

No breakdown was given on where or how the cards might have been stolen, but they are believed to be from around the globe and possibly culled using online Trojan-related techniques.

"The site, which appears to use Google's Blogspot service, is typical of a number of portals promoting the exchange of fraudulent card data. But what is apparent from the SellCVV2 site is the level of commercialization of the traders involved," said Finjan's CTO Yuval Ben-Itzhak.

The site gets its rather apt name from the three-digit CVV2 (Card Verification Value 2) number on the reverse of credit cards, essential for remote transactions, and implying that the numbers themselves are also being supplied.

All this after Finjan reported recently on a similar site found to be selling a large number of valid FTP server logins, many used by large companies around the world. As with SellCVV2, that site used a sophisticated trading model.

"If further proof were needed that there is a very serious problem facing the card acceptance and processing industry, this is it. The level of sophistication shown on the site, acts as a clear warning to anyone who thinks card fraud is a containable problem," said Ben-Itzhak.

## **HONEYWELL STUDY: ORGANIZATIONS MOVING TO CONVERGENCE**

*Mar 18, 2008*

Honeywell has released survey results that reveal how some organizations are integrating physical security measures such as video surveillance and access control with traditional IT security systems. According to "Enterprise Threat Management and Security Convergence: A Benchmarking Study," significant barriers still exist that prevent organizations from converging their systems and many of these organizations remain conflicted on how to best attain optimal results.

More than 50 chief information officers, chief security officers and chief information and security officers of U.S.-based global companies with revenues from \$1 billion to more than \$100 billion participated in the survey.

"The convergence of physical and traditional IT systems can provide compelling security benefits for an enterprise," says Mark Diodati, Identity and Privacy Strategies senior analyst with Burton Group. "Successful compliance initiatives can be enhanced when the organization adopts a holistic approach for managing access to these systems."

Most respondents indicated increased interaction between their security and IT functions:

- 63 percent said their security and IT organizations "had a formal coordination mechanism"
- 10 percent stated the two functions are run as one entity within their organizations
- 52 percent noted their security functions had a formal working relationship with their audit and compliance functions, while 11 percent said those functions are combined

The majority of respondents (nearly 73 percent) believe vulnerabilities in either physical or IT security can lead to a breach in the other system:

- 91 percent of the responding companies showed an increase in security investment
- 75 percent of which said those investments increased by more than eight percent
- 31 percent suggested a greater than 12 percent rise

"This study reinforces that companies are increasingly concerned with protecting their information assets as well as their physical assets, and they recognize that integrating once-disparate systems can be effective in addressing threats," says Jim Ebzery, senior vice president of Identity and Security Management at Novell, which recently collaborated with Honeywell to develop a converged physical-IT security system. "How they choose to implement convergence varies on a number of factors including internal roles and overall attitudes about its effectiveness."

When asked whether having physical security systems on IT backbones is a security risk, the answers were split: 59 percent said no while 42 percent said yes. The results also differed with regards to personal responsibility for organizing responses to a coordinated physical-IT security attack:

- 34 percent said there isn't a single internal contact
- 27 percent said the Director of Security is responsible
- 14 percent said a single CSO deals with the threats
- 14 percent said the Crisis Management Group is ultimately responsible

When asked to define "convergence," responses varied from using IT backbones for security systems to automating manual processes through an IT system. Additional responses included the strategic partnership of physical and IT security organizations in risk management. Although these responses varied, they reinforced existing research.

Thirty-three percent of respondents said they envision convergence happening within their organizations in the next two to five years, while another 33 percent said convergence will never happen. The barriers associated with true convergence include: Turf control, complexity and skills needed to handle multiple disciplines, budget conflicts, compatibility across groups, lack of technical platforms and expanding privacy laws

"A multitude of elements must be in place for convergence to truly improve overall security and streamline internal business processes," says John Lorenty, Honeywell Systems Group president. "A strong IT backbone and common protocols are essential for convergence to be effective. Most importantly, a strong partnership between cross-functional teams is critical to ensure that each converged solution meets the challenges of ever-evolving threats."

## **Feds losing war on information security, senators told**

By Gautham Nagesh March 13, 2008

The federal government is losing the battle to keep its information systems secure, according to expert testimony at a Senate hearing on Wednesday.

Officials from the Government Accountability Office, Office of Management and Budget and industry groups testified that the number and intensity of attacks on the government's networks increased significantly during 2007. They spoke at a hearing of the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management.

"Quite frankly, the bad guys are winning," said Tim Bennett, president of the Cyber Security Industry Alliance. He added that attacks on federal networks were now occurring on a daily basis, and are now backed by large criminal enterprises and enemy states with tremendous financial resources. "This is warfare, and it needs to be stopped," Bennett said.

The hearing's focus was on the effectiveness of the 2002 Federal Information Security Management Act. Sen. Tom Coburn, R-Okla., pressed the panel on whether, six years later, agencies are focused on real security issues or simply trying to comply with the law's provisions. "How much of FISMA is paperwork vs. actual security?" asked Coburn.

"That depends on how an agency goes about doing its work," said Karen Evans, administrator of e-government and information technology at OMB. "FISMA has put together a framework, but if [an agency] does it just for compliance, then it's purely a paperwork exercise."

Responding to the same question, Gregory Wilshusen, director of information security issues at GAO, said that FISMA measures the implementation of control activities, not the actual effectiveness in preventing cyber attacks.

"Despite the progress reported by agencies, they continue to confront longstanding information security control deficiencies that limit the effectiveness of their efforts in protecting the confidentiality, integrity and availability of their information and information systems," Wilshusen said. He noted that 20 of 24 agency inspector generals have identified significant weaknesses in the financial management systems of their agencies.

When asked about the dramatic jump in attacks in both the private and public sectors, Evans acknowledged that OMB found [a 60 percent rise](#) in the number of reported incidents from 2006 to 2007. But she attributed the increase in large part to improved reporting. Bennett had a different take.

The increase "is real, and the federal government is not immune to it," he said. He blamed the increase on a shift from attacks by lone hackers to those launched by organized crime and state-sponsored organizations, noting that the ability to stage attacks offshore made this both easier and less risky.

Bennett noted the increasing sophistication of hacker attacks and said that the market for personally identifiable information is "thriving, profit-driven and very entrepreneurial."

## **"Congress Raises Call for Data Safeguards"**

**Wall Street Journal (03/31/08) P. A4 ; Schatz, Amy**

In the aftermath of the breach of the passport files of Sens. Hillary Clinton, John McCain, and Barack Obama at the State Department, some in Congress are once again calling for legislation that would require companies and federal agencies to better protect Americans' personal data. The legislation, which would also require companies and federal agencies to notify consumers when their personal information has been improperly accessed, has been stalled in the Senate since last May. But on March 25, Sens. Patrick Leahy (D-Vt.) and Arlen Specter (R-Pa.) asked Senate leaders to give them floor time for the bill. In addition to the security breach at the State Department, the senators' effort to push their bill forward also comes in response to statistics that show other federal agencies are having data-security problems as well. According to a Department of Homeland Security report, there were nearly 13,000 data-security incidents in fiscal year 2007--a figure that was more than double what it was in fiscal year 2006. The report noted that roughly one-fourth of those incidents involved "improper usage" of government data by federal employees or contractors. It remains unclear why the figure increased. Other investigations into data security in the federal government have not been favorable either. In March, the Government

Accountability Office also had little positive news about the state of information security in the federal government in the latest of a series of reports it has issued since 1994.

## Online crooks target government Web sites for phishy tax refunds

**Phishing attacks targeted at government Web sites seek to steal money through fraudulent tax refunds.**

3/28/2008 5:00:00 AM  
by Joaquim P. Menezes

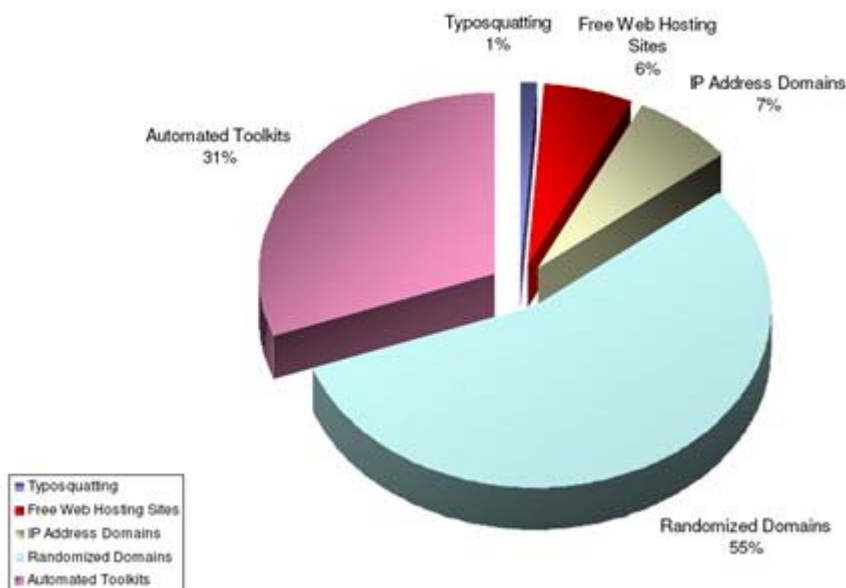
Stealing money through fraudulent tax refunds was the main purpose of phishing activity targeting government Web sites during the month of February.

This was a finding of "The State of Phishing" monthly report compiled by the anti-fraud team at [Symantec Security Response](#).

A computer security research group at Cupertino, Calif.-based Symantec Corp., Symantec Security Response analyzes viruses, blended threats, and other security vulnerabilities.

Most phishing attacks in February – 84 per cent of observed fraud activity – targeted the financial sector (specifically, e-commerce and banking sites), the report said.

### February's Phish Pie



The next target was the information services sector at 13 per cent.

However, there was a vital difference in the objective of assaults on each of these sectors.

"Most [phishing attacks](#) on the information services sector did not involve stealing user credentials for the purpose of [stealing] money, but probably for carrying out spam activity."

Around one per cent of the attacks were directed at a bunch of other sectors – such as retail, communications, retail trade, ISP, aviation and entertainment, the Symantec report said..

A piece of good news, though, is the slight drop noted in the number of unique phishing sites – 17,471 such sites were identified, 1.8 per cent lower than the previous month. These sites targeted a total of 227 known brands.

There was a 12.5 per cent month-over-month decrease in the number of attacks phishing URLs generated using toolkits. During the month of February such [phishing toolkits](#) generated around 7,847 phishing URLs.

These automated toolkits simplify the creation of phishing Web sites, allowing people without any technical knowledge to launch phishing attacks.

The use of free Web-hosting services to create fraudulent Web sites continues to be a common phishing strategy.

More than 108 Web hosting services were used to host phish pages targeting more than 147 brands in the reporting period.

According to the report, 293 domains – spoofing 51 brands – were used to mount [typo-squatting attacks](#). Typo-squatting refers to the practice of registering domain names that are typo variations of financial institution or other popular Web sites.

Phishers continue to use IP addresses as part of the host name instead of a domain name.

The report said 1,803 attacks used IP addresses instead of domain names in the URL field.

This tactic is used to hide the fake domain name, which would otherwise be easily detected. The fact that many banks use IP addresses in their Web site URLs makes it difficult for customers to distinguish a legit from a fake IP address.

Phishing sites used to launch these attacks were hosted in 62 countries – and among the non-English phishing sites Italian language phish sites were most frequently identified followed by sites in French and German.

Top level domains used with the greatest frequency were .com, net and .org.

However, among the country code top level domains those with Russian, French and German extensions headed the list.

The number of randomized domain names used in phish sites decreased by 1.8 per cent compared to the previous month.

## **'Millennials' buck IT security policies**

Age matters when it comes to information technology security. A new survey from Symantec shows what many CIOs are no doubt discovering: Young men and women entering the workforce -- dubbed "millennials"-- are not only less inclined than older employees to draw a line between corporate and personal use of technology, but they will also buck corporate security policies to access information.

The survey shows that millennials -- defined as employees 28 years or younger -- access Web 2.0 applications much more frequently than their older counterparts. According to the survey, for example, 75% of millennials access Web-based personal email at work, compared with 54% of other workers; 66% regularly access Facebook or MySpace, compared with 13% of other workers; and 51 % of millennials access personal finance applications, compared with 27% of other workers.

That's just the tip of the culture shift.

When asked whether they feel entitled to use whatever application or device or technology they would like, regardless of source or corporate IT policies, 69% of millennials said yes, compared with 31% of other workers. Indeed, 75% of millennials have downloaded software on their work computer for personal use, vs. 25% of other workers -- even though 85% of the organisations surveyed indicate their policies restrict that practice. Millennials also regularly store their corporate data on personal devices: 39% on personal computers, 38% on personal USB devices, 20% on personal hard drives and 16% on personal smartphones.

The survey, conducted in March, is based on phone interviews with 600 employees, 20% of them millennials, 20% "others" and 20% identified as "IT decision makers."

### **What's security got to do with it?**

The proliferation of technology devices and applications, combined with a generation's indiscriminate use of those IT assets, obviously exposes businesses to huge risks -- in data loss, compliance issues, legal implications and so on.

How should the IT establishment respond? Not by yelling and telling, said Samir Kapuria, managing director, Symantec Advisory Consulting Services.

"This is a large volume of people who use these personal technologies," Kapuria said. "Businesses need to ask themselves, 'How do I harness the capabilities of this tech-savvy group while also making sure of eliminating the risks associated with the use of this technology?'"

Kapuria, who has [blogged](#) about the survey, said the first step is to define the risk: how many people use social networks on a regular basis, how many access Web-based email, what applications are being download to your corporate assets, and so on. An information lifecycle strategy designed for data that lives in a corporate environment isn't very effective for data that is sitting on a USB drive, smartphone, home PC or external hard drive.

This is not an easy task. The blurring of the line between personal and corporate control of technology makes it hard to know where "the endpoints" are. "In some areas, the CIOs have no hands and eyes to manage the endpoint, so they need to really rely on their people to manage that risk on their behalf," Kapuria said.

But that brings up another worrisome finding from the survey: a majority of IT managers said they are doing an adequate job of educating the workforce about their companies' policies around technology usage. But only 57% of both groups believe they have been trained. (Eleven percent of millennials said they have been trained, but do not follow policies.)

Kapuria said there needs to be a council of people who understand the mind-set of the millennials and can measure the business's risk level through this lens, then identify the hard and soft skills required to remediate the risk. He suggested the council include the chief risk officer, if there is one, the CTO, CSO, general counsel and operations and human resources staff members.

His other piece of advice: Millennials don't like to be told what to do. They respond better to the boss who "coaches" than they do to the boss who bosses. Training and educational programs should show how the risk of ignoring company policies on technology usage is "everyone's risk, thereby making everyone feel they are part of the solution," Kapuria said.

### **Millennials under the microscope**

The survey from Symantec is hardly the first to look at the work habits of the millennials. Psychoanalysing the quirks and capabilities of these tech-savvy young workers, as well as their capacity for disrupting the workplace, has become something of a cottage industry of late.

Quick learners, adaptive, creative and tribal, millennials are not looking to employers for help, per se, according to Melanie Holmes, an executive at staffing firm Manpower -- just give them the tools to accelerate and they will manage their own careers. This young cohort feels no special loyalty to employers, being more likely to work at a place for a few years and leave. Some millennials will have four or five careers over their working lifetimes.

Jack Harrington, principal of Atlantic Associates, a staffing firm specialising in IT, said millennials are hard-working "but have different demands from other generations." They want flexible work schedules and flexible roles at their organisations, Harrington said. They are not only quick to adopt cutting-edge technology, but they are also turned off by companies that don't offer the latest technology.

And by the way, CIOs aren't the only executives wondering how to manage this collective sense of entitlement. In a recent Atlantic Associates survey of executives, more than half of the respondents said that managing young workers was a top challenge.

## Loss of personal data on rise

### 'BREACHES' UP 40 PERCENT IN '07, ALTHOUGH FRAUD LOSSES DROP

By Mark Boslet

Mercury News

Article Launched: 03/25/2008 01:35:38 AM PDT

Despite the public outcry over identity theft, the loss of personal information still appears to be on the rise.

Experts say the number of reported "breaches," where sensitive personal data such as credit card numbers or financial information is lost or stolen, increased more than 40 percent last year.

"We think people are going to learn from their mistakes, but they aren't," said Mary Monahan, senior analyst at Javelin Strategy & Research, a Pleasanton research firm.

According to Monahan, 446 breaches were reported in the United States last year, exposing a total of 128 million records. In 2006, 312 breaches occurred, compromising 20 million records.

Last week, Agilent Technologies of Santa Clara added itself to the list of corporate victims. The maker of test and measurement equipment acknowledged that a laptop containing personal data on 51,000 current and former employees was stolen from a car of a vendor on March 1. The vendor, Stock & Options Solutions of San Jose, said it has since enhanced security measures.

"While we have no reason to believe that any of the information has been misused, we recognize that our clients entrust us with their data and have taken additional steps to ensure this sensitive information is as secure as possible," Sean Lembree, chief executive of Stock & Options Solutions, said in a statement.

Despite the growing identity theft problem, experts see reason for optimism.

Fraud from the misuse of the information appears to be on the decline. In 2006, there were 8.4 million victims in the United States with losses of \$51 billion, Monahan said. That fell to 8.1 million victims in 2007 with losses of \$45 billion.

Corporations are making better use of technology to monitor their systems for possible fraud, she said.

Still, many companies haven't yet put into place adequate policies to prevent the theft or loss in the first place. In some cases, they haven't adopted technology that encrypts data on a laptop and makes it difficult for thieves to read.

Also, companies have not done a good job of educating their employees about privacy issues, said Paul Stephens, director of policy and advocacy at the Privacy Rights Clearinghouse, an advocate of consumer privacy rights. "You should not leave the building before the data is encrypted," he said.

On security issues, smaller companies often lag behind larger ones, said Michael Weathers, senior vice president of governance and security at Fidelity National Information Services of Jacksonville, Fla., a data processing firm. Large businesses have invested significantly in their security systems, he said.

At Agilent, spokeswoman Amy Flores said no fraud has yet been linked to the missing employee data, which includes names, Social Security numbers and financial information. The company sent a letter to notify affected staffers, and the theft of the laptop is under police investigation.

## "Panel: Users Still Worst Enemy to Endpoint Security"

eWeek (03/28/08) ; Dern, Daniel P.

No matter how much training employees receive, security will still be compromised as long as end users seek shortcuts that allow them to finish their work faster, agreed a panel of corporate security experts at the recent Boston SecureWorld Expo. "Unless you have an almost inoperable lockdown on a tool, if a user sees a shortcut that's easier to get work done with then how effective can end-user awareness be?" asked EMC's Dave Martin. "They can still do things they know are against policy, because they know it saves time." PDAs and cell phones now give users more points-of-access than ever before, and experts say Google's new Android phone, set for release this fall, will unleash a new wave of risk factors with its many

applications. The experts believe security training and technology must go hand-in-hand; fundamentally, however, applications such as email should be automatically secure. "You have to make doing the right thing easier than doing the wrong thing," says panelist Jody Saarmaa, a Liquid Machines executive.

## "In-Stat Reports Shortfall in VoIP Security Implementations"

TMCnet.com (03/25/08) ; Campbell, Susan J.

With the use of Voice over Internet Protocol (VoIP) becoming more widespread, it makes sense that businesses would be paying more attention to security, but research shows this is not the case. In-Stat recently performed a survey of U.S. businesses and found that security mechanisms for VoIP were no more than 50 percent effective. "Proactive measures, including periodic security audits and pre-deployment assessments had low percentages of penetration too, even among larger organizations," says In-Stat analyst Victoria Fodale. More than 80 percent of respondents use a VoIP platform in some capacity, and In-Stat predicts the total number of IP BX lines in use will reach 168 million by 2010. In order for VoIP to gain widespread credibility, security experts must seek out more efficient solutions to security, integration, and end-user transparency, In-Stat says.

## *Keeping Your Thumb on Thumb Drives*

**Those little USB drives certainly are handy, but how do you keep your company's sensitive data from walking away? Here are a few ideas**

MARCH 28, 2008 | 5:30 PM

**By John Sawyer, CISSP**  
**A Special Analysis for *Dark Reading***

Every time it begins to seem safe to read the news again, there's a new security breach report: Another company is reporting the potential exposure of customers' personal data as a result of the loss or theft of a laptop, backup tape, or external drive. You'd think all these reports would teach companies a lesson, but it's apparent that most companies must learn that lesson firsthand -- by experiencing it themselves.

While laptop thefts are reported nearly every day, it's unusual to hear about the loss of portable USB storage devices (thumb drives). Is that because enterprises have learned to secure them properly? Or is it because thumb drives are nearly impossible to track, and most companies have no idea when they have been lost or stolen?

There's no easy way to answer that question, but it is worth noting that there are technologies, both hardware and software, which are helping enterprises to secure data stored on thumb drives. These technologies differ in effectiveness and transparency to the user, but in the end, securing data at rest on thumb drives isn't rocket science -- and it can be done on an enterprise level or in an ad hoc fashion.

Thumb drive manufacturers have been including "security" software on their products for a couple of years, but the functionality has been limited, and typically only provides basic encryption of files stored on the device. Last year, we saw more sophisticated thumb drives that perform file encryption at the hardware level -- such as the eye-catching IronKey -- but the cross-platform functionality and read/write speeds vary greatly, as we saw in the recent reviews from [Information Week](#). Only a few thumb drives offer enterprise-level management features.

Some organizations are attempting to secure their data by completely disallowing all thumb drives, but that isn't a decision that many organizations are ready to make -- there are many legitimate uses for these little babies. The real question is how to secure the data that the users place on the drives -- not how to prevent data from being written to the drive.

One solution is to take a hybrid approach, using a software product that only allows usage of thumb drives with pre-defined serial numbers in conjunction with an IronKey to handle the encryption. Some antivirus suites, like Symantec's Endpoint Protection (SEP) 11, already offer this type of capability. Pair that control with company-issued IronKeys (or a similar product), and you can almost eliminate the panic that's caused by the accidental exposure of these devices (provided the user didn't write the password on the device).

One disadvantage of the IronKey products: They aren't cheap. If your users are prone to losing thumb drives, a smarter

investment might be to purchase cheaper thumb drives and rely on a software-only solution to handle the security. [Lumension Security Sanctuary Device Control](#) and [Credant Mobile Guardian for External Media](#) are two solutions that can transparently encrypt data that is copied to thumb drives -- without any special hardware or interaction from the user.

If you're on a very tight budget -- and if you have a high level of trust in your users and don't need an enterprise solution -- cheap thumb drives and the open-source TrueCrypt technology could be the way to go. Once you've trained your users and done the initial setup, the data stored in encrypted TrueCrypt volumes on the thumbdrives would be secure -- and you've got a solution that works equally well for Windows, Linux, and Mac OS X.

Each of these approaches has its own pros and cons, depending on the level of user interaction you need, the hardware and software costs you can afford, and the centralized management capabilities you require. As with most security solutions, when it comes to protecting sensitive information from accidental disclosure, there definitely is no "one size fits all."

If you aren't doing any of these approaches, though, take a closer look at all of them and make a move soon. It's a lot cheaper to implement portable drive security than it is to notify thousands of customers that their data has been breached.

## Number of viruses to top 1 million by 2009

Dr. Evil-like number not, however, cause for utter panic

By Darren Pauli

- 
- April 4, 2008 The total number of viruses will reach 1 million by year's end, according to security experts. Malware writers have been forced to create new types of viruses and exploits more regularly as businesses and individuals improve security practices, the experts said.  
  
Sophos PLC Chief Technology Officer Paul Ducklin said about 25% of unique malware has been created in the past six months of its 20-year history.  
  
"About 85% to 90% of malware families have a fix created for them almost immediately," Ducklin said.  
  
"Malware writers aren't getting the same bang for [their] buck as they used to because businesses and consumers have become much more diligent with security over the last five years," he noted.  
  
"The number of infectious e-mail attachments getting through are down from about 1 in 40 [about five years ago] to 1 in 1,000," said Ducklin.  
  
He said the decline in infections is the result of better gateway filters, more relevant corporate policies and user education, and dilution from a rise in legitimate e-mail traffic.  
  
While the security industry is on top of conventional spam and phishing attacks, more effort needs to be put into preventing and eliminating so-called drive-by downloads, according to Ducklin.  
  
The attacks allow hackers to redirect mass amounts of traffic by inserting malicious iFrames into legitimate Web sites. The hacks are usually invisible to Web site visitors and often do not draw attention from security personnel because they only require a single line of code to be manipulated.  
  
He said it is essential that exploits be patched because hackers search for compromised sites for follow-up attacks.  
  
Jari Heinonen, Asia-Pacific vice president at [F-Secure Corp.](#), said his company logs about 25,000 malware samples each day, the highest on record.  
  
"The total number of viruses and Trojan [horses] will pass the 1 million mark by the end of 2008 if this trend continues," Heinonen said. "While there are more viruses than ever before, people report seeing less of them [because] malware authors are changing their tactics.  
  
"Drive-by downloads are the preferred way of spreading malware [because] they happen automatically by visiting a Web site, unless users have a fully patched operating system, browser and plug-ins," Heinonen said.

Heinonen said malware will increasingly target the kernel sector through rootkits such as Mebroot, which attacks the bootstrap sector.

A resurgent Mebroot was detected last month, some 15 years after the DOS-based malware was created.

## Security Manager's Journal: Confronting the application layer

A security manager can't simply ignore the things she doesn't understand. So it's time to secure Web-enabled apps.

By C.J. Kelly

April 7, 2008 (Computerworld) An independent consultant is evaluating our security posture, and he'll be here for the next several weeks. It's the sort of thing that makes me as nervous as a mother whose child is applying to colleges. I used to be a security consultant myself, so I understand what the consultant is looking for. I have prepared. But it's always nerve-wracking to see your "children" judged by outsiders.

I'm glad we're following this security best practice, though I don't really expect any surprises. In fact, upon receiving the first of what will be many reports from the consultant, I broke into laughter, for there in writing was what we have long known to be our weakest link: the application layer.

I don't make any claims of being an expert in application-layer security. I don't have an application development background, and I find myself avoiding the topic. It's probably not the best position, but I don't know what to do about it.

### TROUBLE TICKET

**AT ISSUE:** A security consultant quickly turns up problems with the application layer.

**ACTION PLAN:** Buckle down and finally learn about an aspect of security that's been ignored.

I am fairly expert at network security, Windows and Unix operating system security, physical security, wireless security, building security and access controls. But a security manager can't secure just the things she understands. All those other things could be tight as a drum, but it's all for naught if hackers can get in through the application layer.

And that's the problem with the application layer: Hackers can get in if it's not secured, because most applications have been Web-enabled.

Right now, we're protecting our applications by placing the Web servers in the DMZ, keeping the application and database servers behind the firewall, running "pinhole" connections between them, maintaining rules on whether a server can pull or push information, and mandating access control based on roles. The servers are patched on a regular basis (weekly, lately), and we scan for vulnerabilities. But that's about it. I'm trying to figure out how to ensure that the applications that are built in-house are properly secured.

I'm not sure where to start. I could never do a source-code audit. I wouldn't even know what I was looking for.

### Seeking Answers

To gain some insight, I turned to the Nessus open-source tool and decided to run it against a production server that is accessible only by the security staff — or should be. We run several security applications on it. If I happened to knock down the server with my probing, I had access to bring it back online.

Nessus provided information on 30 open ports and offered 73 notes on those ports, eight warnings and zero holes. There are a few things we can do to better secure the server at the operating-system level, but I didn't learn much more than I already

knew about how this server was configured. And, of course, it's behind a firewall. Not a particularly helpful exercise in understanding application-layer security. Any host in the DMZ would certainly not be listening on that many ports.

All the application-layer vulnerabilities spotlighted in the security consultant's report can be resolved by application patching. But I'm digging deeper, as I tend to do, because of the highly sensitive nature of the health information that's on our network.

And I do know that there are many ways of protecting applications. We can allow only certain types of communication between hosts, and we can encrypt data. But I have to wonder what else we can do. I'm sure that vendors will read that as an invitation to tell me all about their "application-layer security solutions." I hope they don't bother unless they can bring a fresh perspective to this topic. And they had better remember that we have no budget.

## Feds face challenge of balancing data access and security

Government agencies wrestle with security issues as they work to share info more broadly

By Patrick Thibodeau

April 7, 2008 (Computerworld) The U.S. government's reputation for protecting data has been hurt by a parade of bad headlines about spies, [stolen laptops](#) and, most recently, some [Department of State](#) contract workers [snooping into](#) passport files.

But the inability of intelligence agencies to share data that might have helped them detect the events that led up to the 9/11 terrorist attacks may have been the government's biggest information failure ever. And balancing data accessibility and security has become a big challenge for federal agencies in the post-9/11 era.

Charles Allen, assistant secretary of the Office of Intelligence and Analysis within the [Department of Homeland Security](#), said last September that making vital information more readily available to authorized users is "at the heart of efforts to prevent another 9/11," according to the transcript of a meeting held that month by a data privacy and integrity advisory committee at the DHS.

But improving data-sharing remains a work in progress at many agencies. For instance, the Department of Defense wants to create an enterprisewide view of data with the flexibility to put information into the hands of an "unanticipated user," said Lloyd Thrower, director of strategic planning and transformation in the DOD CIO's office.

By "unanticipated user," he means a person or department not originally expected to need a certain piece of data — an Army unit that wants to use a satellite photo taken by the Air Force, for example. To make information available broadly but securely, the [DOD](#) needs to ensure that data is tagged appropriately and that user authorization criteria are attached to it, Thrower said. Credentials encoded in ID cards then can determine whether users are allowed to access information.

But the unauthorized access into the passport records of presidential candidates [Hillary Clinton](#), [John McCain](#) and Barack Obama illustrates what can go wrong. The State Department uses a monitoring system that alerts administrators whenever flagged passport files are accessed, but that sort of after-the-fact security system won't work with highly sensitive defense and intelligence data that could be a matter of life or death.

Making data broadly visible "doesn't mean that everybody is going to get a hold of it," Thrower said. "It just means that anybody can determine that there is this type of information in existence." He added that individual units within the DOD will still be able to "maintain exactly the same control" in determining what level of access is proper for their data as they have all along.

Nonetheless, like private-sector businesses trying to [guard their systems](#) against possible rogue insiders, the DOD and other federal agencies face a major cultural issue: can users be trusted to do the right thing?

Lucian Russell, a consultant at Expert Reasoning & Decisions LLC, said that agencies are typically inclined to limit data access in order to "reduce the risk to zero. It's sort of like the mentality of the Cold War."

But even that may not be fail-safe. The passport-files breach was a case of [misplaced trust](#) in workers, not a technology failure. And take the case of that Air Force satellite photo. "How do I make sure that a person requesting it isn't being held by gunpoint out in the field?" Russell said. "These are the kinds of questions that come up."

Matt Newman, who teaches enterprise architecture and other IT-related classes at the National Defense University, said that opening up data and making it more transparent is a huge change for government agencies, because access to information traditionally has been equated with power. But the opposite is true for the government as a whole, Newman added. "If you share the information, you can be more powerful," he said.

## Malware count blows past 1M mark

Nearly two-thirds of all threats were detected in 2007, says Symantec

By Gregg Keizer

---

April 8, 2008 (Computerworld) [Symantec Corp.](#)'s malware tally topped 1 million for the first time in the second half of 2007 as the number of new malicious code threats skyrocketed, the company said in its semiannual report on the state of security.

Of the 1.1 million code threats that Symantec has detected since it began writing signatures more than a quarter-century ago, 711,912 were discovered in 2007; 499,811 were picked up in the last six months of the year alone.

In other words, nearly two-thirds of all the threats that Symantec has ever uncovered were found last year.

Symantec credited the explosion in threats to a shift to specialization by malware makers and the existence of well-oiled -- and well-financed -- organizations that hire those programmers to write exploits and craft attacks.

"This [six-month] reporting period has seen the strongest evidence yet of this," said Ben Greenbaum, a senior research manager with Symantec's security response team. He ticked off a slew of traits now common in the malware industry, from the development of what he called "crime management kits" to proof that hackers work in a market-driven economy where threats are the coin of the realm.

"Some organizations only handle one part of the phishing process," Greenbaum said, giving an example of the specialization that's taken place. "For other parts, [those hackers] can outsource the work."

The specialization and organization, Symantec argued in its Internet Security Threat Report, mean that crimeware benefits from economies-of-scale, just like many other businesses.

"A group of specialized programmers can create a larger number of new threats than can a single malicious code author, bringing about economies of scale and therefore an increased return on investment," the report said. "Many of these threats can be used for financial gain [and] these proceeds can then be used to pay the programmers to continue creating new threats.

"The combination of these factors results in a high volume of new malicious code samples that threaten users online."

Greenbaum called 2007's tsunami of threats a "tipping point," and said that it is clear that security vendors -- and their users -- will soon need to switch to "whitelisting" legitimate code rather than "blacklisting" threats, as is now the practice.

A whitelist-based approach to security could take many forms, Greenbaum said. He declined to get specific about what Symantec's considering, saying only that the company is looking at some "interesting" ideas. But it would clearly have some pay-offs.

"It would reduce the size of the definition set," he said, "and make security software more efficient at catching malicious code."

By Symantec's estimate, 65% of the 54,000-plus unique applications deployed on Windows-based PCs in the last six months were malicious. "[Whitelisting] is a better approach," said Greenbaum, "considering the modern threat landscape."

Just last week, security experts [predicted](#) that the one-million mark would be reached by the end of 2008.

The [Internet Security Threat Report Volume XIII](#) can be downloaded from Symantec's site.

## IT 'Big Brothers' trying to keep internal users under control

Activity-monitoring tools may be able to help stop rogue insiders from compromising data. But they aren't being widely adopted yet.

**By Jaikumar Vijayan**

April 7, 2008 (Computerworld) When it comes to protecting his company's data, Tom Scocca doesn't mind that he might be seen as something of a Big Brother by internal end users.

Scocca, who is a global security consultant at a large company that supplies products to the semiconductor industry, thinks that threats from within businesses require as much attention from security managers as external threats do.

So in addition to the usual network perimeter defenses, Scocca has put monitoring tools on end-user PCs and internal networks to help guard against inadvertent or malicious data breaches.

"There is a bit of a Big Brother syndrome attached to it," he acknowledged. But IT managers need to get over their trepidation about being called snoops, added Scocca, who asked that his employer not be named.

"These tools are not there to spy on people," he said. Rather, they're designed to "make sure the things that keep the revenues rolling in aren't compromised."

The issue of rogue insiders surfaced in a high-profile way last month, when the U.S. Department of State [disclosed](#) that three contract workers with access to its systems had improperly viewed the passport records of presidential candidates [Hillary Clinton](#), [John McCain](#) and [Barack Obama](#). The activities of the contractors were detected by a security-monitoring system designed to alert administrators whenever flagged passport files are accessed.

But technologies that can keep a close eye on the activities of internal users have yet to be widely adopted. For example, [Gartner Inc.](#) analyst [John Pescatore](#) estimates that less than 30% of Fortune 5,000 companies have installed such tools.

The lack of active monitoring of end users is a big reason why some insiders have been able to pull off spectacular data heists without getting caught -- at least not right away.

A prime example is the case of [Gary Min](#), a former research scientist at DuPont who in 2005 downloaded about 22,000 document abstracts containing confidential information about most of the company's major products. Min was caught only after he gave his notice; at that point, an internal investigation showed that he had accessed about 15 times more data than the next-highest user of DuPont's electronic document library.

In another prominent insider case, Certegy Check Services Inc. [disclosed last summer](#) that a database administrator had sold the personal and financial information of 8.5 million consumers to data brokers over a five-year period. The check-processing firm didn't nab the DBA until a retailer reported a link between check transactions and marketing solicitations that some of its customers had received.

### More On This Topic

Read about the effort by federal agencies to share critical data more widely while still keeping it secure: [Feds face challenge of balancing data access and security](#)

To try to avoid becoming the next DuPont or Certegy, Scocca's company is using a pair of tools from Raytheon Oakley Systems Inc. One is a desktop agent called SureView that monitors all activity on an end user's system to make sure that no data or computer usage policies are violated. If a violation does occur, the agent issues an alert to the company's security team and begins collecting data for further review.

The tool features a video-like playback feature that lets security administrators view precisely what a user was doing before, during and after a policy violation was flagged, Scocca said. That can help the admins determine almost instantly whether the violation was an accident or the result of deliberate action, he added.

Complementing the desktop agent is a monitoring tool called CoreView that keeps an eye on all internal network traffic for sensitive or inappropriate material.

Other vendors that sell products designed to help companies stop insider threats include Symantec Corp., Vericept Corp., Websense Inc., Tizor Systems Inc., Fidelis Security Systems Inc., Tripwire Inc. and Reconnex Inc. Other vendors, such as Guardium Inc. and Imperva Inc., offer tools that monitor database activity and check for improper access and other abuses.

Tampa International Airport is using system-log monitoring and analysis software from LogRhythm Inc. as part of its effort to comply with Florida's data retention laws and the Payment Card Industry Data Security Standard. And because the software can quickly correlate log events from practically every IT system, it also serves as both a real-time alerting system and an after-the-fact forensic tool, said Katherine Mullin, the airport's IT systems security manager.

Pasadena Federal Credit Union has set up a log management product from TriGeo Network Security Inc. to take actions such as quarantining a computer when it detects a policy violation. Mike McDannel, the Pasadena, Calif.-based credit union's IT security manager, said his team is also using a companion tool that can send alerts when users insert unapproved USB devices into their computers.

Gartner's Pescatore said he expects the adoption of user-monitoring tools to pick up, largely because of regulatory compliance needs. But such technologies have their limits. For one thing, tools that are designed to restrict user actions, such as downloading data onto USB drives, may require far too many built-in rules in order to distinguish between legitimate and illegitimate activities. "It's hard to describe *authorized* to a computer," Pescatore said.

And if tools are set up to generate real-time alerts about data leaks, there's a danger of being overwhelmed by false positives if the rules aren't set properly. That's particularly true, Pescatore said, when monitoring software is used to track data that may not be well defined, such as intellectual property.

Prat Moghe, chief technology officer at Tizor, which sells data-auditing software, acknowledged that many of the tools available for protecting data from inside threats remain unfamiliar to most IT managers. "These are still early days for this industry," Moghe said. "There's a lot of confusion."

## [Online crooks face tough competition](#)

By JORDAN ROBERTSON, AP Technology Writer Tue Apr 8, 12:58 AM ET

Fierce competition among identity thieves has driven the prices for stolen data down to bargain-basement levels, which has forced crooks to adopt mainstream business tactics to lure customers, according to a new report on Internet security threats.

Credit card numbers were selling for as little as 40 cents each and access to a bank account was going for \$10 in the second half of 2007, according to the latest twice-yearly Internet Security Threat Report from Symantec Corp. released Tuesday.

Symantec detected 711,912 new threats last year, 468 percent more than in 2006, when it found 125,243 and almost two-thirds of all 1,122,311 Symantec has cataloged since 2002.

The data is usually sold through instant-message groups or Web forums that exist for only a few days or even hours, according to Symantec, and the hacking community exacts harsh consequences when members try to pass along fraudulent information.

"If the seller says there's \$10,000 in a bank account, and there isn't \$10,000 in there, their ability to sell will drop through the floor," said Alfred Huger, vice president of Symantec Security Response. "It's a sort of honor among thieves, and it's very strictly enforced."

Researchers said they found more evidence during the last six months of the year that Internet fraudsters are adopting mainstream tactics, including hiring teams of hackers to create new viruses and offering volume discounts on stolen data to encourage larger orders.

In some cases, stolen credit card numbers were sold in batches of 500 for a total of \$200. That's 40 cents each, less than half the price observed during the first half of 2007, when they were down to \$1 apiece in batches of 100, according to the report.

Full identities including a functioning credit card number, Social Security number or equivalent and a person's name, address and date of birth are going for as little as \$100 for 50, or \$2 apiece.

Certain identities are more alluring than others, according the report. Stolen identities of citizens of the European Union sell on the high end for \$30 an average of 50 percent more than U.S. identities.

Researchers said the higher prices reflect the fact that the identities can be used in multiple countries, instead of just one. They added, however, that scarcity of a certain type of identity will drive up its price.

Also popular with attackers are Web site-specific vulnerabilities because few are fixed quickly. Of 11,253 so-called "cross-site scripting" vulnerabilities found on specific sites during the second half of 2007, only 473 were patched.

Cross-site scripting vulnerabilities are flaws in the coding of Web applications that allow hackers to insert malicious code into the pages and then deploy it to unsuspecting visitors.

The report was released as thousands of security professionals gathered in San Francisco for the RSA Conference, a weeklong event at which Symantec's CEO John Thompson Tuesday keynote is among several high-profile speeches.

The survey is based on malicious code gathered from more than 120 million computers running Symantec antivirus software and some 2 million decoy e-mail accounts that collect spam.

## **Regulations not making data safer, says RSA chief**

And by the way, security's dying as an independent industry

**By Jaikumar Vijayan**

April 8, 2008 (Computerworld) An increasingly complex and cumbersome regulatory environment may be forcing many companies to focus their information security efforts purely on meeting compliance and audit goals rather than on understanding and addressing business requirements, warned Art Coviello, president of [EMC Corp.](#)'s RSA security group.

Delivering the inaugural keynote at the annual [RSA Conference](#) in San Francisco this week, Coviello called on regulators and policymakers to create regulations that focus on outcomes, rather than laying out a prescriptive list of controls.

Regulators need to make sure that any regulations they mandate do not end up "actually weakening a business by enforcement actions that drive companies to spend unnecessarily on perceived but not genuine security risks," Coviello said. Such "make-work projects" add little material value to a company's overall [security stance](#). "Instead of passing regulation that creates a climate of 'what's the least I can do to get a check mark,' drive regulation that focuses on outcomes," Coviello said.

An example of a properly functioning regulation is California's SB 1386 bill, which focuses on requiring companies to notify consumers of data breaches involving their private data rather than on telling them how to protect that data, Coviello said.

One step that regulators can take to reduce the current complexity is to create a national baseline standard for protecting sensitive data — passing one federal data breach notification law that preempts the 40 separate state laws with which

companies have to currently contend, he said. More effort also needs to be put on punishing cybercriminals, Coviello added, urging Congress to ratify a national cybercrime bill already [passed](#) by the [U.S. Senate](#) in late 2007.

At the same time, security practitioners themselves need to start thinking more about information-centric security strategies, as opposed to mere information security strategies, he said.

"We must look beyond tools that blindly lock down data [and] toward mechanisms that can *understand* information and safeguard it intelligently throughout its life cycle," Coviello said.

Instead of implementing products for dealing with specific security threats, the goal really should be on making security an indistinguishable part of the infrastructure, he said, Processes for monitoring and enforcing security need to be automated as far as possible, and companies need to get away from static controls that are focused simply on controlling access to data, he said.

"Many security products force people to think the way the tool wants, resulting in a sea of complex, static and inflexible mechanisms," Coviello said. Effort should instead be directed toward implementing tools that are capable of making dynamic decisions based on an understanding of how the network, users and content normally behave, he said.

The vendors that will enable these sorts of capabilities are not going to be today's vendors of stand-alone security products, Coviello predicted. Rather, the technologies will be developed and integrated by large IT infrastructure vendors. Independent vendors will continue to provide components of this infrastructure, Coviello said, but he predicted that there will eventually be no need for an independent security industry.

## Assessing the risks and cost of encryption

What does that frozen-chip hardware hack *really* mean to you?

**By Charlie Martin**

April 9, 2008 (CIO) With major data breaches occurring on a regular basis, encryption vendors are going into hyperdrive, touting the need for their products. However, encryption is only one aspect of protecting your sensitive data, and a new attack shows that it may not be enough.

Recently, the [security research group](#) at [Princeton University](#) [published a report](#) on its success at recovering data from an encrypted disk image on a laptop. This caused a good bit of consternation and some breathless coverage in the press (as with this [New York Times](#) story that got the headline "[Researchers Find Way to Steal Encrypted Data](#)"), leading to some speculation that this meant on-disk encryption was simply not worth the effort. (Read more on [Laptop Encryption Strategies](#).)

The next morning, having read the *New York Times*, your CEO stops you in the coffee room and asks, "Is it worth using this disk encryption? It's a pain, and from this article it sounds like someone could get my data anyway."

The security community gets excited about any cool hack that can be exploited to get something you're not supposed to get, and we know that sometimes it's really an important issue. On the other hand, sometimes it isn't. How is a nonspecialist to know the difference, and how can a CIO answer the CEO's questions in the coffee room the morning after a story like this appears?

It turns out that we can answer this sort of question quickly with some good expectation of accuracy, using ideas from that half-remembered Finance 101 class we took years ago. What we're concerned with is the *risk* posed by this new attack, risk as defined in finance as the probability of the undesired event multiplied by the cost of the undesired event (which is called the *hazard*). We can manage security issues, first of all, by considering the risk.

### **Risk = probability x hazard**

An easy way to see how this is applied is to think about the PIN on your ATM card. Most banks have simple policies for ATM cards: You have a four-digit PIN; there is a limit on how much cash can be taken out of the account every day, say \$500; and there is a policy that says after three wrong PIN attempts, the ATM annoyingly eats your card, usually on Friday afternoon just before you leave for that weekend in Vegas.

Now, assume the card is lost, and someone is attempting to get money from it illicitly. The chances of guessing the PIN correctly with no extra information (you *didn't* write the PIN on the back of the card, right?) are 1 in 10,000 for one try, or about 1 in 3,333 for the three tries you get. The hazard is \$500, so the risk is about 15 cents. In other words, the bank can be pretty confident that over many thousands of depositors and ATM cards, the cost of this kind of fraud per card is about 15 cents each.

Of course, with more data and a longer time to explore it, we could get a much better estimate that takes into account the people who *do* write the PIN on the back of the card, the people who manage to watch over your shoulder as you enter the PIN and so on, but remember, we're in the coffee room and the CEO doesn't want "I'll get back to you in a week or so when I've had time to research this." In any case, for many purposes this is good enough: If someone is trying to sell you a \$5 solution to a 15-cent problem, it really doesn't matter much if the accurate answer is really 16.231 cents.

### Evaluating risk

So, how can we apply this to the problem of an encrypted disk? The attack the Princeton group outlined goes something like this: You have data stored on a disk, say on a laptop, that you have protected with a commercial disk-encryption program like [Microsoft's BitLocker](#) or [Apple's FileVault](#). (Also read [How to Lock Up Laptop Security](#).) A technically sophisticated attacker wants that data and has significant resources he can apply to the problem, including tools, a bottle of "canned air" and a computer with some specialized software.

To execute the attack, the bad guy must first get the computer with the power on, or within a few minutes of the power being turned off; second, cool the memory chips in the computer to -50 C using the "canned air"; third, get the chips where they can be read by the attacker's computer; and finally apply a statistical method and some knowledge of the disk encryption to find and extract the keys. He can then read the data from the disk.

Can it be done? Sure: See the Princeton Web site for a description and even a video, but it isn't easy. Still, "It can be done, but it's hard" isn't necessarily reassuring in the coffee room on Monday morning; using a risk estimate, though, we can compare it to other possible problems.

To start with, how much is the data on the disk worth? Let's take an all-too-common example: Someone has copied the customer data for 100,000 customers to his laptop to work on over the weekend, and this data includes enough information to be of use to an identity thief. If this data were to be lost or compromised, your company would have to respond by, say, buying a year's credit monitoring service for each of the 100,000 customers, at a cost of about \$20 each. So, from the standpoint of a potential loss, the data is worth around \$2 million. (Let's stop and think about that number for a minute: two million dollars. The loss of a \$2,000 laptop is nothing.)

Assume we don't protect the data at all, and one laptop is lost every 10 years, so the probability of one loss in one particular year is about one-tenth. The risk: \$200,000. In other words, without using disk encryption or some other protection, you can expect data loss to cost about \$200,000 a year on average.

Now, let's assume you *did* use encryption. We start with the same assumptions, and guess that one time out of a hundred a laptop is lost to a skillful thief; instead of taking the laptop to a pawnshop in the seedy part of town, the thief is actually going to try to extract data from it. Let's say further that about half the time the computer is actually stolen with the power on, because for convenience it was simply put into sleep mode. So now, about one time in 200, our skillful thief gets a computer full of recoverable data. The probability of loss is now one two-hundredth of one-tenth, or about 0.0005, and the risk is now about \$100 per year. So the answer to the CEO's question is this: With disk encryption we can expect data losses to cost us around \$100 a year on average; without it, we can expect data loss to cost \$200,000 a year, again on average.

Of course, the *easiest* protection is to use a disk-encryption program and simply make sure you turn the laptop off when you're not using it; then this technique won't work at all, because there won't be any recoverable keys left in memory.

This technique of risk analysis can be applied to almost any decision about any security measure: It's worthwhile only if it costs less than the reduction in your expected loss per year. For example, there are a number of special disks available now that have specialized on-disk encryption hardware. How much of a premium is it worth to buy one of these disks, compared to using encryption software? Simply extend the reasoning: If the special hardware makes it 100 times harder to get data off the disk, the expected loss per year is around \$1. If the special hardware costs significantly more than \$199, it doesn't actually pay off.

So the next time the CEO asks you one of these questions, you can make a back-of-the-envelope estimate in just a few seconds' thought. Won't that make you look good?

## THE CYBERCRIME ECONOMY

Posted by [Thomas Claburn](#), Apr 9, 2008 08:33 PM

Dot-coms daunted by the financial downturn would be well advised to look to the cybercrime economy.

Cybercriminals "have very sound [business models](#)," said Joe St Sauver, manager of Internet2 [Security](#) Programs through the University of Oregon at an RSA Conference panel on Wednesday, "better than many corporate business plans I routinely see."

The conference session, "Deconstructing the Modern Online Criminal Ecosystem," offered interesting insight into the way the Internet's black market works.

While most of the security professionals I've spoken with at RSA expressed optimism about dealing with future cyberthreats, I find it hard to see where that optimism comes from, given the economics of cybercrime as explained by the participating panelists.

One of them was Larry. He provided no last name and asked that his picture not be published, presumably for his safety. He's the chief investigator for [Spamhaus.org](#), a site that tracks spammers. "It's almost impossible to take these [spam Web sites] down because the DNS changes every five minutes or so," he said.

"Almost impossible" is not the stuff of optimism.

As the panelists explained, a single spam message might be tied to as many as 10 separate organizations and perhaps five suppliers. Every task in the criminal economy has become a separate specialty. Some people sell e-mail lists, others sell lists of compromised IP addresses, there are sellers of credit card numbers, and those who sell access to bot nets. Then there are those who handle product fulfillment for spammers, and those who specialize in laundering money.

All this specialization insulates the network from prosecution by providing a degree of deniability. "You mean my associate was using the names I sold him for spamming?" a cornered cybercriminal might say. "I told him not to do that." The modern cybercrime economy is a franchise model that scales, explained St Sauver.

And it pays well. [IronPort's](#) Patrick Peterson observed that an IT graduate in Romania might be able to earn \$400 per month legitimately, compared with several thousand per month in the cybercrime economy. And I've spoken with security researchers who suggest the difference in pay between being a security researcher and a security exploiter differs by a factor of 10 quite often.

Cybercriminals make so much money, in fact, that they employ money mules, networks of thousands of people to help them launder money by receiving and sending cash for a commission. Many of them are unaware that they're facilitating crime. And many of them end up being scammed.

A typical scam: They're wired money and asked to send out a lesser amount via Western Union. Only later do they learn that wire transfers can be reversed, whereas Western Union money transfers are irrevocable.

And a final factoid from the session: Lawrence Baldwin, chief forensics officer with My Net Watchman, said that in the past few months he was aware of about 30 data breaches at companies and only two have been publicly reported.

The trend, Baldwin said, was to go after midsize organizations because the big ones have too much security and individuals don't have enough valuable data. Sounds like the recent Hannaford breach to me.

## 3 things your facilities group should know about your company's data security

These workers literally hold the keys to your company's physical security.

April 14, 2008 (Computerworld) Here are two facts from security experts: First, physical access always trumps technical savvy; and second, facilities and maintenance staffers make soft targets.

That's why Eric Cowperthwaite, chief information security officer at Providence Health & Services in Seattle, recommends developing specific training and awareness programs for building managers, cleaning crews and other facilities workers.

"The key is using multiple delivery tools, including electronic, in-person and paper [presentations]," he says. Providence, for example, distributes trifold brochures, and cards that workers can carry in their wallets. Every month, a half-page security bulletin goes out via e-mail that addresses a new security topic and offers three to five tips on how to recognize a threat and prevent it.

Keep these three things in mind when considering potential threats at your company.

### 1. Don't assume all is as it should be.

If a person is wearing a badge, most employees assume that he is authorized to be there. But crafting a counterfeit badge is well within the talents of your average 10-year-old with a color printer, notes Michael Theis, chief of cyber-counterintelligence at the U.S. National Reconnaissance Office.

**IT's response:** Security training "should aim to get employees invested in the idea that they need to be curious," Theis says. "If you see someone you don't recognize, ask them who they are."

[Darryl Lemecha](#), CIO at Vertafore Inc., provides the company's security guards and janitorial and building staffs with a list of names and photographs of outside service workers, such as delivery and cleaning people who are authorized to enter the building.

### 2. Beware big risks in small packages.

Incoming letters and packages can easily be tampered with en route, but they are rarely inspected closely upon arriving at a company's mail facility. This can cause big problems, especially for companies like Vertafore, which frequently receives CDs, tapes and other media containing customer data.

**IT's response:** Vertafore has developed a process of due diligence to make sure that all packages are intact before they're accepted. "We refuse packages that have been damaged in shipping, because customer data may have been lost or tampered with," says Lemecha.

### 3. Now's the time to change the access codes.

Four- and five-digit push-button locks on corridor doors, elevators and even data center doors offer another line of defense against intruders. But all too often, the access codes remain the same for years, experts say. That means anyone who has ever worked in that building can still enter areas that should be off-limits to them.

"The building I'm in has a code on the elevator, and the code hasn't changed since we moved in three years ago," says Chris Blake, workstation administrator at The Benchmark Group. "Everyone who has ever been in this building knows the code, but the building owner has been reluctant to let us change it."

**IT's response:** Have a regular schedule for changing access codes to secured areas. Also, when employees leave a company, their key cards should be deactivated and their badges confiscated and destroyed.

## 5 things your HR people should know about your company's data security

Huge stores of personnel data make this department a target for thieves.

By Mary K. Pratt

- April 14, 2008 (Computerworld) Human resources departments typically have some of the biggest collections of sensitive data in any organization. But even if companies have corporatewide security measures in place, HR staffers are particularly vulnerable to data leaks because of their departments' vast holdings. The nature of the HR job, which requires nearly constant collecting and sharing of data, presents further challenges.

### 1. Keep track of inconsistent legal requirements.

Companies often keep employee information in one global HR system because it's efficient, says Rena Mears, a partner in the security and privacy services unit at [Deloitte & Touche LLP](#). Yet labor and privacy laws vary from country to country, she says. Data that's considered sensitive and must be encrypted in Europe might need to be more readily accessible for employee-employer transactions in the U.S.

**IT's response:** Assign ownership and responsibility. Companies must bring together stakeholders -- HR executives, the chief privacy officer (if there is one), the chief security officer and IT architects -- to sort through the complex requirements, develop processes for handling data, and design applications that include appropriate safeguards, such as encryption and restricted access, for each location.

### 2. Don't collect unneeded information.

The University of Nebraska, like many organizations, once used Social Security numbers to identify employees. But this practice increased the chances for sensitive data to fall into the wrong hands, says Joshua Mauk, the university's information security officer.

**IT's response:** Pare down the amount of information that is collected. Mauk says the university looked at the information it was gathering and determined where it could forgo the use of Social Security numbers. IT developed a process that now allows HR to assign workers unique numbers known as NUIDs that can be used on forms and records.

### 3. Protect sensitive data in every location.

Today, personnel data exists not only on paper, but also in electronic files that can reside in multiple locations. What's worse, many of those locations may be orphaned -- and left unsecure. "HR people in the field can have a bunch of information which may never make it back to a centralized HR office," Mauk says, "but that information has to be protected as much as the organization's ERP."

**IT's response:** Seek, monitor and manage all personnel data. Organizations must adopt records retention policies that specify what documents are kept where and by whom. The policies must also say how those documents should be stored and for how long.

The University of Nebraska uses an application that scans files and servers for sensitive data, allowing Mauk to find information residing in unauthorized or unmanaged areas.

### 4. Secure your paper files.

Improper handling of paper files is an ongoing problem, according to a number of security experts. "We still use paper a lot, but we focus so much on technology that we have a tendency to minimize paper," says Howard A. Schmidt, security strategist at International Information Systems Security Certification Consortium Inc., or (ISC)<sup>2</sup>, and a former government and corporate security executive.

Moreover, Schmidt says, because data protection often falls under the purview of the IT department, policies addressing the protection of paper files can fall through the cracks.

**IT's response:** Assign ownership of updated paper management policies. Companies need to implement policies on how to secure paper records and when to dispose of them. They should also provide ongoing training to HR staffers to underscore why those policies are needed and improve compliance reviews to ensure that the policies are followed.

#### **5. Share information -- carefully.**

HR professionals often need to share sensitive and legally protected information with colleagues inside and outside the company. That sharing, however, creates opportunities for data leaks, says Brad Johnson, a vice president at SystemExperts Corp., an IT compliance and network security consulting firm in Sudbury, Mass.

**IT's response:** Use automated and multilayered protections. Automatic encryption will help safeguard any data that's being electronically transmitted. And Johnson points out that automatic log-outs and session timeouts can help ensure that sensitive information doesn't remain visible on PC monitors when workers step away from their desks.

## **4 things your remote staff should know about your company's data security**

Your telecommuters are out there in the ether, along with all your company data.

**By Julia King**

April 14, 2008 (Computerworld) No matter their job title, business department, industry knowledge, computer savvy and/or exposure to security training, end users are the second-weakest spot in every organization's security fence. They are bested only by one subgroup of employees -- remote workers.

Think of the person who works in a satellite or branch office, perhaps with just one or two other employees. Think of the person who works three days a week at corporate headquarters and then travels with his laptop or telecommutes on other days. Think of the countless salespeople working from hotel rooms, airport gate areas, customer sites and [Starbucks](#) shops. These are the people who cause security managers to lose the most sleep.

### **1. Be aware that almost every data decision has a security implication.**

Security awareness training typically occurs on an annual basis, yet remote users make hundreds of security choices every week in the course of their work, says Carol Suchit-Hudson, director of citywide security for the New York municipal government.

For example, should they pop into the corner coffee shop and hop on its wireless network to answer an urgent e-mail? Or if their flight is delayed, should they use that extra hour to work on that customer spreadsheet?

**IT's response:** One of the best ways to ensure that remote workers make the right decisions is to offer them more frequent training coupled with periodic security reminders that are tailored to the way they work.

"The appropriate step is to tweak your education program based on the type of user," says Suchit-Hudson. That means using real-life examples and anecdotes. "No one wants to sit through training that isn't applicable to their needs," she says.

### **2. Your children aren't afraid to download.**

"Mom, can I use your computer to check online for my homework?"

Answering "yes" to this question -- as many parents do -- can open the gates to security hell, experts say. "Letting kids and others download programs and data of unknown origin onto their machines is one of the biggest worries we have for telecommuters," says Matthew Kesner, chief technology officer at Fenwick & West LLP in Mountain View, Calif.

**IT's response:** Even the most Draconian of usage policies won't end such incidents altogether. Instead, try appealing to users' self-interest, Kesner advises. If a user has downloaded an unauthorized program or left a wireless connection open

after working at home, it will really slow their computer down, he notes. "That's how we message it," he adds. One more tip: Regularly monitor users' hard drives.

### **3. Be a responsible gadget geek.**

BlackBerries, flash drives, mobile phones and handhelds frequently contain critical corporate data, yet most users treat these relatively low-cost devices far more casually than laptops.

**IT's response:** "Our rule is, if we don't own it, you don't plug it into our network," says Chris Blake, workstation administrator at The Benchmark Group, an architectural and engineering firm in Rogers, Ark.

Another option is to instead have users upload and download data from the server and to encrypt all data transmissions, he says.

### **4 Don't forget it -- shred it.**

Paper may seem quaint in our increasingly digital world. Yet, it's actually quite dangerous if tossed around carelessly, says [Darryl Lemecha](#), CIO at Vertafore Inc., an insurance software and services company in Bothell, Wash. "Dumpster diving remains a common way for thieves to get information," he says. "People have become quite accustomed to shredding at work, but there are still individuals who work from home who are without a shredder."

**IT's response:** Shredders for all. And they should be cross-cut shredders, so thieves can't piece back together documents that have been torn in only one direction.

## **4 things your administrative staff should know about your company's data security**

Just one step from the executive is a worker who often has high-level data access.

By Stacy Collett

---

April 14, 2008 (Computerworld) Administrative staffers may not have their fingers on the pulse of business-critical operations, but they do get their hands on a lot of sensitive company information.

Executives often grant administrative assistants and record-keepers access to strategic data and correspondence to make their own lives easier. As a result, these well-meaning assistants are often targets of hackers, scammers and even espionage.

### **1. Beware of 'pretexting.'**

Up to 70% of IT breaches are internal in nature, according to Douglas Beaver, vice president, North America, at Asero Worldwide Inc., a Washington-based security consulting firm. In many cases, employees give out information accidentally.

Administrative staffers must guard against pretexting scams, which involve setting up a scenario to persuade a target to release information or perform an action.

"It's typically done over the phone," Beaver explains. "It's not as simple as a lie. The pretexter does some prior research and uses pieces of known information, such as a birth date or Social Security number, to establish legitimacy in the mind of the target." That information can include how to access systems, customer information or any variety of data.

"There's a lot of turnover in these positions, and generally it's a younger workforce," he says. "The inexperienced workforce is more prone to fall prey to pretexters."

**IT's response:** Beaver advises companies to train staffers on how to properly screen calls. Establish policies on what information they can or can't release, and retrain them with real-world examples on a regular basis.

### **2. Administrative staffers can be espionage targets.**

In 2005, Israeli fraud investigators cracked a major espionage case in which several corporations hired private investigators to secretly install software on administrative staffs' PCs. The machines became infected by a Trojan horse that would steal financial information.

According to investigators, the hacker who created the program used two methods to plant his malicious software in the target computers. One was to send it via e-mail. The other was to send a disk to the target company that purported to contain a business proposal from a familiar firm that would arouse no suspicions. Then, when an employee loaded the disk to view the proposal, the Trojan horse would infect his computer.

**IT's response:** Make workers aware of the various methods of espionage. "Losing sales projections for next quarter is potentially much more damaging than getting a virus on the network that inconveniences the IT department," says Avishai Wool, chief technology officer at Algorithmic Security Inc., a firewall management company in Reston, Va.

### **3. Don't accept gifts from strangers.**

Most administrative staffers are happy to pick up a few free items at a conference or trade show. But those disks and memory sticks can come loaded with software that could disrupt your systems.

**IT's response:** Set a policy discouraging employees from bringing these items to work. "If somebody gives you a free CD or DVD," even at a trade show or business conference, "don't plug it into your work computer," Wool says. "Definitely don't plug in USB sticks," because they can contain software that can launch automatically, he adds.

### **4. If you want to move up the corporate ladder, keep your record clean.**

When administrative assistants are hired, the position might not call for a criminal or financial background check. But as they move up the corporate ladder, a clean record becomes more important.

Tell staffers that they should expect to be "revetted." They should keep their personal finances and police records spot-free.

"You have an administrative staffer working at a junior level who now has a credit card for booking travel. Or the CEO might have a massive expense account, and they're not going to notice if [the staffer] buys a computer to sell on [eBay](#) when paying the bill," says Bill Nichols, a senior consultant and practice leader at Control Risks Group Ltd. in Washington.

**IT's response:** Run occasional checks. Knowing that an employee hasn't committed a crime or gotten into financial difficulty since his initial hiring will reduce risk.

