

# Security Trends Report

09/21/07

## Infected job search sites lead to info theft for 46,000

Researcher says hoards of stolen data swiped by Prg malware

**August 17, 2007** ([Computerworld](#)) -- A security researcher at [SecureWorks Inc.](#) has uncovered a cache of financial and personal data that was stolen from about 46,000 individuals by a variant of Prg, a Trojan program gaining notoriety for its quick-change behaviors.

The stolen data includes bank and credit card account information and Social Security numbers as well as usernames and passwords for online accounts. Many of the victims were infected and reinfected as they visited several leading online job search sites, including the popular Monster.com.

Don Jackson, the SecureWorks researcher who found the collection, said it was the largest single cache of data he discovered from the Prg Trojan, a piece of malware first seen in the wild in June. According to Jackson, the server he examined is still collecting stolen data, with up to 10,000 victims feeding it information at any particular time.

That server is one of 20 similar servers worldwide that are collecting and storing data stolen by Prg. Twelve of those servers - including the one with the large data cache -- are being managed by a single hacking group known for naming their attacks after car manufacturers such as Bugatti, Ford and Mercedes, Jackson said.

The "car group's" success in compromising and stealing information from so many individuals is based on two factors, Jackson said. The first factor appears to have been their success in widely distributing the malware. He says the group used online ad aggregation services to place infected ads on job-search services as well as other Web sites, he said.

A user clicking on one of the malicious ads is taken to an exploit page that "fingerprints" the user's browser and then serves up between one and four exploits designed to infect the user's system with the Trojan. From that point on, all information the user enters into the browser is captured and sent off to the hacking group's servers, Jackson said.

The other reason for the widespread compromises is the group's sheer industry -- they've been releasing a new variant of the Trojan every five days to a week, on average, and sometimes even quicker. Antivirus tools are having a hard time keeping up with the variants, Jackson said, so infections are going undetected for several weeks in many cases. Many of those whose data has been stolen appear to have been infected multiple times by successive variants of the Trojan.

A number of Prg variants are known to operate in part by opening up Port 6081 on victims' computers and listening for connections there. Almost no legitimate programs are known to use 6081; some experts suggest that concerned parties looking to cut Prg off at the knees might [start by](#) blocking inbound and outbound traffic on the port. If a Prg infection on your machine is undetectable by your anti-virus package but you detect the malware's characteristic activity on Port 6081, your computer will need to be booted into Safe Mode and another scan will need to be run.

If that fails, manual removal or reinstalling the operating system may be necessary. [Symantec](#), which refers to the malware as Trojan Infostealer.Monstres, has posted [additional info](#) on how to detect and remove the threat.

Prg appears to be a variant of a somewhat older Trojan known as wnspeem, discovered last October. Like the earlier model, Prg is designed to sniff sensitive data from Windows internal memory buffers before the data is encrypted, which means that the malware can circumvent SSL security measures. When SecureWorks researchers [noted back in June](#) that a Prg construction kit was making the rounds, the data caches they analyzed contained a remarkable amount of information from corporate PCs -- indicating perhaps that attackers are now expanding their focus.

It's not entirely clear how the stolen information in the latest attacks is being used, but Jackson says that the kind of data that the Trojan has cached seems to indicate that the data is being stolen for identity theft purposes.

## --One in Five US Surfers Are Victims of Internet Scams

16 August 2007

According to a survey commissioned by Microsoft, one in five US based Internet users has fallen victim to an online scam. Of those victims, 81% admitted doing something to compromise their system, such as clicking on attachments in an email which appeared to be from someone they trusted. The survey revealed that more than half of those surveyed "had little or no knowledge of current online threats and scams." The report highlights that while security tools are important, "people need to be constantly updated to the threats that exist and how to avoid them"

<http://www.vnunet.com/vnunet/news/2196820/one-five-surfers-fallen-internet-scam>

[Editor's Note (Skoudis): We really do need an awareness campaign directed at the general public, like the anti-smoking, anti-drug, anti-litter, and anti-crime TV campaigns of the past.

(Paller) An awareness campaign is definitely needed. For it to have an impact it needs to be required, timely, and repetitive. The best model is the USAID "Tips of the Day" in which every user reads a security tip and answers a quiz question BEFORE being allowed to start computing - every time they sign on. That approach allows repetition of the critical tips and up-to-the-minute education. The fact that the rest of the federal government still uses ineffective online or live annual awareness training implies that many government security leaders are unaware of the methods attackers are using to penetrate their agency computers and networks.]

---

Aug 15, 2007

## Spam Surge Sways Stock Market

Last week saw the Internet's biggest-ever spam surge in a single day, and also offered a lesson on why "pump and dump" stock-market spam campaigns have become so prevalent, according to Postini.

The campaign was an example of the recent trend of junk e-mail using PDF attachments as a way of getting around spam filters. But Postini said the surge marked the biggest increase in spam it had ever recorded, boosting total spam volumes 445 percent in a one-day period at its peak on Thursday morning.

Sophos Labs, which also detected the spam surge beginning on Tuesday, said it intercepted about 500 million PDF spams advertising shares in a particular target company.

The massive size of the campaign is unusual, according to Sophos Labs Director Mark Harris. "To date, the trend has been for smaller campaigns that rapidly evolve and modify themselves to try to get round anti-spam products," he said on the Sophos blog.

The campaign had tailed off by Thursday but didn't disappear—rather, it continued to mutate over the weekend, Sophos said.

In the meantime, the campaign appeared to have another notable effect, in that the company targeted a small Florida-based firm called Prime Time Group involved in wireless and retail interests, and as of Thursday afternoon actually saw its share price rise 84 percent from its Monday value, before plummeting again.

In response, Prime Time was forced to issue a statement avowing it had nothing to do with the campaign, and even ordered a Non Objecting Beneficial Owners list to track down investors who violated stock-market regulations during the course of the share price fluctuations.

Harris said the spam's effect on Prime Time's share price shows how such campaigns play on human nature. He noted that many of those who buy into the stock advertised are not necessarily fooled by the campaign, but simply want to get in on the profits that might be generated by the "pump and dump" scam.

"While recipients of this type of spam continue to try and profit on these 'tips' stock, spam will continue," Harris wrote.

— *Matthew Broersma*, [Techworld.com](http://Techworld.com)

## Numbers, Sophistication Way Up"

Information Security (08/07) Vol. 10, No. 7, P. 13 ; Fisher, Dennis

Security officials have long claimed there has been a shift in the demographic of hackers, as troublesome teenagers have been supplanted by computer science experts, possibly funded by hacking gangs. This transformation has resulted in an increased number of successful and sophisticated malicious online attacks, while stopping such attacks has become more difficult. "For things like this, signature-based defenses are dead. They can't compete," says Pete Allor, IBM ISS director of intelligence. Allor says the company encounters about 14,000 pieces of malware monthly, while hackers are targeting applications such as Web browsers, databases, and CRM applications. Previously, operating systems have been the choice

target for hackers, but applications tend to allow accessibility to more valuable data such as personal user information linked to users' bank accounts. Allor says that there has been an increase in "commercialization" of attacks, while most of the hackers join together for one or two efforts then dismantle before moving on to other attacks. In 2006, downloaders remained the leading choice of malware attacks, followed by Trojans and worms. Viruses and keyloggers ranked at the bottom of the hacking list.

## **More Than \$7 Billion Lost to Online Threats"** **Government Technology (08/07/07)**

Viruses, spyware, and phishing schemes have cost U.S. consumers more than \$7 billion over the last two years, according to Consumer Report's latest "State of the Net" survey. The survey also found that the number of computer virus infections held steady last year--a finding that is seen as a mark of progress for consumers and software makers because the threats have become more challenging. Meanwhile, the number of spyware infections dropped, though the chances of being infected with spyware are still one in three. The chances of suffering serious damage as the result of a spyware infection remain one in 11. Based on the findings of the survey, Consumer Reports estimated that the problems caused by viruses and spyware resulted in damages of at least \$5 billion during the past two years. Finally, the survey found that phishing emails are improving by using better grammar, more believable stories, and more legitimate-looking Web addresses. Nevertheless, the percentage of users who submitted personal information in response to phishing emails last year remained at 8 percent, where it has stood for the past two years.

## **Flight Plan for Security"**

**Government Computer News (08/13/07) Vol. 26, No. 21, ; Jackson, William**

Seymour Goodman of the Georgia Institute of Technology argues that the IT community must take a proactive stance toward securing cyberspace, and suggests using the Civil Aviation Convention as a prototype. The convention, to which nearly every country belongs, concentrates on standardizing rules for guarding the aviation infrastructure, and mandates operational competence in participating countries. As a result, the aviation industry is relatively safe despite its innate risks and high target profile. Meanwhile, the current information infrastructure was designed to be easily accessible, and "access is the enemy of security," according to Goodman. There are currently some 1.3 billion users of the Internet in over 220 countries. The majority of email traffic is spam, malware has infected roughly 14 percent of American household PCs, and today's global, interactive networks have no single source of authority or control. While the Council of Europe's Convention on Cybercrime is attempting to address such issues, its emphasis on law enforcement is too passive, says Goodman. Moreover, the convention does not insist that member countries create strategies for enforcing its regulations. In comparison, the Civil Aviation Convention insists that participating countries be able to fulfill and enforce its safety standards. A similar scheme in the cybersecurity world may find a helpful vehicle in the International Telecommunication Union, suggests Goodman.

## **Web 2.0 Means Re-examining IT Security Approach, Says Gartner"** **Government Technology (08/14/07)**

Gartner reports that Web 2.0 is fostering the technological expansion of businesses, yet such benefits are not without security exposures. At the company's IT Security Summit, Gartner's Joseph Feiman said the increased usage of online services and communities has led to employers "relinquish[ing] a level of control that they historically would not tolerate." As such, Feiman said enterprises must reevaluate their management of Web 2.0 security risks that can be categorized into two categories: Protecting internal users and the organization, and protecting external applications. Internal risks include malware-infected RSS feeds and leaking information via blogs while external threats include third-party content and participating in open user communities. Since enterprises remain divided on policies regarding controlling company content via the Web, reviewing the content they wish to have open to the public and using licensing agreements will reduce exposures to security vulnerabilities. Gartner recommends companies employ Web vulnerability scanners, validate input on the server-side, employ secure coding, and assume that public content may be used in unforeseen ways. Firewalls and content monitoring and filtering and data loss protection are also useful tools to mitigate security risks.

## **TJX says breach costs may exceed \$150M**

Takes \$118M second-quarter charge to cover some expected losses  
**Jaikumar Vijayan**



**August 15, 2007 (Computerworld) -- TJX Companies Inc.** yesterday disclosed that losses from the massive data breach [disclosed](#) in January could reach well over \$150 million, which analysts said make it the costliest theft to date.

The company in January [acknowledged](#) that 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipsed the 40 million records compromised in a mid-2005 breach at [CardSystems Solutions Inc.](#), making the TJX compromise the worst ever involving the loss of personal data.

The Framingham, Mass.-based discount retailer Tuesday [reported](#) after-tax charges of \$118 million in its second quarter ended July 28 to cover potential losses because of the data breach.

The charge includes \$11 million in costs incurred during the quarter and a reserve of \$107 million to cover potential future losses related to the breach. The reserves reflect the company's best estimation of probable future costs stemming from litigation, cash liabilities, investigations and other claims, the company said.

In addition, TJX yesterday said it expects to incur noncash charges of around \$21 million during fiscal 2009 that are not included in the reserve fund.

"Together, these cash and noncash charges represent the Company's best estimate of the total losses the Company expects to incur as a result of the computer intrusion(s)," TJX said in a statement accompanying its quarterly results.

Yesterday's numbers come on top of the \$25 million in after-tax costs TJX reported in the two previous quarters in connection with the breach.

Deven Bhatt, director of corporate security at Airline Reporting Corp., said the rising costs related to the TJX breach should help him convince management of the importance of heavy security investments.

Bhatt said he is not surprised by the projected costs of the breach, but noted that top executives at the Arlington, Va.-based provider of ticket distribution and settlement services to more than 145 air and rail carriers were when he showed them TJX's SEC filings.

"They definitely were shocked," by the numbers, Bhatt said. "It definitely helps security guys like me to make a solid business case. It's a lot cheaper to protect than to do cleanup."

As high as the costs disclosed by TJX are, the total could easily go even higher over the longer term, warned [Avivah Litan](#), an analyst at Stamford, Conn.-based [Gartner Inc.](#)

"They have incurred about a third to a half of the costs they could end up having to pay," for the breach, Litan estimated. "They are facing potentially expensive and extensive litigation, which is why they have reserved more for losses. There's never been anything this big in terms of the breach itself and its cost implications."

Litan said the breach will likely cost TJX about \$500 million over the long term.

TJX, which owns retail companies such as T.J.Maxx, Marshalls and Bob's Stores, disclosed in January that someone had broken into computer systems and illegally accessed credit card data of customers in the U.S., Canada, Puerto Rico, the U.K. and Ireland.

The disclosure prompted several lawsuits, including one by the Massachusetts Bankers Association, which seeks tens of millions of dollars in restitution for banks that were forced to block and reissue thousands of debit cards. The Arkansas Carpenters Pension Fund, which owns 4,500 shares of TJX stock, and the Merchant Law Group LLP in Canada have filed other lawsuits.

Several more states are actively contemplating lawsuits against the retailer, according to an analyst who is helping one state with such litigation. Such litigation could end up costing TJX millions of additional dollars, said the analyst, who requested anonymity.

The TJX breach and its anticipated costs should serve as a "wake-up call that current security approaches are not working," said Bill Bartow, vice president of marketing at security vendor Tizor Inc. in Maynard, Mass. Like Litan, Bartow also expects that the costs associated with the intrusions could be much higher than the current TJX estimates.

Khalid Kark, an analyst at Cambridge, Mass.-based [Forrester Research Inc.](#), said the latest disclosure by TJX supports his earlier prediction that the breach will ultimately cost the retailer close to \$1 billion.

"The first-year costs are significant," Kark said. "But we tend to underestimate the costs over time," especially from lawsuits that play out over several years. "There's no way to figure out how much this thing is going to cost them in the long run."

Despite the charges, TJX reported strong second-quarter results. Sales in the period increased by 9% to \$4.3 billion from \$3.9 billion a year earlier. Sales for the first six months of the fiscal year are up by 7%, the company said. Similarly, the company's stock prices have for the most part not been affected by the breach.

Even so, the sheer scope of its breach-related costs should convince "people who are on the fence" to spend the millions of dollars they sometimes need on security fixes, Litan said. "Strengthening data security is much less expensive than

responding to a security breach." The TJX breach gives "security managers a strong business case," for seeking additional investments in information security, she added.

## Greetings! Someone has sent you an e-card virus

Fake plain-text e-card variants look real, carry nasty computer viruses

**Todd R. Weiss**

**August 15, 2007** ([Computerworld](#)) --

Think you got a cheery greeting card from a friend via e-mail?

Well, think again, and be careful before opening it. A new form of fake e-card notification e-mails are unleashing nasty viruses and virus-carrying Trojan horses on unsuspecting users.

While e-card-triggered viruses and Trojan horses are not new, the latest versions are becoming more difficult for typical antivirus and antispam defenses to detect, according to alerts issued today by security software vendors [Avinti Inc.](#) and [F-Secure Corp.](#)

The new complication, said Dave Green, chief technology officer at Lindon, Utah-based Avinti, is that the latest slew of fake e-card e-mail notifications are using plain text in their messages, which don't get scanned and scrutinized by antivirus and antispam defense applications. While the e-mails don't contain pasted links or attached files that a recipient can click on to get a computer infection, many e-mail clients automatically convert the included text into a clickable link when the e-mail clients recognize a Web address in the text.

"It appears they have done that to get around a lot of the parsing used by antivirus and antispam applications" to fight such attacks, Green said. "It's an interesting cat-and-mouse game between the bad guys and the good guys."

"Apparently, they've found that they can be very successful in getting these through by not having it be formatted as an HTML message," Green said.

All recipients have to do to trigger the virus is to click on the link created by the e-mail client once they have read the message, he said.

Adding to the confusion and the potential seriousness of the problem, he said, is that the perpetrators sending these e-mails are using the names of some of the most popular electronic greeting card companies in their messages and Web links.

Avinti said it has updated its Avinti Isolation Server product to protect against such attacks, while other vendors are still updating their own products.

Avinti's alert said the links to the fake e-greeting cards lead to IP addresses in various locations, including the U.S. and Eastern Europe, and many are registered to U.S. Internet service providers. The damaging payload files are new variants of the Storm Worm virus that was first detected in January, the company said.

In its alert today, Helsinki, Finland-based security vendor [F-Secure](#) said the fake e-card messages from one group of online criminals appear to have changed since last night, when they dropped the use of attached files and went to plain-text messages.

An included link then tells the recipient to install a free "[Microsoft](#) Data Access" application to retrieve the e-card, but that file - msdataaccess.exe -- is a damaging virus. F-Secure said it has identified the virus as Email-Worm.Win32.Zhelatin.gg.

Danny Allan, director of research at security analysis vendor [Watchfire Corp.](#) in Waltham, Mass., said he has seen similar all-text e-greeting mailings before, but the numbers have increased lately.

For antivirus and antispam vendors, the theory had been that if the message includes plain text without links and attachments, it could cause no harm, he said. That approach has to change, Allan said.

User need to be cautious and not click on links they find in e-mails, Allan said. Instead, they should go directly to a Web site by typing its address into a Web browser and go there on their own, bypassing links that could be malicious.

Vendors will have a tough time making the problem go away completely, he said, because they can't devise ways of evaluating every Web link or instance in an e-mail. However, they can improve detection of suspicious encoded characters and domain names in messages.

"If there was a silver bullet that could solve the problem, the antivirus companies would have done it," Allan said.

Zully Ramzan, a senior principal researcher at Cupertino, Calif.-based security vendor [Symantec Corp.](#)'s security response team, said Symantec has seen plain-text attacks before and doesn't view them as a new problem.

"There's been a bit of a resurgence lately" with e-card notification messages, possibly because of last month's July 4 holiday or because criminal groups have been organizing mailing campaigns, he said.

Andrew Jaquith, a security analyst at Boston-based [Yankee Group Research Inc.](#), said the latest e-greeting attacks are an example that criminals "are going to be coming up with more and more ingenious ways of tricking people or exploiting ways of tricking your e-mail client. This is just one of any number of ways that these guys are going to try to lure users to do something they shouldn't."

## PCI Is Security Simplicity, Not Complexity

**The payment card industry data security standard seems to make relatively smart people instantly dim-witted as**

**they complain about its so-called complexity.**

The irony is that PCI, as the standard is called, is one of the best things to happen to the security of consumer data, yet many think it is as complex as rocket science.

### **PCI's Genesis**

The last decade has seen the growth of security and privacy standards and regulations, from decent standards such as ISO-17799 to abhorrent regulations such as Sarbanes-Oxley. At the same time, billions of dollars of credit card purchases, combined with insecure networks and systems that process consumer data, have placed consumer data at significant risk. Credit card fraud is getting out of control and the losses are becoming too great to bear. The outgrowth of that was the [PCI data security standard](#), or PCI DSS.

Visa, MasterCard, American Express, Diner's Club, Discover and JCB collaborated to create a new set of standards and require that all merchants and service providers that handle, transmit, store or process information concerning any of these companies' cards, or related card data, be compliant with them. If they are not compliant, they can face monetary penalties and/or have their card processing privileges terminated by the credit card issuers.

The primary purpose of PCI is to force organizations to embrace common security controls to protect credit card data and reduce fraud and theft. The following are the six primary control areas comprising 12 specific requirements of the PCI DSS:

- **Build and maintain a secure network**
  - Install and maintain firewall configurations
  - Do not use vendor-supplied or default passwords
- **Protect cardholder data**
  - Protect stored data
  - Encrypt transmissions of cardholder data across public networks
- **Maintain a vulnerability management program**
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
  - Restrict access to need-to-know
  - Assign unique IDs to each person with computer access
  - Restrict physical access to cardholder data
- **Regularly monitor and test networks**
  - Monitor and track all access to network resources and cardholder data
  - Regularly test security systems and processes
- **Maintain an information security policy**
  - Maintain a policy that addresses information security
  -

A quick review of these 12 items reveals a textbook outline of the fundamentals of information security. They reflect attention to detail and risk management. One can sum up PCI in a single word: pragmatic. It takes a realistic approach to the problems of consumer credit data and applies a common sense set of security solutions. PCI takes a narrow focus on what it attempts to solve, as opposed to Sarbanes-Oxley, which lacks any form of specific detail. PCI is a godsend for the protection of consumer credit card data.

Gordon Rapkin, CEO of security solutions provider Protegrity, notes that “PCI DSS is truly a sensible approach to data security. It’s not an arcane set of rules established by some remote authority; it’s a set of industry best practices that help retailers secure their networks and protect their customers’ privacy. Compliance with the standard brings real benefits; it’s far less costly to prevent attacks than it is to clean up after a breach.”

### **The Backlash**

Given what PCI is trying to accomplish, one would expect it to be welcomed with open arms by the industry. To a degree, it has. But surprisingly, there seems to be a cabal that has made it its duty to attack PCI rather than embrace it. There is nothing complex or mysterious about PCI, yet that appears to be lost on some very smart people.

One recent example: Michael Mathews, chief operating and technology officer at security-services company CynergisTek, wrote an article called [PCI Has Lost Its Way, Growing Overly Complex and Costly](#), for the June 2007 issue of *Information Security*. Mathews repeatedly stresses the complexity of PCI. But where is it? Each of the 12 main requirements and corresponding specifics are extremely pragmatic and can be classified as information security 101. Mathews writes that because of these and other “complications,” many merchants remain noncompliant to many facets of PCI DSS.

The issue really is that these merchants have created their networks with little to no thought to security and privacy. They have placed minimal controls on their users, given no direction to their application developers, nor documented required procedures for their administrators on how the network should be managed. Merchants are not noncompliant due to PCI DSS; they are noncompliant because they never developed their security programs in the first place.

Mathews also states that unwarranted complexities in the standard are raising the cost of compliance, but does not name any of these complexities. No matter how many times the author uses the word *complex*, it can’t change the reality that the PCI DSS is practical, not complex.

An additional complaint is that answering the [PCI DSS self-assessment questionnaire](#) requires small merchants to hire teams of experts to help them interpret the intent of the questions. The 9-page PCI self-assessment questionnaire is straightforward and requires minimal interpretation. As to teams of experts, that is clearly overkill. Answering the questionnaire can be done by a single consultant in collaboration with the client, for the vast majority of merchants.

In another example, the director of IT at Virgin Entertainment Group [told Computerworld](#) that while much of the PCI standard includes good, solid network and security policies, some of it is “over the top” and can be confusing. For someone smart enough to be the director of IT for a leading-edge company like Virgin Entertainment, which places significant importance on IT, it is difficult to understand how he could find PCI confusing.

He also contends that the costs of meeting the requirements do nothing to boost a retail company’s bottom line, with no direct return on investment. Recent events demonstrate otherwise. Had TJX Companies better developed its security posture, it would likely not be facing myriad law suits. TJX violated some of the basic tenets of the PCI DSS, and its insecurity has had a direct negative financial effect. The company announced that in the most recent quarter, it took a \$12 million loss, equal to 3 cents per share, because of the loss of more than 40 million credit and debit card numbers stolen from its systems over an 18-month period—one of the largest customer data breaches to date.

The \$12 million in losses was for costs incurred to investigate and contain the intrusion, improve computer security and systems and communicate with customers, as well as for technical, legal and other fees. The company also reported that it expects that it will continue to incur these types of costs related to the intrusion in the second quarter and it estimates that those costs will total 2 cents to 3 cents per share.

Besides facing numerous other federal and state lawsuits, the Massachusetts Bankers Association, which represents 207 financial institutions, filed suit against TJX in federal court in Boston in April 2007. In addition, the Securities and Exchange Commission said that complaints seeking class-action designation on behalf of customers were filed in April and May in the federal courts of five additional states: Illinois, Michigan, Missouri, Ohio and Texas.

Such breaches are precisely what PCI comes to prevent. Had TJX followed the principles of PCI and properly secured its systems, it would have had a positive return on the investment, and saved the organization millions of dollars, in addition to significant negative publicity. Absolutely nothing complex about that.

Dave Taylor, president and CEO of the [Payment Card Industry Security Vendor Alliance](#), notes that “the PCI DSS demonstrably benefits card holders, the payment card industry as a whole and individual businesses—it’s a comprehensive, sensible security standard built on the shared knowledge of industry leaders and security experts.”

All it takes is one successful hack attack to wipe out years of so called “savings” gleaned from not implementing security. Online crime has become more sophisticated and far better organized over the past several years. No business wants to risk its bottom line or consumer confidence on the hopeful idea that a security breach just won’t happen to them.

The time to take security seriously is before an attack happens, not after. That is precisely what PCI aims to do.

## Conclusion

Rather than making excuses about how difficult or costly PCI is, companies need to step up to the plate and start taking security seriously. They need to get a clear roadmap of their priorities and ensure they are accomplished to meet the minimal security requirements.

PCI is the best thing that has happened to consumer data protection in the payment industry in many years. The quicker it is embraced and implemented, the better off we all will be.

*Ben Rothke, CISSP, QSA, is a security consultant with BT INS and the author of [Computer Security: 20 Things Every Employee Should Know](#) (McGraw-Hill, 2006).*

**--DOD Requires Mobile Data To Be Encrypted** (August 13, 2007) The CIO for the US Department of Defense, John Grimes, has issued a memo requiring the encryption of all sensitive data stored on mobile devices. Mobile devices are defined as laptop PCs, personal digital assistants, USB thumb drives and other removable media devices such as compact discs. According to the memo, all mobile devices must be encrypted in accordance with the National Institute of Standards and Technology's Federal Information Processing Standard 140-2. Dave Wennergren, DOD's deputy CIO states, "The memo will help to ensure that we protect all DOD information on devices and media while outside a protected workplace"

<http://www.fcw.com/article103467-08-13-07-Print>

[Editor's Note (Pescatore): The July 3 memo says that "unclassified DoD data that has not been approved for public release" must be encrypted when on mobile devices like PDAs or USB drives and the like. This is badly needed - there have been many reports of boxes of USB drives at dry cleaners near military bases with sensitive but unclassified information on them.]

**--Agencies Struggling To Implement OMB Policies** (August 13, 2007) Many agencies report that they are struggling to keep up with the number of policies issued by the Office of Management and Budget in response to the 2006 security breach at the Veterans Affairs Department, where an employee lost personal data on 26.5 million veterans. The requirement to log and verify all computer-readable extracts from databases containing sensitive information is proving to be the most difficult to meet for most agencies. In the latest memo issued by the OMB, a deadline of September 21 is set for agencies to report on their plans to remove Social Security numbers from publicly accessible information systems and procedures for notifying federal authorities when a data breach occurs.

<http://www.fcw.com/article103460-08-13-07-Print>

## Your data's less safe today than two years ago

Crooks are outpacing prevention efforts; ID theft is up 50% since 2003

**Robert L. Scheier** 

**August 20, 2007** ([Computerworld](#)) -- Today's electronic world is a risky place for your personal data -- and it's not getting any safer. More than 158 million data records of U.S. residents have been exposed as a result of security breaches since January 2005, according to [The Privacy Rights Clearing House](#), a nonprofit consumer rights organization.

As fast as banks, merchants and consumers add new layers of security to their storage systems and network, say security analysts, new technologies -- or simply careless users -- create new security holes that aggressive and sophisticated identity thieves eagerly exploit. The result, says [Avivah Litan](#), a vice president and distinguished analyst at [Gartner Inc.](#), is that "things will get worse before they get better."

### Clever Crooks

Attacks against both consumers and retailers have "really grown in the last couple of years," says Litan, who cites a Gartner survey showing that approximately 15 million Americans were victims of identity-theft related fraud in the 12 months ending in the middle of 2006. According to Gartner, that's a 50% increase since 2003, and the average loss per incident was \$3,257, more than twice the level for the same period a year earlier, according to the survey.

The number of companies whose customers were targeted by phishing attacks -- a fake e-mail asking for sensitive information -- grew by 20% in the second quarter of 2007, says Terry Gudaitis, cyberintelligence director at Cyveillance Inc., an Arlington, Va.-based firm that monitors the Internet for malware and other threats. While such attacks used to target customers of only a few large banks, they now impersonate "credit unions, hotel chains, insurance companies -- it's all over the board," says Todd Bransford, vice president of marketing at Cyveillance.

During the same period, Cyveillance also identified more than 2 million URLs that distribute malicious downloads to site visitors without their knowledge, as well as 2.5 million stolen credit card numbers online.

Criminals are also getting smarter. [Larry Ponemon](#), chairman and founder of Ponemon Institute, which conducts research on privacy and security issues, calls it "inverted customer relationship management," in which criminals target the wealthiest individuals for their attacks.

Some are even buying marketing lists to piece together profiles of "who's got the Platinum [American Express card] and who's got the account with Merrill Lynch and who doesn't," says Litan.

"Hackers are exploiting Internet auctions, nonregulated money transmittal systems and the ability to impersonate lottery and sweepstakes contests," among other scams, wrote Litan in a February 2007 research report.

### **Theft and fraud?**

Hard figures on identity theft and identity fraud (using stolen data to commit a crime) are difficult to come by. A June 2007 report from the Government Accountability Office said that of 24 large data breaches reported in the media between January 2000 and January 2005, only three "appeared to have resulted in fraud on existing accounts, and one breach appeared to have resulted in the unauthorized creation of new accounts."

However, the study noted it's difficult to determine the exact damage, because while at least 36 states require companies to notify consumers of data breaches, victims often don't know their information has been stolen or how it was stolen. Thieves may wait a year or more before using the data, and may use only some of it so as to not alert the card issuer, which could cancel the entire block of stolen cards.

Mary Monahan, a partner, editor and analyst at Javelin Strategy & Research, a research and consulting firm in Pleasanton, Calif., takes a more upbeat view. She says that prevention and awareness by both consumers and businesses helped reduce the number of adult victims of identity fraud in the U.S. from 8.9 million in 2005 to 8.4 million in 2006, and the dollar amount of fraud dropped 12% from \$55.7 billion to \$49.3 billion.

Those figures, however, include all types of identity fraud, the vast majority of which Javelin says result from traditional causes such as lost or stolen checkbooks or credit cards. Rachel Kim, a research associate at the firm, also points out that less than 1% of victims whose information has been stolen experience fraud. Despite the publicity of data breaches at companies such as The TJX Companies Inc., she says, the percentage of victims who knew how their data was lost who cited a data breach actually fell from 6% to 3% from 2005 to 2006.

Given all the unknowns, it's not surprising that even the experts are sometimes in the dark. A December 2006 survey of more than 200 North American security professionals by [Enterprise Strategy Group Inc.](#) showed that more than one-third had experienced a data breach at their company in the past 12 months, and another 10% didn't know if they had lost data.

### **Weak points**

One reason concern about identity theft is increasing is that with the expanding adoption of high-speed Internet service, more consumers are spending more time online, where they might share sensitive data.

And just as hackers target consumers they believe to be wealthy, they also take aim at companies they believe to have loose access controls, says Ponemon. Many companies don't maintain the same strict access control for contractors or part-time employees as they do for full-timers, says Mark McClain, CEO and founder of SailPoint Technologies Inc., an identity risk management vendor. "Folks on long-term contracts live outside the employee control system," he says. "It's very ad hoc: Bob hired Joe to help his group, and only Bob knows what access Joe has, and if Bob leaves, nobody knows what access Joe got."

"The old mind-set was that data breaches were the result of nefarious outside hackers, while the latest industry rhetoric blames insider attacks," Enterprise Strategy Group analyst Jon Oltsik says in his June 2007 report, "The Case for Data Leakage Prevention Solutions." However, the report states, breaches can be caused by either internal or external attacks, as well as logical hacking, physical theft and accidents. To reduce this wide variety of risks, he says, "large organizations need layered and extremely flexible defenses."

Just finding where sensitive data sits within the organization and where it's most vulnerable is a daunting task, says Scott Crawford, a research director at Enterprise Management Associates. Customer credit card information, purchase histories and other information might be stored anywhere, from a user's notebook computer to a Fibre Channel storage array at headquarters. "The data may move wirelessly; it may move through public links on the Internet; it may or may not be encrypted within the business and may be encrypted [only] part of the way," he says.

Retailers also often overlook vulnerabilities in devices such as point-of-sale (POS) systems that store data read from magnetic stripes on credit cards and can be accessed from the Internet, and printers that store data on hard drives as part of the printing process, says Gartner in a December 2006 report. The report predicts that by 2008, more than half of attacks

against retailers will be directed at POS systems and that by 2009, less than one-third of POS software will comply with prevailing security standards.

While retailers are always reluctant to spend money on security that could otherwise be spent to drive sales, they might be convinced by the news from TJX that a large data breach disclosed in January will cost the company \$118 million, says Litan.

Industry regulations such as the Payment Card Industry data security standard are forcing many companies to strengthen their security processes as well as the security tools they use, says Crawford. Visa U.S.A. Inc. says that about 40% of its 327 Level 1 merchants -- those that process more than 6 million transactions a year -- have demonstrated their compliance with the standard, up from 36% of the 230 Level 1 retailers counted at the end of 2006.

To counter a big spike in the use of counterfeit credit cards, Litan said card issuers, for a cost of about \$5 per card, could add strong authentication mechanisms such as a unique password that would be downloaded to the card each time the owner tried to use it. Because the user would need the physical card (and not just the card number, expiration date and security code) to make a purchase, "it wouldn't matter" if companies lost credit card information through data breaches, she says.

Even as companies try to tighten their existing systems, Web 2.0 sites -- such as social networking services where much or all of the content is generated by users -- have become a handy way to distribute malware as well as yet another innocent-sounding business to impersonate in a phishing scheme, says Bransford. "You tend to trust these social networking sites because you belong to them and wind up with malware on your PC."

In the second half of the year, Cyveillance predicts another 10% to 20% growth in the number of traditional phishing attacks, with more than 80% of the attacks aimed at customers of financial services customers.

So what's an IT manager to do to protect sensitive data? "Don't store [information] if you don't need it, encrypt it if you can, and put strong access controls around it -- and then monitor the access," says Litan.

And when you get home, check your own bank statement for any odd-looking transactions.

### **Tips for avoiding identity theft**

For companies:

- Just as you did for Sarbanes-Oxley, identify and secure the applications and devices most vulnerable to attack.
- Track access rights (and access activity) for contractors as tightly as you do for employees.
- Don't store data if you don't need to; encrypt it if you must store it.
- Educate and remind all your employees about the need for data security.

Tips for consumers:

- Monitor bank statements, credit card bills and credit reports for signs of ID fraud.
- Use up-to-date firewalls and antivirus/antispysware software on all computers.
- Be wary of performing transactions or spending time on unknown Web sites.
- Be alert for changes in the look or wording of emails from banks or other institutions, which might signal a phishing attack.

## Portable Devices Pose Growing IT Security Threat

Managers scrambling to manage flood of storage systems.

**Brian Fonseca**

**August 20, 2007** ([Computerworld](#)) -- Fabiana Gower considered some unconventional methods to prevent data losses when portable storage devices began appearing in her company's IT environment about three years ago.

"I stopped just short of Super Glue," said Gower, vice president of information systems at Martin, Fletcher, an Irving, Texas-based medical staffing firm.

"I wasn't able to find a way to lock USB ports so that they are inaccessible to employees short of going to a thin-client environment, which would have meant [an investment of] hundreds of thousands of dollars," she added.

Increasing numbers of IT and security managers are facing similar pressures to control access to corporate information stored on portable storage devices that are used both with and without the blessing of IT managers, according to experts.

Just this summer, the U.S. Department of Veterans Affairs issued a directive requiring that its employees, contractors and business partners use encryption or other means to protect data stored on all drives, including portable devices.

The edict follows the VA's loss of two drives over the past 15 months in incidents that exposed personal information of tens of millions of veterans and others.

In a statement to *Computerworld* last week, Bob Howard, CIO and assistant secretary for information and technology at the agency, said that the VA is also in the process of acquiring encrypted thumb drives and applying encryption to other devices and storage media. The process will be completed by the end of 2007, he said.

Martin, Fletcher eventually deployed PatchLink Corp.'s Sanctuary Device Control software on the 150 PCs on the company's network to curb data breaches via portable storage devices, Gower said.

The software from Scottsdale, Ariz.-based PatchLink enables IT personnel to issue and manage permissions based on employee rank. It can also be used to compile detailed audit reports and to encrypt content as it travels from corporate networks to portable devices, she said.

"For IT administrators, our job is not just setting up a computer for an employee to do their job. Our job is to safeguard the information of a company and make it accessible to those who need it and unavailable to those who don't," Gower said.

Businesses will struggle to keep their networks secure as long as they lack IT control over tiny storage devices connected to their systems, said Larry Ponemon, chairman of Traverse City, Mich.-based Ponemon Institute LLC.

"Attackers today aren't just college-aged kids sitting in their room at night trying to get into government systems. A lot of these guys are very sophisticated cybercriminals looking to take advantage of companies that don't have the best control over their network and devices," said Ponemon.

According to a Ponemon Institute security study, 59% of 1,035 IT security, data protection and privacy practitioners surveyed through June said their organizations currently lack the ability to detect lost or stolen USB memory sticks containing unprotected confidential information.

Ponemon recommended that IT managers step up their database scanning methods, do a better job of managing identity data and apply encryption techniques even if such moves harm system performance.

Jason Pufahl, information security team lead for IT services at the University of Connecticut in Storrs, is evaluating several portable media encryption products, including the open-source TrueCrypt tool from the TrueCrypt Foundation.

Pufahl noted that many students are either ambivalent or unaware of the high risk for data loss whenever they share ministorage devices.

"A lot of people don't even know what they're doing is inappropriate," said Pufahl. "A basic USB memory stick has up to 8GB

— that's a ton of space, and you can put them anywhere. They're really dangerous."

Jeff Moss, organizer of the DefCon hacking convention, suggested that IT managers approach TrueCrypt with caution because it runs only on Microsoft Windows-based machines.

Moss said the lack of an industry standard for encrypting data on portable drives is hampering efforts to boost the security of such devices.

"Something definitely needs to be done because these devices definitely get lost or stolen or [are] given to friends," said Moss.

Joe Gabanksi, network administrator for the city of Lake Forest, Ill., said municipal IT personnel first noticed a problem with portable devices after distributing removable storage devices to employees about two years ago.

Officials hoped to help employees more easily transport data, but found after a scan of the IT environment that a host of unauthorized devices were also linked to the network. At that point, Gabanksi said, the city's IT managers realized that the unofficial policy of connectivity-at-will needed to be tightened.

"We found considerably more activity on the network than we had ever anticipated," he said. "We had the iPod, digital music players [and] universal flash drives. We were shocked to see how much end users had already used them."

Gabanksi said the discovery spurred concerns over how to monitor and manage data coming in and out of his environment. Thus, the city moved to require that users register any devices they wish to connect to the corporate network.

Over the past year or so, the city also installed PatchLink's Device Control and Device Scanner tools to centrally manage and encrypt those devices.

"The thing that really moved us was to see that the companies and the agencies that did lose data [through portable storage devices] made the news. We didn't want to be a part of that," Gabanksi said.

## **Identity attack spreads; 1.6M records stolen from Monster.com**

Convincing phishing mail seeds bank account-stealing Trojan horse and 'ransomware'  
Gregg Keizer

**August 19, 2007** ([Computerworld](#)) -- The **46,000 people reportedly infected** by ads on job sites may be only a fraction of the victims of an ambitious, multistage attack that has stolen data belonging to several hundred thousand people who posted resumes on Monster.com, a researcher said this weekend.

According to [Symantec Corp.](#) security analyst Amado Hidalgo, a new Trojan horse called [Infostealer.Monstres](#) by Symantec has stolen more than 1.6 million records belonging to several hundred thousand people from Monster Worldwide Inc.'s job search service. That data is then used to target the Monster.com users with credible phishing mail that plants more malware on their machines.

"We are investigating the reports related to this Trojan and will take any necessary steps indicated by that investigation," Monster.com spokesman Steve Sylven said Sunday in an e-mail.

The personal information filched from Monster.com includes names, e-mail addresses, home address, phone numbers and resume identification numbers, said Hidalgo, who traced the data to a remote server used by the attackers to store the stolen information. Infostealer.Monstres ripped off Monster.com by using legitimate log-ins, likely stolen from recruiters and human resource personnel who have access to the "Monster for employers" areas of the site. Once inside, the Trojan horse ran automated searches for resumes of candidates located in certain countries or working in certain fields. The results were then uploaded to the attackers' remote server.

"Such a large database of highly personal information is a spammer's dream," said Hidalgo. In fact, that's exactly what the attackers are using their newly-acquired data for.

"The attackers first gather e-mail address and other personal information from resumes posted to Monster.com with Infostealer.Monstres," Hidalgo said. "Next, they will try to infect the computers of those candidates by sending targeted Monster.com phishing mails which install [Banker.c or Gpcoder.e]."

The first piece of malware, dubbed Banker.c by Symantec, is a run-of-the-mill information-stealing Trojan horse that monitors the infected PC for log-ons to online banking accounts. When it sniffs a log-on in process, Banker.c records the username and password, then transmits the data back to hacker HQ. Gpcoder.e, on the other hand, is "ransomware," the name given

to Trojan horses that encrypt files on the hacked computer, then hold those files hostage until the user pays a fee to unlock the data.

Although both Banker.c and Gpcoder.e may be distributed in other ways -- [SecureWorks Inc.](#) last week said it had spotted something like the former coming from infected ads placed on job search sites -- Infostealer.Monstres' built-in mailing code and template lets it send messages posing as missives from Monster.com straight to the job-site users it finds in its automated searches.

Infostealer.Monstres' second-stage attack, which uses Gpcoder, is especially insidious. Realistic-looking e-mails that contain convincing personal information -- the very information stolen from Monster.com -- instruct the recipient to download a program called "Monster Job Seeker Tool." There is no tool, of course; victims download the ransomware Gpcoder.e instead.

Hidalgo's research led him to conclude that the three pieces of code -- Infostealer.Monstres, Banker.c, and Gpcoder.e -- are related, and probably the work of a single group.

"While their final purpose is different, their modus operandi is very similar, using identical file names, creating the same system folder, injecting code into the same processes and hooking the same system functions using root-kit techniques to gain control of network functionalities and to steal sensitive information," said Hidalgo. "They share code and a number of traits that could indicate they were developed by the same group or perhaps [created using a kit.](#)"

Monster.com's Sylvén defended the service's automated searches and said that although the company monitors database activity, stolen credentials have been used in the past to access the system. Moreover, he said, it's difficult to tell a valid automated search generated by a real person from one cranked out by software. "Many of our larger customers rely heavily on our database, and their use may be similar to programmatic or scripted access," said Sylvén.

He could not confirm that the stolen accounts had been disabled, although Hidalgo noted in a [blog entry posted Friday afternoon](#) that Symantec had notified Monster of the compromised log-ins. "When unusual access is detected, we do terminate that access and investigate if possible," Sylvén said.

## **Lawsuit filed on behalf of 8.5M consumers in data breach case**

Fidelity National, subsidiary accused of negligence, invasion of privacy  
**Jaikumar Vijay**

**August 20, 2007** ([Computerworld](#)) -- A California law firm has filed a class-action lawsuit against [Fidelity National Information Services](#) (FIS) and one of its subsidiaries over an incident involving the potential compromise of personal data belonging to 8.5 million consumers.

The lawsuit was filed last week in federal court for the Central District of California. It does not seek specific damages, but it accused FIS and Certegy Check Services, the subsidiary involved in the breach, of negligence, invasion of privacy and breach of implied contract.

The complaint, filed on behalf of 8.5 million consumers by the San Francisco-based law firm of Girard Gibbs LLP, charged both companies with failure to implement and maintain adequate security measures for protecting confidential financial information belonging to consumers. The suit also alleged that the companies failed to properly monitor and supervise the activities of employees entrusted with consumer data.

A spokesman for FIS and Certegy did not immediately respond to a call for comment.

Jacksonville Fla.-based FIS is a large transaction processor and outsourcing provider to the financial services sector. It is not affiliated with the better-known [Fidelity Investments](#). Certegy provides check verification services for many major retailers. The breach in question was disclosed by FIS in July and involved a Certegy [senior database administrator](#) who illegally accessed and downloaded millions of consumer records and sold them to data brokers.

Initially, FIS said about 2.3 million records may have been compromised by the database administrator's actions. However, in filings with the [U.S. Securities and Exchange Commission](#) about two weeks later, [FIS increased that number](#) to as many as 8.5 million records that may have been compromised.

According to the company, the data appeared to have been misappropriated purely for use in marketing purposes and not for identity theft or other types of fraud.

The case was initially brought by a Los Angeles-based resident, Theodore Borreson, "who, prior to the public announcement by Certegy and FIS of the data breach, started noticing an influx of direct marketing and promotional offers, as well as phone calls to his home," a statement announcing the suit from Girard Gibbs noted.

"Once the internal breach became known, it should have been communicated to the public in a timely and adequate manner," said Eric Gibbs, one of the attorneys at the law firm in the statement. "The failure by these companies to make the internal data breach immediately known exposed consumers to direct marketing campaigns and the risk of unauthorized use of their bank accounts and identity theft."

Legal experts have long been warning companies that they could become targets of such lawsuits in data breach incidents. Even so, few cases have been filed in data breach incidents and fewer still have been won by consumers. In the past, legal experts have said the plaintiffs in such cases usually have a hard time establishing and proving a direct link between a disclosed data breach and identity theft or other forms of fraud.

## **TJX Says Breach Costs May Exceed \$150 Million**

Analysts contend latest estimate by retailer is woefully low. By Jaikumar Vijayan

**August 20, 2007** ([Computerworld](#)) -- The TJX Companies Inc. last week reported that losses from a massive data breach it disclosed in January could surpass \$150 million, which analysts say makes the crime the costliest such incident to date.

The Framingham, Mass.-based discount retailer in March acknowledged that 45.6 million customer credit and debit card numbers were stolen from one of its systems over a period of more than 18 months.

"We have continued to learn more about the computer intrusion(s) and are now able to estimate the company's liability," said Carol Meyrowitz, president and CEO of TJX, in a statement.

Last week, TJX reported a charge of \$118 million in its second quarter, which ended July 28, to cover potential costs related to the breach. The company said it expects to incur additional noncash charges of \$21 million during its 2009 fiscal year.

The new charges are in addition to the \$25 million set aside in the previous two quarters to cover breach costs.

Meyrowitz noted that the company "over the past months [has] worked diligently to further strengthen the security of our computer systems."

Deven Bhatt, director of corporate security at Arlington, Va.-based Airlines Reporting Corp., said the rising costs of the TJX breach should help him convey the importance of heavy security investments to top management at his firm, which provides ticket distribution and settlement services to more than 145 air and rail carriers.

Bhatt said that while he was not surprised by TJX's projections of its breach-related costs, top executives at Airlines Reporting were amazed when he showed them TJX's Securities and Exchange Commission filings.

"They definitely were shocked," Bhatt said. "It definitely helps security guys like me to make a solid business case. It's a lot cheaper to protect than to do cleanup."

Avivah Litan, an analyst at Stamford, Conn.-based Gartner Inc., said the costs of the TJX breach are likely to increase significantly.

"They have incurred about a third to a half of the costs they could end up having to pay," Litan estimated. "They are facing potentially expensive litigation. There's never been anything this big in terms of the breach itself and its cost implications."

Litan predicted that the breach will ultimately cost TJX about \$500 million.

Lawsuits related to the breach have already been filed against TJX by the Massachusetts Bankers Association, the Arkansas Carpenters Pension Fund and the Merchant Law Group.

Several more states are actively contemplating lawsuits against the retailer, according to an analyst who is helping one state with such litigation.

Another analyst, Khalid Kark at Forrester Research Inc., also predicted that the total costs will far exceed the TJX estimate. "The first-year costs are significant. But we tend to underestimate the costs over time," especially from lawsuits, Kark said.

He said the final costs to TJX could approach \$1 billion.

Despite the charges, TJX reported strong second-quarter results, with sales increasing by 9% to \$4.3 billion.

Even so, the scope of the breach costs should convince companies that are "on the fence" to invest heavily on security fixes, Litan said.

"Strengthening data security," she said, "is much less expensive than responding to a security breach."

## **Mobile workers still struggling with security**

Many ignore security threats; end-user education urged

**Matt August 22, 2007** ([InfoWorld](#)) --

SAN FRANCISCO -- A fair amount of business users remain oblivious or unconcerned about many of the security issues involved with mobile devices, according to a new study published by [Cisco Systems Inc.](#) and the National Cyber Security Alliance.

While a greater number of business users are carrying laptop computers and handheld devices every year, a good number of them ignore security threats related to the machines or policies meant to protect them from attack or data loss, the report finds.

Cisco and the alliance cite IDC research that predicts roughly 70% of all workers in the U.S. will carry some sort of mobile device by 2009. Another piece of research cited in the report and published by [Korn/Ferry International](#) concludes that 81% of all business executives worldwide are already using mobile devices of some kind.

Based on those figures and their findings, the report's authors said that a great deal of end-user education is still needed to help people protect their mobile devices against potential attacks or data loss.

In the study, which was carried out via interviews with 700 businesspeople who use mobile devices in the U.S., the U.K., Germany, China, India, South Korea and Singapore, the researchers contend that the situation merits an increased focus by organizations to overcome the lack of awareness of potential security problems among users.

The interviews themselves were carried out by independent research firm InsightExpress LLC.

According to the report, 73% of those surveyed said they do not always consider security issues when using their mobile devices, and 28% admitted that they hardly ever give a thought to adhering to recommended procedures.

Asked why they didn't consider potential mobile security risks, most users said they were more focused on getting their work done as quickly as possible.

Logging on to unknown or untrusted sources of wireless Internet access remains one of the most significant issues, the researchers said, with roughly one-third of all respondents admitting that they have done so at times. Users in China were the most grievous offenders, with 54% of those users saying they've gone onto unknown wireless networks, followed by 46% of users in Germany and 44% of those in South Korea.

Many respondents said they couldn't initially tell when they were connecting to untrusted sources or only did so when their own networks weren't up and running, while others acknowledged that they simply wanted free access.

As with e-mail, the practice of opening messages or attachments from unverified sources remains a major problem in the mobile sector, according to the report. The mistake is amplified by the knowledge that most of today's mobile malware threats demand such user interaction to get onto devices in the first place.

### **Education is the key to security**

Some 44% of those surveyed said they have opened messages or attachments from unknown sources. Part of the problem is that 76% of those interviewed said they have a hard time differentiating such messages from legitimate content. The smaller screen size of handheld devices was cited as a primary contributor to the problem.

Experts said educating end users will play the most important role in correcting the ignorance of mobile security because the biggest problems are related to process rather than tangible threats at this point in time.

"While this study shows mobility provides businesses with new risks, so do other Internet services and new technologies," said Ron Teixeira, executive director of the National Cyber Security Alliance, in a report summary. "Mobility and the Internet can be used securely and safely if businesses institute a culture of security within their workforce by providing their employees with continuous cybersecurity awareness and education programs."

Among the tips offered to improve mobile worker behavior by the alliance -- a nonprofit organization dedicated to advancing public awareness of security and privacy issues -- are for users to adopt mobile device passwords, use antivirus programs, download any recommended security patches and back up all important content on their machines.

The group also advises users to encrypt sensitive data stored on mobile devices and recommends that businesses have response plans for handling wireless security incidents.

On a higher level, organizations should attempt to "marry" education with technological protections for both networks and devices, according to the report.

"What's key is knowing that the issues outlined in this study can be addressed," said Jeff Platon, vice president of security solutions at Cisco. "Technology is important in helping to resolve security issues for wireless mobile users, but education and communication are proactive measures IT can take to help address corporate security and generate greater [returns] on their investments."

"IT should be a strategic asset to the business, enabling business process transformation and unlocking the power of collaboration," said Platon. "As more workers become mobile, proactively educating them to practice good security behavior should be a key tenet of any business' approach to IT security and risk management."

**--Study: Mobile Workers Leave Security to IT** (August 21 & 23, 2007) A study commissioned jointly by Cisco Systems and the National Cyber Security Alliance found that most mobile wireless workers view security as "IT's job." Forty-four percent of respondents said they open email messages and attachments from unknown or suspicious senders and one-third use unauthorized wireless connections. While many of the 700 mobile workers surveyed said they are sometimes aware of security issues and best practices, more than a quarter said they "hardly ever" consider those issues. Those workers said that they were busy getting their work done and that security should be addressed by IT.

### **"Survey: Security Policies Neglect Off-Network Devices"** **Network World (08/22/07) ; Dubie, Denise**

Nearly 75 percent of corporations have experienced the loss or theft of a "data-bearing asset" within the past two years, according to a recent survey of 735 IT security practitioners that was conducted by Ponemon Institute and commissioned by Redemtech. The study also found that the overwhelming majority of these data breaches involved unprotected information stored on devices that go off the network for relocation, repair, or disposal. Sixty-eight percent of the data breaches involved laptop computers, while another 67 percent occurred on PDAs. Many companies also reported data breaches involving USB flash drives. According to the study, the frequency of security breaches involving off-network devices is due in part to a lack of policies that address how critical data stored on devices that could leave the network should be treated. The survey's respondents cited a number of reasons why their companies had not implemented such policies. Roughly 60 percent said they lacked the resources to implement proper policies and put controls on off-network devices. Eighty-nine percent of the survey's respondents said that off-network security activities represented no more than 10 percent of earmarked IT security spending--a funding level that the study called "inadequate."

## **Symantec: Bank account details fetch \$400 online**

### **And e-mail passwords can cost upwards of \$350**

Jeremy Kirk [Today's Top Stories](#) ▶ or [Other Security Stories](#) ▶

**September 17, 2007** (IDG News Service) -- Stolen bank account numbers are commanding the highest price in an underground trade of personal details stolen by hackers, according to a survey released Monday by security vendor [Symantec Corp.](#)

Bank account details command prices of up to \$400, while credit card details sell for between 50 cents and \$5, e-mail passwords from \$1 to \$350 each, and e-mail addresses from \$2 to \$4 per megabyte, according to Symantec's "Internet Security Threat Report," which covers the first half of the year.

The online trade in stolen data highlights the commercialization of Internet crime, with gangs researching, developing and marketing nefarious software for other criminals, said William Beer, director of Symantec's security practice for Europe.

There has been an increase in the quality and quantity of malicious code sold on the Internet, driven by well-funded international groups of criminals, Beer said.

The hackers are obtaining the information through increasingly targeted attacks on computers that often involve collecting personal information about a person from social networks such as [MySpace.com](#) or [Facebook](#), Beer said.

With specific personal details, a hacker can construct a personalized e-mail that entices the victim to either click on an attachment containing malicious software or visit a phishing site.

Symantec is also seeing multistage attacks where the attacker places a small piece of software on a target computer that then acts as a beachhead for downloading other software.

"The end user will not even notice the attacks have taken place because it's a very gradual process," Beer said.

On the spam front, Symantec said it has noticed a 30% drop in so-called pump-and-dump spam, in which e-mails touting penny stocks are sent out, causing a rise in the stock price before the perpetrators sell the stock early. The decline can be attributed to a crackdown by the [U.S. Securities and Exchange Commission](#).

Also down is the percentage of spam with images, which started as a highly effective way to bypass spam filters but is now less so. About 27% of the spam analyzed by Symantec between April and May contained images, down from 50% the first week in January, Symantec said.

The decrease is due to an improvement in spam filters as well as the decline in pump-and-dump spam, which often used images, the company said.

--**DoJ Mobile Workers May Not Use Own PCs or PDAs** (September 13, 2007) Due to concerns over data security, US Department of Justice employees are no longer permitted to use their own computers or PDAs to access agency email and files. Teleworkers must now use department-issued laptops, docking stations, or BlackBerries so the devices can be properly monitored and equipped with encryption.

<http://www.fcw.com/article103746-09-13-07-Web&printLayout>

--**Calif. Breach Liability Bill Awaits Gov's Signature** (September 12, 2007) All that now stands between Californians and a new data breach law is the governor's signature. AB 779, known as the Consumer Data Protection Act, would make retailers responsible for the costs incurred by banks and credit unions that have to notify consumers and issue new cards as a result of a data security breach. Breached entities would also have to be forthcoming with information about the types of data exposed and would also have to refrain from storing certain types of financial transaction data. Retailers who suffer a breach but have proof that they had followed certain security guidelines would be exempt from the law.

Governor Schwarzenegger is expected to sign the bill. Privacy legislation in California has been known to have a "ripple effect"

across the rest of the country.

<http://www.scmagazineus.com/California-a-signature-away-from-passing-consumer-protection-data-breach-law/article/35643/>

