

# Security Trends Report

03/08

## *Still Insecure After All These Years*

---

Posted by Carl Weinschenk on February 5, 2008 at 6:00 pm

In a bit of cognitive dissonance, it seems that laziness is as much a mobile security problem as ever. It doesn't seem like this should be so, but it is. In a perverse way, security forces and corporate lawyers should be happy: They apparently always will have jobs cleaning up after messy corporate incidents and accidents.

[Cisco this week released a 10-country survey on attitudes to mobile security.](#) The results, here reported in **The Register**, are disheartening in their suggestion that workers' security habits are regressing due to a widespread feeling that the Internet has become more secure and therefore they need not be as vigilant as before.

The wide-ranging survey dealt in part with behavior toward wireless. Workers are increasingly willing to hijack the services of others. A year ago, 6 percent said they would engage in this dangerous practice. The number is 11 percent now. The reasons for doing so include an immediate need that for some reason required jumping on neighbors' networks, convenience and not being able to determine to whom the network belonged. Ironically, the most honest group said they do so because they can get away with it.

The idea that security is getting worse is the key takeaway of this AirDefense study. [The company assessed wireless security at the National Retail Federation Convention & Expo](#) earlier this year in New York City. These results [and other recent news items](#) show that all of the screaming that security mavens have done during the past year has been a waste of breath. Fewer than 10 percent of the access points (APs) surveyed used Wi-Fi Protected Access version 2 (WPA2), currently the top security measure. Eighty percent of devices in the hall were liable to evil twin attacks, while 60 percent used the wired equivalency protocol (WEP), a defense that is about as good as that of the New York Knicks (not very good).

This is not an academic exercise, either: The firm found that people in the hall were using hacking tools and detected 39 attacks.

As always, there are good stories out there detailing how to secure networks — whether or not anybody really is listening. For instance, [Wi-Fi Planet goes a shade deeper](#) than most pieces in explaining the problems. It also does a good job of describing how organizations can secure the data remote workers insist on throwing around so freely.

Many of the ideas are familiar to security forces. One particularly clever idea involves what could be described as a sort of positive social engineering: An organization should contract with a known hotspot provider. This service, then, would involve no out-of-pocket expense for remote workers. But the traveler would have to pay to use other providers and "T&E it" later. It is a virtual certainty that this would cut down on the use of unauthorized hot spots.

[There isn't anything in this Wall Street Journal piece](#) that security forces don't already know. But it is nice to see the issue getting coverage in such a high-profile publication. The piece provides a good overview of the problem and discusses tools available from T-Mobile and AT&T to protect its subscribers. It also makes the important point that the problem is, if anything, worse than reported because companies try to hide the fact that they lost data.

The usual list of steps is outlined: Make sure computing device security is up to date; use a virtual private network (VPN); change the name of the service set identifier (SSID); turn off Wi-Fi capabilities when they are not needed; be sure that the Wi-Fi network being used is legit; and forgo banking over Wi-Fi links.

## Hackers camouflage 100% of Web attacks, IBM researcher says

### JavaScript the prime culprit, says researcher

**By Gregg Keizer**

February 12, 2008 (Computerworld) Hackers now mask virtually every Web browser exploit as part of their normal procedure to evade detection by security software, said [IBM's](#) X-Force research team today.

By the end of last year, according to Kris Lamb, director of IBM Internet Security Systems' X-Force, nearly 100% of all Web exploits were either self-encrypted or relied on obfuscation techniques to make it difficult for standard intrusion detection and intrusion prevention technologies to identify the attack code.

"In 2006, we saw about 50% of Web exploits obfuscated or encoded," said Lamb, adding that, on average, 80% were camouflaged throughout 2007. "But that jumped to almost 100% by the end of the year."

The reason for the cover-up boost is straightforward, said Lamb. "They're not dumb. They only do what they're forced to do," he explained. "For them to continue to get a high rate of return, they had to understand the protection technologies that were being used. And [security] vendors were doing a pretty good job.

"A lot of network security technologies were doing a good job in 2006, when they shifted from e-mail to Web browser as an [exploit] entry point. Vendors have been keeping up with that trend and building new types of [security] technologies to keep up with technologies extending the browser, like Flash and JavaScript," Lamb continued.

That pressured attackers into hiding more of their browser exploits, and doing a better job of concealing their work -- largely by focusing on JavaScript. "More than any other technology, JavaScript is used to obfuscate and self-encrypt," Lamb said.

JavaScript is ubiquitous -- it is cross-platform and cross-browser -- and its inherent complexity lends it perfectly to hacker use, argued Lamb. "Attackers can do very advantageous things, like encode it so when it goes over the wire, all the recipient sees is a data blob," he noted.

And getting rid of JavaScript is not an option for most users. "Even I'd be hard-pressed to disable JavaScript entirely," acknowledged Lamb. "So much of my experience and my productivity experience depends on JavaScript, or another scripting language, like VBScript or Adobescript."

This year, he predicted, the camouflaging will continue, with hackers increasingly adding secondary scripting languages to their obfuscation and encryption portfolios. "They'll start using other browsing scripting frameworks more -- more vendor-tied scripts, like Adobescript," Lamb said. Also known as JavaScript for Acrobat, Adobescript allows customizing of PDF files using scripting.

Hackers have already put Adobescript to work -- very recently, in fact. Yesterday, [McAfee Inc.](#)'s Vinoo Thomas was one of several researchers who noted that [attacks are under way](#) that use at least one of the still-unnumbered vulnerabilities in [Adobe](#) Reader disclosed last week. Thomas, however, pegged the exploit to Adobe JavaScript.

"The current vulnerability can be embedded in a PDF file and manipulated through Adobe JavaScript," he said in a [warning posted](#) to the Avert Labs' blog on Monday.

The masking and encryption, however, is just one facet of the ongoing trend toward attacks aimed first and foremost at browsers, said Lamb. "Whether through drive-by downloads or compromising legitimate sites, or a combination of advanced, targeted phishing, the browser is involved in some way," he said. "It's the main frontier of exploit right now.

"We used to call the operating system the 'keys of the castle,' but as exploits moved up the application stack and as the browser became the new OS, it's now the keys to castle," he added.

## Groups call for passage of health IT legislation

There's fear that companies will develop systems that don't interoperate

### By Grant Gross

February 12, 2008 (IDG News Service) WASHINGTON -- Congress needs to pass health care IT legislation before private companies develop multiple systems that don't talk to one another, two advocacy groups said today.

Members of the Health IT Now coalition and the Information Technology Industry Council (ITI) urged Congress to move ahead with health IT legislation such as the Promoting Health Information Technology Act ([PDF format](#)). The bill would establish a public/private group to recommend health IT standards and certification, and it would budget \$163 million annually for health care providers to adopt health IT products such as electronic health records.

Health technologies can help improve health care quality, reduce costs and encourage changes in treatment, said former U.S. Rep. Nancy Johnson, co-chairwoman of Health IT Now.

Health IT is "going to produce radical change," Johnson said at a press conference. "It's going to radically improve the quality of health care that Americans receive."

With health care costs climbing, a move to an electronic system that reduces paper and medical errors is the best hope to extend health care to U.S. residents who are uninsured, she added. "It is the only way that we guarantee to Americans of every age that our health care system will continue to deliver the state-of-the-art medicine for which it has been known worldwide," Johnson said.

The Promoting Health Information Technology Act has stalled in the House of Representatives, and a similar piece of legislation, the Wired for Health Care Quality Act, has stalled in the Senate.

Some groups, including the Patient Privacy Rights Foundation, have raised concerns that the legislation doesn't adequately address privacy issues. "The Senate Wired Act has no privacy protections or language ensuring patient control of health records," the group said on its Web site. "It must not pass unless patients have the right to keep their health records private."

Privacy and security must be major components of a health IT bill, Johnson said. But she and [Rhett Dawson](#), ITI's president and CEO, said that Congress should pass a health IT bill before vendors develop multiple systems that don't interoperate. "The public interest is in interoperability," Johnson said.

A health IT bill would be a major accomplishment that lawmakers could show to voters before the November elections, Dawson said. "We believe the time to act is now," he added.

## Lockheed wins 10-year FBI biometric contract

Irises, faces, and more -- it all goes into the pot

### By Grant Gross

February 13, 2008 (IDG News Service) The [Federal Bureau of Investigation](#) has awarded [Lockheed Martin](#) a \$1 billion contract to build a next-generation biometrics-based identification system.

The biometric collection system and database, which has raised concerns of privacy groups, would include imaging of irises, faces and other identifying characteristics, the FBI said in a news release late Tuesday. Lockheed Martin will design, develop, test and deploy the Next Generation Identification System over the 10-year life of the contract.

The new system will expand on the FBI Criminal Justice Information Services Division's Integrated Automated Fingerprint Identification System (IAFIS), primarily a fingerprint-based identification system operated in Clarksburg, West Virginia, the FBI said.

"IAFIS has been a fantastic tool in support of criminal justice and the war on terror," Thomas E. Bush III, assistant director of the FBI's CJIS Division, said in a statement. "[The new system] will give us bigger, better, faster capabilities and lead us into the future."

The [American Civil Liberties Union](#) has raised concerns about the biometric database, saying it's part of the U.S. government's efforts to collect more and more information about residents.

The new system will expand fingerprint capacity, doubling the size of the FBI's current database, and will also include palm prints, iris and facial recognition, Lockheed Martin said in a news release. The system will be designed to be flexible enough to accommodate future biometric technologies, the company said.

Among the companies working with Lockheed Martin on the contract will be Accenture and BAE Systems Information Technology.

Lockheed Martin will provide program management and oversight as well as development of biometric and large systems, the company said. Accenture's responsibilities will include interoperability and change management. BAE will work on external interface requirements engineering and security design.

The FBI contract was awarded through an open bidding process. [Northrop Grumman](#) and [IBM](#) also bid on the contract.

## Time to Take Information Classification Seriously

Feb 12, 2008 |

Recent high profile data losses have highlighted the need for better information classification along with the implementation of data protection measures based on the level of...

...sensitivity and confidentiality, according to the Information Security Forum (ISF).

In its latest report, the ISF suggests that because many existing approaches to information classification are overly complex they rarely deliver business benefits, and are often simply ignored.

"Traditional information classification is characterized by the 'Top Secret' rubber stamp in James Bond films," says Nick Frost, the report's author and a senior research consultant at the ISF. "Today, information exists in many different forms, from paper documents and verbal communications to the masses of electronic data stored, transmitted and processed. While introducing an effective enterprise-wide scheme is daunting, organizations can no longer afford to ignore its importance if further embarrassing data losses are to be avoided."

Information classification requires a consistent process to determine: the level of confidentiality of a piece of information; the development of techniques for communicating the level of classification; and the practical implementation of measures to protect information accordingly.

But according to the ISF report the benefits of successful information classification are considerable. By ensuring that information is adequately protected, good information classification helps to prevent over- or under-engineering of controls,

so reducing potential operational overspend and unnecessary drains on resources. Information classification can also help to enforce better access control policies and can be used to demonstrate compliance with legislation such as Data Protection and Privacy along with regulations including HIPAA and Gramm-Leach Bliley.

The report highlights that achieving these levels of success requires participation across an organization from HR and Legal to IT and Audit, along with Board-level support. "Having senior managers with a shared strategic vision and understanding of information classification and the value it can deliver is critical to overcome budgetary and organizational issues," says Frost: "It is also vital to run a successful pilot project to show a 'quick win' to demonstrate the benefits."

## **"Workplace Autopilot Threatens Security Risk Perception"** **University of Leeds (02/08/08)**

Human psychology and the way we perceive risk make it impossible for organizations to completely secure their data, no matter what preventative steps they take, concludes research conducted by Britain's Leeds University Business School. During the study, people who regularly used IT systems at work were asked to list examples of possible data security risks, either imaginative or ones they have seen in their personal experiences. Another group was asked to comment on the probability, underlying causes, likely consequences, and impacts of the scenarios that were most commonly listed. The study found that many of the risk examples listed by the participants matched recent security breaches, despite the fact that the survey data was collected over a two-year period. Professor Gerard Hodgkinson, director of the Center for Organizational Strategy, Learning, and Change, says the research shows that organizations will never be able to remove all of the latent risks in the protection and security of data stored on IT systems because people's brains naturally run on "automatic pilot" in routine situations. Dr. Robert Coles, the study's co-author, says the results of the study show that employees exhibit a highly-sophisticated perception and categorization of risk, as well as insight into the consequences of risk scenarios, when asked to focus on potential problems. But since this perception is not always translated into practice, errors are still happening and will continue to happen in the future, Coles says.

## **"Human Error Tops the List of Security Threats"** **CIO (02/05/08) ; Daniel, Diann**

Most companies cite human error as their prime security concern, reveals a Deloitte survey. Human error was ranked by 75 percent of media, technology, and telecommunications businesses surveyed as the culprit for security vulnerabilities. Over 90 percent attributed on-the-job misconduct as another factor hampering security controls, while about one-third credited third parties with security failures. The survey also found that management executives are not usually notified about security issues and most companies still designate their IT sectors with being accountable for protecting information security. Almost half of the respondents stated that flawed operations and technology weakened overall security. "A prerequisite for effective information security is the implementation of a proactive information security strategy that is closely linked to the company's overall business strategy, business requirements, and key business drivers," says Deloitte's Rena Mears. Deloitte advises companies to incorporate security initiatives into their overall business plans and that continual security training and evaluation should be implemented.

## **White House Wary of Proposed Changes to FISMA**

February 14, 2008 - The White House is questioning the need for many changes to the Federal Information Security Management Act (FISMA) described in the Federal Agency Data Protection Act. One section would require US government agencies to inform Congress about the methods they are using to protect their systems from the risks of peer-to-peer file sharing programs. The objection to this element stems largely from a reluctance to focus on a specific technology in outlining security requirements. The proposed legislation "would [also] require agencies to develop policies and plans to identify and protect personal information and to develop requirements for reporting data breaches." Office of Management and Budget (OMB) administrator for e-government and information technology Karen Evans is resistant to some of the proposals because they could "seriously impact established security and privacy practices while not necessarily achieving the

outcomes of improved privacy and security." The bill's sponsor, Representative William Clay (D-Mo.) maintains that it "would move us toward more rigid security requirements while staying within the FISMA framework."

## Privacy group sounds alarms over personal health records systems

Medical data stored online may fall outside of HIPAA's privacy protections, report claims

By Jaikumar Vijayan

---

February 20, 2008 (Computerworld) In some cases, people whose health care information is stored in online personal health records (PHR) systems may be exposed to serious data privacy risks, according to a warning issued by a privacy advocacy group.

That's because not all PHR systems are covered by the federal Health Insurance Portability and Accountability Act, the World Privacy Forum said in a 16-page report released today ([download PDF](#)). The [WPF](#) contended that as a result, many of the privacy protections offered under the HIPAA statute don't apply to the personal health care data being maintained in such systems.

PHR systems typically store medical records gathered from a variety of sources, including health care providers, insurers and patients themselves. The information is made accessible via the Web to individuals and to others who they have authorized to view the data. "As a new type of convenience technology for consumers, PHRs are promoted as giving consumers more knowledge and an opportunity to be more actively engaged in their own health care," the San Diego-based WPF noted in its report.

But people need to be aware that the systems may fall outside of HIPAA's protective umbrella, said [Pam Dixon](#), the group's executive director. The HIPAA privacy rules cover health plans, doctors, hospitals, clinics, nursing homes and even researchers working with medical data collected from those entities, she said. But commercial PHR systems maintained by IT vendors or services providers and supported by means such as advertising may not come under HIPAA's purview, according to Dixon.

And even in cases in which a PHR system is covered by HIPAA, there are circumstances under which an individual's medical records may not be protected, Dixon said. For instance, she pointed to medical information that a person puts into the PHR system on his or her own behalf.

There are several problems that could result from the lack of privacy protections, Dixon said. For starters, she claimed, health records could lose their privileged status if a patient authorizes a doctor to send a copy of the information to a PHR system that isn't covered by the HIPAA mandates.

"Many consumers have this deeply held belief that their health information, no matter where it travels, is protected in the same way as when you have a doctor/patient relationship," Dixon said. In reality, consenting to have data transmitted to a noncovered system likely would be viewed as an indication that you had waived your privacy privilege, she added.

Health information stored in commercial PHR systems is also less protected against subpoenas than it otherwise would be, Dixon asserted. Under HIPAA, if someone seeks to subpoena medical records about an individual from a covered entity, the patient has to be informed first. But that protection doesn't apply to PHRs in all instances, she said.

"If a lawyer has a choice between subpoenaing a record from a physician or from a PHR vendor, the lawyer may find it easier to go to the PHR vendor," the WPF noted in its report. "Notice for the subpoena is not a legal requirement for non-HIPAA covered PHRs, and the lawyer seeking the record does not have to worry that the physician will claim privilege or otherwise resist the subpoena."

Even more worrisome to Dixon, though, is the potential for protected medical information stored in PHRs to be used for marketing purposes. HIPAA explicitly prohibits such uses, but the terms under which many PHR systems are operated could enable their owners to sell personal health data to marketers, she said.

People should be aware of such issues when choosing whether to use PHR systems, Dixon said. She added that the operators of PHR systems should be required to clearly disclose whether they are covered under HIPAA and what sort of privacy protections they offer.

The WPF's report raises some important, if long-standing, issues, said Peter MacKoul, president of HIPAA Solutions LC, a Sugar Land, Texas-based firm that offers a set of tools and services to help companies comply with HIPAA. "We see some serious privacy violations" within PHR environments, MacKoul said.

But he added that a bill proposed in the [U.S. Senate](#) last summer by [Sen. Patrick Leahy \(D-Vt.\)](#) should address the issues cited by the WPF if it is passed by Congress and signed into law. The bill, called the Health Information Privacy and Security Act and referred to by the number [S.1814](#), would provide individuals with access to their health records and ensure personal privacy with respect to that information, MacKoul said. One of the bill's provisions, he noted, touches on the issue of health-information data brokers and their privacy responsibilities.

The bill was referred to the Senate Committee on Health, Education, Labor and Pensions after it was introduced by Leahy. No further action has been taken thus far, according to information posted on the Senate's Web site.

## "The Web Is Less Risky Than Phone or Mail for Identity Theft, Survey Finds"

**Internet Retailer (02/14/08)**

Consumers are at greater risk of having their personal and financial information stolen via traditional communications channels than they are over the Internet, reveals Javelin Strategy and Research's 2008 Identity Fraud survey. The survey found that just 14 percent of the cases of identity fraud that were reported by victims could be traced back to the Internet. Meanwhile, physical methods and venues made up 75 percent of the known sources of identity theft. Lost or stolen wallets, checkbooks, or credit cards represented a third of the known sources of identity theft, while thefts involving in-store, mail, or telephone transactions represented 23 percent of the known sources of identity theft. The survey also found that the number of cases of identity theft involving information that was fraudulently obtained in a mail or telephone purchase increased, while the number of identity theft cases involving information obtained in an online purchase declined. The report attributed the drop in the theft of personal information online to the fact that payment service providers have been working to increase the security of online transactions.

## "Most Mobile Users Don't Know If They Have Security"

**InternetNews.com (02/13/08) ; Needle, David**

More than three quarters of mobile users have no security software on their devices, reveals a McAfee-sponsored survey. Although mobile devices have been less likely targets of malware and spam attacks, there is no current software that supports smart phones and similar devices. Sixty percent of respondents say they relied on mobile operators to protect their devices, a factor corroborated with the lack of user flexibility allowed on mobile devices for loading antivirus applications. Web 2.0 technology is among the platforms that pose a greater threat to mobile security, McAfee says. The security vendor also notes that most mobile devices lack filters for unsolicited messages or phishing attempts. McAfee's Victor Kouznetsov says mobile security has focused on handset and network security, but the popularity of Web 2.0 creates the need for mobile content certification and application assurance. "We are witnessing the evolution of an entirely new wireless experience, where applications are no longer tied to specific devices and networks and mobile users are able to reap many of the rewards they already enjoy on the Internet," Kouznetsov says.

## Losses From Cyber Intrusions at US Banks Rise Significantly

February 20, 2008 - According to an anonymously obtained copy of a non-public Federal Deposit Insurance Corporation (FDIC) quarterly Technology Incident Report, financial institutions in the US experienced a considerable increase in the number of intrusions leading to account hijackings and stolen money over the last year. The report indicates that the cost of these breaches is increasing for all involved - banks, businesses, and consumers. The report looks into suspicious activity reports, or SARs.

Banks are required to report fraudulent and suspicious transactions of US \$5,000 or more. The report says that the average cost per SAR in the second quarter of 2007 was US \$29,630; the average cost per SAR in the same period a year earlier was US \$10,536. The majority of SARs were classified as "unknown unauthorized access - online banking." The report suggests that Trojan horse programs and keystroke loggers are used in many instances of unauthorized access.

[http://blog.washingtonpost.com/securityfix/2008/02/banks\\_losses\\_from\\_computer\\_int.html](http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html)

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=206801184>

[Editor's Note (Pescatore): That report does point out that the number of suspicious activity reports that are computer intrusion-related are still less than 2% of those due to mortgage and check fraud, but the widespread prevalence of compromised PCs is causing the computer related incidents to be fast growing.

(Paller): While the overall pattern of increase may be correct, several banks have experienced significant decreases in losses from money taken stolen from customer accounts through theft of customer credentials (via phishing or keystroke loggers, primarily). These banks set up a series of increasingly difficult challenges to transactions based on the transaction's score on (at least) three variables: (1) whether the transaction is done regularly, (2) whether the IP address is the one usually used,

and (3) how large the transaction is. Customers doing their regular banking from home are not impacted because they don't trigger the defenses. Defense in depth; simple and effective.]

## Workers Often Peek at Customer Data

(25 February 2008)

Documents made public in a lawsuit indicate that employees throughout Wisconsin utility company WE Energies were accessing data about friends, family members, politicians, and others. Several years ago, a WE Energies employee leaked information about a mayoral candidate.

Following that incident, the company began paying closer attention to which accounts its employees were accessing; 17 people were fired between 2005 and 2007. Federal agencies are struggling with similar problems.

<http://ap.google.com/article/ALeqM5ghPenZUJTE7BfSfgQbj6RX597DEAD8V019TGO>

<http://www.securityfocus.com/brief/687>

## Information Security: Protecting Personally Identifiable Information

GAO-08-343 January 25, 2008

[Highlights Page \(PDF\)](#) [Full Report \(PDF, 29 pages\)](#) [Accessible Text](#)

The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. As shown in prior GAO reports, compromises to such information and long-standing weaknesses in federal information security raise important questions about what steps federal agencies should take to prevent them. As the federal government obtains and processes information about individuals in increasingly diverse ways, properly protecting this information and respecting the privacy rights of individuals will remain critically important. GAO was requested to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' progress in developing policies and documented procedures that respond to recent guidance from the Office of Management and Budget (OMB) to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. To do so, GAO reviewed relevant laws and guidance, surveyed officials at 24 major federal agencies, and examined and analyzed agency documents, including policies, procedures, and plans. In commenting on a draft of this report, OMB stated that it generally agreed with the report's contents.

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agencywide programs to provide security for their information and information systems (which include personally identifiable information and the systems on which it resides). The act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas, including minimum information security requirements for information and information systems. In the wake of recent incidents of security breaches involving personal data, OMB issued guidance in 2006 and 2007 reiterating agency responsibilities under these laws and technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices and follow NIST security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter. Not all agencies had developed the range of policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. Of 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the 24 agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts from databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Gaps in their policies and procedures reduced agencies' ability to protect personally identifiable information

from improper disclosure. At the conclusion of GAO's review, OMB announced in November 2007 that agencies that did not complete certain privacy and security requirements, including those just described, received a downgrade in their scores for progress in electronic government initiatives. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area and GAO's previous recommendations on improving agency information security and implementation of FISMA requirements, GAO is making no further recommendations at this time.

## **"Data Protection in a Snap"**

**Information Security (02/08) Vol. 11, No. 1, P. 44**

Data protection is today's overriding issue, says consultant John Moynihan, formerly deputy commissioner and internal control officer at the Massachusetts Department of Revenue (MDOR). MDOR's data security strategy includes laptop encryption, secure email, background checks on vendors, ongoing training, and a homegrown database monitoring program designed to monitor compliance with its access policy. Roughly 68 percent of Information Security magazine readers say they will spend more time on protecting the data that is in their possession, according to a recent survey. The majority of these organizations--66 percent--say they would work to protect data by securing their databases. Meanwhile, about 31 percent of Information Security readers say they would evaluate database encryption tools. Software-based encryption is the choice of almost 30 percent of readers, while around 29 percent say they preferred hardware-based encryption. Forrester Research analyst Paul Stamp notes that encryption will help companies meet several goals, including complying with mandates such as the Payment Card Industry Data Security Standard and preventing employees from accessing data that they should not have access to. Finally, the survey finds that 35 percent of companies will look into data leak prevention products in order to prevent employees from accidentally leaking or stealing data via email or copying it onto a removable storage device.

## **"Feds Wrestle With Security Threats"**

**Dark Reading (02/20/08) ; Wilson, Tim**

Federal officials are warning enterprises and individuals about the progressively sophisticated tactics of hackers. Cybercriminals have relied on phishing attacks for impersonating IRS officials, while others have deployed sleeker strategies such as keyloggers for accessing users' financial information. Phishing attacks have also been a common exploit, prompting users to disclose sensitive information over the phone. Jerry Dixon, Team Cymru director of analysis and former executive director of the National Cyber Security Division and the US-CERT, says many users mistakenly believe that antivirus tools preclude them from being victims of malware attacks. A Team Cymru study found that less than 40 percent of 1,000-plus pieces of malware were detected by 32 selected antivirus programs. Team Cymru notes that botnets are on the rise, with more hackers using P2P and encryption to circumvent security filters. The IRS is monitoring the P2P attacks, though officials predict keyloggers will be the preferred exploit for the future. A majority of cyberattacks have been tracked to eastern European origins, though many of these attempted security attacks have been unsuccessful.

## **"Sniffing Out Insider Threats"**

**EurekAlert (02/19/08) ; Ang, Albert**

Researchers at the Air Force Institute of Technology at Wright Patterson Air Force Base are developing technology that could help find insider threats by analyzing email activity, helping identify malicious individuals hidden within groups of tens of thousands of employees. The technology uses data-mining techniques to search email and build a picture of social network interactions. The technology could be used to prevent security breaches, sabotage, and even terrorist activity that otherwise could have damaging results, says researcher Gilbert Peterson. The same technology can also find individuals who feel alienated within an organization or identify any worrying changes in an individual's social behavior. Peterson says security efforts have tended to focus on external electronic threats, and points out that insiders pose the greatest threat to an organization. Peterson's defense against insider threats is based on an extended version of Probabilistic Latent Semantic Indexing, which can discern employees' interests from email and create a social network graph showing their various interactions. The research is reported in the International Journal of Security and Networks.

## **Over 50% of companies have fired workers for e-mail, Net abuse**

Most employees knew they were being monitored

By Nancy Gohring

February 28, 2008 (IDG News Service) Think you can get away with using e-mail and the Internet in violation of company policy? Think again.

A new survey found that more than a quarter of employers have fired workers for misusing e-mail and one third have fired workers for misusing the Internet on the job. The study, conducted by the [American Management Association](#) (AMA) and The ePolicy Institute, surveyed 304 U.S. companies of all sizes.

The vast majority of bosses who fired workers for Internet misuse -- 84 percent -- said the employee was accessing porn or other inappropriate content. While looking at inappropriate content is an obvious no-no on company time, simply surfing the Web led to a surprising number of firings. As many as 34 percent of managers in the study said they let go of workers for excessive personal use of the Internet, according to the survey.

Among managers who fired workers for e-mail misuse, 64 percent did so because the employee violated company policy and 62 percent said the workers' e-mail contained inappropriate or offensive language. More than a quarter of bosses said they fired workers for excessive personal use of e-mail and 22 percent said their workers were fired for breaching confidentiality rules in e-mail.

Companies are worried about the inappropriate use of the Internet, and so 66 percent of those in the study said they monitor Internet connections. As many as 65 percent of them use software to block inappropriate Web sites. Eighteen percent of the companies block URLs to prevent workers from visiting external blogs.

Companies use different methods to monitor workers' computers, with 45 percent of those participating in the survey tracking content, keystrokes and time spent at the keyboard. An additional 43 percent store and review computer files. Twelve percent monitor blogs to track content about the company and 10 percent monitor social-networking sites.

Companies are keen to track employee e-mail and Internet behavior in part due to legal fears. According to research done by the AMA and ePolicy in 2006, 24 percent of companies in the study had e-mail subpoenaed by courts and another 15 percent have faced lawsuits based on employee e-mails.

The researchers found that even though only two states require companies to notify their workers that they're monitoring them, most tell employees of their monitoring activities. Of the companies that monitor workers in the survey, 83 percent said they tell employees that they are monitoring content, keystrokes and time spent at the keyboard. As many as 84 percent tell employees that they review computer activity and 71 percent alert workers that they monitor their e-mails.

## Google Health Privacy Concerns

(February 27 & 28, 2008)

The emergence of personal health record management services has raised privacy concerns. Google is piloting one such product - Google Health - with the Cleveland Clinic. While the online dossiers offer the convenience of being able to merge health data, they are controlled by consumers, not physicians, and are therefore not protected by the Health Insurance Portability and Accountability Act (HIPAA). Although Google and other entities developing similar products maintain they will offer even more stringent protections than HIPAA's, "the very existence of a detailed health dossier accessible in an instant can make control difficult."

<http://www.washingtonpost.com/wp-dyn/content/article/2008/02/26/AR2008022602993.html>

[http://www.usatoday.com/tech/webguide/2008-02-28-google-health\\_N.htm?csp=34](http://www.usatoday.com/tech/webguide/2008-02-28-google-health_N.htm?csp=34)

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=206900841>

[Editor's Note (Schultz): The issue described in this news item introduces a new dimension to data security protection woes. Count on the fact that if users are in the loop, security risk will skyrocket.

(Pescatore): It is not a given that there will be huge demand from consumers for these personal health records, as the financial information aggregation services that are the finance record equivalent of this really didn't explode. However, it is inevitable that some consumers will want to aggregate and control their own medical information to have some increased level of control of their medical care and some increased leverage in reducing costs through competition and second opinions and the like. The real key issues here are (1) making sure that all such services have external security audits and (2) \*most importantly\* that they be required to make any and all third party use of consumer health be purely opt-in with full audit and accountability. It is one thing for the Googles and the Microsofts or others to make some money by selling advertising around medical record access; it's a whole different issue to be able to resell medical-related information, even if it is only at the aggregate or metadata level.]

## The Best Way to Prevent Identity Theft? Hold on to Your Wallet

### Most identity frauds are traced back to low-tech methods, not the Internet, according to new research from Javelin

By Katherine Walsh

Most identity thieves still obtain the information they use to commit fraud through traditional, low-tech methods, not from the Internet, according to a new study from Javelin Strategy & Research.

The Javelin study--funded by CheckFree, a financial e-commerce service provider, now part of Fiserv, Visa and Wells Fargo--was done in October 2007 through telephone interviews with 5,000 consumers about their "day-to-day financial behaviors." Of respondents who had been the victim of identity fraud, 35 percent said they knew how their data was taken.

Of those respondents, only 12 percent said online channels, including phishing, hacking and spyware, were used by the perpetrators, and 7 percent traced the fraud back to a data breach. The majority of known cases still occur through traditional methods. A theft method is considered "traditional" if the criminal makes direct contact with the consumer's personal identification. This includes lost or stolen wallets, credit cards, checkbooks, and shoulder surfing (when a thief looks over the victim's shoulder at an ATM machine, in order to obtain PIN information).

The breakdown:

Traditional methods (79 percent):

- \* Lost or stolen wallets: 33 percent
- \* While conducting a transaction: 23 percent
- \* "Friendly" theft (perpetrators are friends or family members): 17 percent
- \* Stolen paper mail: 6 percent

Other methods (21 percent):

- \* Online (including phishing, hacking and spyware): 12 percent
- \* Data breach: 7 percent
- \* Other: 2 percent

### "Identity Management Critical for Security, Government IT Shops Say"

Network World (03/03/08) ; Fontana, John

Identity management plays a major role in the network security efforts of most government IT organizations, concludes a recent Pursuant survey, and will continue to do so over the next five years. The survey's respondents, 474 IT professionals from all levels of government, say they believe it is important for identity management to have a large role in network security efforts because data breaches could have disastrous consequences. Among the consequences cited by respondents are the loss of personal privacy and data security, compromised critical public infrastructure, deflated national security, and increased financial terrorism. Respondents also say they are concerned about how they would fund their expensive identity-management projects. The survey found that almost 31 percent of respondents say they had not reached their objectives because of a lack of funding. However, nearly 56 percent say their organizations are deploying an identity-management system despite the lack of funding. But 37 percent say they are not sure when their organizations would be compliant with government mandates, and 32 percent say it would take anywhere from one to five years for their organization to come into compliance.

### "Contractor Networks Create Security Risk, Defense Official Says"

GovExec.com (03/04/08) ; Aitoro, Jill R.

In his remarks during a panel discussion at the recent Information Processing Interagency Conference in Orlando, Defense Department CIO John Grimes said the federal government's use of information technology contractors creates a major security risk because the contractors fail to properly lock down their networks. In addition, smaller contractors present a security risk because they are typically not as accustomed to dealing with sensitive or classified information moving through their networks as large systems integrators are. To address these issues, the Defense Department is working with large contractors to educate them and develop standards to ensure that they follow proper security protocols. DOD is planning to do the same with network and IP providers at some point in the future. However, globalization, mergers and acquisitions of IT firms by foreign companies, and the offshoring of sensitive processes, will still make it difficult to protect intellectual property, Grimes said.

## "7 Rules Employees Love to Break"

CSO Magazine (02/08) Vol. 7, No. 1, P. 16 ; Walsh, Katherine

Firms are either not establishing, or workers are not obeying, information security protocols in numerous high-risk areas, concludes a recent Ponemon Institute report. For the report, "Data Securities Policies Compliance and Enforcement," Ponemon surveyed 893 business information-technology staff, studied the risks related to storing and moving sensitive data, and examined how well corporations are installing and upholding rules to protect against this threat. The seven areas where workers are violating the most protocols include copying confidential data onto a USB memory stick, with 87 percent of those surveyed thinking their firm's rules prohibit it, but 51 percent admitting they do it. Using Web-based email accounts at workplace computers also made the list, with 45 percent of those surveyed utilizing Web mail in the workplace, and 74 percent claiming there is no written company policy stating they cannot do it. Thirty-nine percent of those surveyed say they have lost or misplaced a portable information-bearing gadget, and 72 percent of them did not report the lost item right away. Workers are also guilty of downloading personal software onto a corporate computer, with 60 percent of respondents stressing there is no official policy that bans downloading such software, something that 45 percent of respondents acknowledge doing. Employees often send workplace documents as email attachments, with 33 percent of those surveyed doing so, and 48 percent are not even certain it breaches company policy. While 87 percent of surveyed respondents are not sure whether disabling firewall and security settings violates regulations, 17 percent of them do it. Lastly, 67 percent of employees surveyed claim sharing passwords with coworkers is banned, but that 46 percent of them do it.

## Identity Theft Mini-Quiz: True or False?

1. There is a higher incidence of identity fraud today than in past years.

**False.** Javelin Strategy and Research, which has conducted an annual mega-study on US ID theft and fraud for the past five years, found some 3.58% of respondents reported experiencing online fraud in the previous year--down from 3.74% in 2007, 4.0% in 2006, and 4.7% in 2003.

2. There are more victims of identity theft and fraud today than there have ever been before.

**False.** The Javelin 2008 study estimates that there were app. 8.1 million victims of ID theft and fraud last year, down from 8.4 million the year before.

3. Identity fraudsters are stealing record amounts of money from their victims.

**False.** Despite reports of big-dollar thefts and a booming black market for credit cards and other personal information, the cost of ID fraud and theft dropped last year to \$51 billion after hitting an all-time-high of \$58 billion in the 2007 Javelin study.

4. Most identity theft and fraud occurs online.

**False.** Some 14% of thefts were carried out using Trojans, viruses, or phishing. Data breaches accounted for another 7%. The greatest percentage, 33%, came from physical theft -- a lost or stolen wallet, purse, or credit card. And 17% were perpetrated by friends, relatives, or in-home employees.

Editor's Note: (Wyman) The results of this year's Javelin study are definitely surprising and perhaps encouraging, but let's not sigh in relief just yet, let alone become complacent about guarding sensitive personal information. The numbers may be down, but at the same time, they show that you are more likely to get ripped off by someone you know than by a faceless Bad Guy on the Internet.

---

## FTC Data: Telcos, Banks are Top Targets for ID Theft - Feb 29, 2008

Compromised accounts within just 25 companies account for nearly half of the identity theft complaints filed with the U.S. Federal Trade Commission, according to recently released FTC data compiled by the University of California, Berkeley.

In data culled from three months' worth of 2006 FTC complaints, Sprint and AT&T averaged more identity theft events than any other institution except Bank of America, the largest consumer bank in the U.S.

The FTC encourages victims of identity theft to file complaint forms in order to help the commission, as well as law enforcement organizations, get a picture of criminal trends. It publishes a survey on identity theft, but until now it has not broken down its data on complaints by institution.

That work was done by Berkeley's Center for Law and Technology, which used the Freedom of Information Act to obtain FTC data on more than 88,000 complaints filed in January, March and September 2006.

The data show that a handful of companies account for the lion's share of identity theft complaints.

Complaints mentioning just 25 companies account for 49.9 percent of all identity theft events in the FTC database, according to the report's author, Chris Hoofnagle, a senior fellow with the Berkeley center. About 7,500 companies are mentioned in the other 50.1 percent, he said.

Not surprisingly, banks dominate the top 25, with Bank of America, JP Morgan, Capital One and Citibank topping the list. But there are many telecommunications and technology companies there too, including Verizon, T-Mobile, Dish Network, Dell, eBay and DirectTV.

According to FTC data, about 8 percent of new account fraud comes from telecommunications companies, Hoofnagle said, calling that number "really astounding."

Often a phony telephone account is the first step toward a more complex identity theft scheme. Thieves can set up fake telephone accounts using real Social Security numbers but phony names, and then pay them for a few months to build up a credit history and apply for credit cards, Hoofnagle said.

AT&T said it is clear that many industries have a problem with identity theft. AT&T takes steps to educate customers about identity theft and what they can do prevent it, and also works with law enforcement agencies when thefts occur, the company's public relations agency said in a statement

Because the FTC data are not comprehensive -- only crimes that get reported to the FTC are counted -- and since there are no reliable figures on the number of consumers who have accounts with these companies, it is impossible to get an accurate picture of how common identity theft really is at any of these institutions, Hoofnagle said.

Companies should make this information public so that consumers can see how bad the problem really is, he said.

In the meantime, the Berkeley study gave the government some ideas about how to tackle the identity theft problem, he said. For example, banks that send out a lot of preapproved credit card applications seem to pop up more frequently in FTC complaints.

It's also worth looking more closely at why these month-by-month complaint numbers change for some companies. For example, Dish Network saw its total number of complaints drop off after spiking dramatically in March. "Something happened in February, or just before March, that caused a huge number of complaints," Hoofnagle said. "I have no idea what it was."

"Regulators should know this, and their attention should be focused on these 25 companies. What is going wrong at these places?"

## ***SURVEY: PRIVACY BREACHES RAMPANT IN CORPORATIONS***

Source: [SecurityFocus](#)

*Posted on February 22, 2008*

Nearly 85 percent of privacy and security professionals believe a reportable breach of personally identifiable information (PII) occurred within their organization in the last year, according to an online survey of 800 such professionals published in Dec./07 by accounting firm Deloitte & Touche and the Ponemon Institute.

Almost two-thirds of the professionals polled stated that their organizations had experienced multiple reportable breaches in the past year. The security and privacy managers only dedicated approximately 7 percent of their time to training employees and, at most, 10 percent of their time to establishing an incident response team, the survey found.

"Frankly, I'm shocked by the high percentage of PII data breaches we're seeing occur within organizations," Rena Mears, Deloitte global and U.S. privacy and data protection leader, stated in the release announcing the study. "This survey provides insight into the scale of the problem and how enterprises are struggling to respond. It's clear that both privacy and security professionals are caught in a reactive cycle, and they agree on the need to move to a more proactive stance."

A number of events in 2007 have raised corporate awareness of privacy issues. In January, retail giant TJX Companies announced that successive online attacks during 2005 and 2006 has resulted in the loss of, at last count, more than 94 million credit- and debit-card accounts. Last month, the head of HM Revenue & Customs, the United Kingdom's tax agency, resigned following a massive data leak that potentially put the sensitive personal details of 25 million people at risk.

The attention has caused many companies move toward encrypting their data. The survey found that 55 percent of companies are implementing "some type of encryption" and 37 percent are currently encrypting data in transit and information stored on servers, according to the survey.

