

# Security Trends Report

02/08

## "SAML: The Master Key?"

Government Computer News (01/21/08) Vol. 27, No. 2 ; Jackson, Joab

Federated identity management, which allows users to log into accounts on several different systems with one set of credentials, could be useful for federal agencies for several reasons. For instance, federal government employees often need to access systems and data held by agencies other than the one they work for. In addition, e-government initiatives often involve people that lack government-recognized credentials. The government authenticates the identities of these people by using the General Services Administration's E-Authentication Identity Federation initiative, which in turn uses an emerging XML-based standard known as the Security Assertion Markup Language (SAML). With SAML version 2.0, systems can attach user attribute information such as certificates, licenses, training, level of education, and privileges to an identity assertion. In addition, SAML 2.0 allows one agency to further check into the credentials issued by another agency. This feature comes in handy when someone wants access to additional resources or when someone wants to go directly to the outside resource without first going through the portal. With SAML 2.0, federal agencies with the right hardware and software can begin to streamline their cross-authentication processes.

## Feds seek 10% hike in IT security spending, as intelligence chief warns of cyberthreats

Proposed FY '09 budget also would earmark 10% of overall IT spending to security

By Patrick Thibodeau

February 7, 2008 (Computerworld) In the same week that Director of National Intelligence Michael McConnell warned Congress that terrorists are showing an increasing desire to use cyberattacks against the U.S., the Bush administration sent a proposed budget to federal lawmakers that calls for the government to spend one out of every 10 IT dollars on information security.

In total, the White House said this week that it will seek authorization for more than \$71 billion in IT spending during fiscal 2009, which begins Oct. 1. That request represents a 3.8% increase, or \$2.6 billion, over what Congress approved last year.

The budget proposal earmarks \$7.3 billion for information security, a 9.8% increase over what was budgeted for the current fiscal year. If approved as is, security spending would account for 10.3% of the entire federal IT budget.

Bush's proposal also would continue a trend in which security spending has been increasing at a rate that's greater than the growth of the overall IT budget. The White House, in its budget analysis ([download PDF](#)), said that if Congress accepts the fiscal 2009 figures as proposed, IT security spending will have increased 73% over the past five years, up from a starting point of \$4.2 billion in fiscal 2004. By comparison, the overall IT budget will have risen 20% during the same period.

[Karen Evans](#), administrator of e-government and IT at the [White House Office of Management and Budget](#), said at a press briefing on the budget today that the proposed spending levels aren't being allocated toward any particular aspect of security within federal agencies.

"The focus isn't investment-specific — it's making sure they are managing the risk associated with the services that they have," said Evans, who is the federal government's de facto CIO.

She added that as more and more government services become available online, "the agencies are very well aware of what the risks are."

McConnell testified before a Senate panel yesterday and a House committee today on his annual threat assessment report to Congress ([download PDF](#)). As part of the report, he issued a broad warning about the cyberthreats faced by both the government and the private sector, saying that potential vulnerabilities are only increasing because of globalization and the growth of computer networks.

McConnell cautioned in the report that Russia, China and other countries "have the technical capabilities to target and disrupt elements of the U.S. information infrastructure." And he said that terrorist groups such as [al-Qaeda](#), Hamas and Hezbollah "have expressed the desire to use cyber means to target the United States."

## MySpace, States Team Up for Children's Safety

---

Jan 15, 2008

An agreement between MySpace and most U.S. state attorneys general will significantly increase the [safety](#) of minors on the popular social network and boost the ability of police to catch and prosecute sexual predators who use the Web, said MySpace and several participating attorneys general Monday.

MySpace and attorneys general from 49 U.S. states and the District of Columbia announced on Monday a set of principles for social-networking safety that they hope will be broadly adopted by companies that operate these sites.

The announcement comes at a time when MySpace and social-networking sites in general are being closely monitored and sometimes sharply criticized by law enforcement agencies worldwide, which charge they aren't doing enough to protect minors on their sites.

Called the Joint Statement on Key Principles of Social Networking Sites Safety, the document states among its goals the development of a truly effective tool that social-networking sites can use to verify the age of members and potential members.

As part of the agreement, MySpace also pledged to develop a registry to which parents can submit their children's e-mail addresses to have them barred from social-networking sites.

MySpace will also make profiles of members under 18 years of age private by default and make it harder for adults to contact children via the site. The minimum age to have a MySpace profile is 14 years old.

In conjunction with the participating state attorneys general, MySpace has also committed to organizing an industry-wide Internet Safety Technical Task Force.

MySpace will also improve its tools and methods to identify and delete inappropriate images, obtain and constantly update a list of pornographic Web sites and break links between them and its site.

The joint statement is the result of about two years of ongoing discussions between the attorneys general and MySpace, said North Carolina Attorney General Roy Cooper and Connecticut Attorney General Richard Blumenthal during a news conference.

Calling the agreement "remarkable" and vowing that it will set "a new standard" for protecting minors online, Cooper said it's crucial for other social-networking sites like Facebook to support this effort.

"I urge other social-networking sites to follow this lead to participate in the task force and adopt the safety principles in this agreement," Cooper said.

Blumenthal predicted that the task force will begin generating concrete results in months, not years, and stressed that the attorneys general believe that it's key for the safety of minors to have effective age-verification tools and methods.

This way, children who aren't old enough to join a social network will be prevented from doing so, and teens under 18 years of age will get special protection, he said.

The attorneys general participating in the call, which also included those from Ohio and Pennsylvania, agreed that parents must also get involved in this effort.

MySpace was happy to engage in these discussions with the attorneys general, said MySpace Chief Security Officer Hemanshu Nigam, adding that he hopes others in the industry will join the effort.

"We have always believed that it takes a partnership of parents, law enforcement and educators to make progress towards a safer online community. Only by working together can we fully succeed in increasing Internet safety for all of our members, and for all other social-networking users," said Hemanshu, who is also CSO for Fox Interactive Media, the News Corp. division that houses MySpace.

Absent from the list of state attorneys general was Greg Abbott from Texas, who takes issue with several points included in the agreement with MySpace.

In a letter sent Monday to MySpace CEO Chris DeWolfe, Abbott characterized the joint statement's measures as "remedial" and as a "starting point rather than a point of conclusion."

"The protective steps memorialized in the joint statement improve online safety and security, but still fail to adequately protect child users," Abbott wrote in the letter, which was obtained by IDG News Service.

Adding his signature to the joint statement could be misinterpreted as an endorsement "of the inadequate safety measures contained therein," Abbott wrote, stressing that a major gap is the absence of an effective age-verification system.

Abbott also criticized the statement for being vague, especially about the specific steps MySpace must implement "to promote and facilitate" cooperation with law enforcement agencies.

## Federal Government Appeals Judge's Decryption Key Decision

(January 16, 2008) The federal government has appealed a decision by a judge in Vermont that has prevented a man from divulging the password necessary to decrypt his computer. Magistrate Judge Jerome J. Niedermeier said that to force an individual to enter the password into his computer is a violation of the Fifth Amendment, which grants protection from self-incrimination. The case involves a Canadian citizen with legal residency in the US whose computer was found to contain child pornography. The computer was seized, but the government has been unable to access data in drive Z because it is protected by PGP encryption.

(please note this site requires free registration) [http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663_pf.html)  
<http://www.heise-security.co.uk/news/101935>

[Editor's Note (Pescatore): In the US (and I think at least also Canada) there is certainly legal precedent for law enforcement using court orders to require a suspect to open a locked desk drawer, locker or safe. So, it is hard to see how in the long run this same thinking wouldn't extend to decrypting data - entering a password is pretty equivalent to entering a combination. But in the short run technology always moves faster than laws and regulations.

(Schultz): The judge's ruling makes considerable sense given that the US Bill of Rights guarantees that a person does not have to testify against himself. Requiring an accused person to surrender a password, encryption key, or some other object that allows investigators to access evidence against that person is in reality equivalent to forcing someone to provide self-incriminating testimony.]

## One year later: Five takeaways from the TJX breach

The retailer has survived the massive data theft, but the card industry remains unsettled  
**Jaikumar Vijayan**

**January 17, 2008** ([Computerworld](#)) -- One year ago today, [The TJX Companies Inc.](#) **disclosed** what has turned out to be the largest information security breach involving credit and debit card data -- thus far, at least.

The data compromise at the Framingham, Mass.-based retailer began in mid-2005, with [system intrusions](#) at two Marshalls stores in Miami via poorly protected wireless LANs. The intruders who broke into TJX's payment systems remained undetected for 18 months, during which time they downloaded a total of 80GB of cardholder data.

TJX eventually said that 45.6 million card numbers belonging to customers in multiple countries [were stolen](#) from its systems. Even that number may be far too low: A group of banks that is suing the retailer [claimed](#) in an October court filing that information about 94 million cards was exposed during the serial intrusions.

The sheer size of the data theft puts TJX in a league of its own among companies hit by such incidents, and the breach has made it something of a poster child for sloppy data security practices among retailers. In addition, the breach highlighted several familiar issues and some not-so-familiar ones.

Here, on the one-year anniversary of the breach becoming known, are five takeaways for security managers:

### **Breach disclosures don't always affect revenue or stock prices ...**

Despite being the biggest, costliest and perhaps most written-about breach ever, customer and investor confidence in TJX has remained largely unshaken. TJX's stock was worth about \$30 per share when the breach was disclosed, and its closing

price today was just over \$29. Meanwhile, the retailer said this month that in the 48-week period that ended Jan. 5, its consolidated comparable-store sales [increased 4%](#) from the year-earlier level.

Clearly, TJX's customers weren't as concerned about the breach as many observers had expected they would be. Much of that no doubt has to do with the fact that consumers realize they themselves won't have to pay for any fraud that might result from payment card compromises, said [Avivah Litan](#), an analyst at [Gartner Inc.](#)

### **... but they can be costly**

TJX has said that in the 12 months since the breach was disclosed, it has spent or set aside about \$250 million in breach-related costs. That includes the costs associated with fixing the security flaws that led to the breach, as well as dealing with all of the claims, lawsuits and fines that followed the breach.

For instance, settlements reached by TJX include offers of free credit-monitoring services for three years to consumers whose driver's license numbers were exposed in the breach, plus cash reimbursements, vouchers and a promised three-day customer appreciation event this year, during which the company plans to offer 15% discounts on all goods.

"I think a lot of companies are seeing how costly these breaches can get," said Forrester Research Inc. analyst [Khalid Kark](#). As a result, there's a lot more awareness in the executive suite about the need for security controls, Kark said. He previously estimated that the breach at TJX could end up costing the company \$1 billion over the next few years.

### **PCI remains a work in progress**

The breach brought to light the fact that many retailers, including top-tier ones like TJX, had not yet fully implemented the set of security controls mandated by the major credit card companies under the Payment Card Industry Data Security Standard, or PCI. The rules took effect in June 2005, and required merchants -- especially ones such as TJX that process a high volume of card transactions annually -- to implement 12 broad security controls for protecting customer data.

But court documents filed by the banks that are suing TJX allege that the company [wasn't compliant](#) with nine of the mandated controls during the period when the intrusions were taking place. And TJX was by no means alone. In response to the slow adoption of the PCI controls, Visa Inc. [threatened](#) to start imposing hefty fines and higher transaction fees on merchants if they didn't become compliant by the end of last September.

Visa won't disclose whether it has fined any merchants since then, but there is ample anecdotal evidence that it has.

### **The card payment process has issues**

The TJX breach exposed a fundamental rift, with banks and credit card companies on one side and merchants on the other. In several states, credit unions and smaller banks have lobbied the legislatures to pass new laws requiring retailers to reimburse them for the costs involved in notifying customers of breaches and reissuing cards.

But the lobbying attempts failed everywhere except in Minnesota, which last May approved the Plastic Card Security Act -- a law that holds breached entities [financially responsible](#) if they were storing prohibited card data on their systems.

In fighting the state bills, retailers have argued that the commissions they pay to card companies on each transaction are supposed to cover fraud-related costs, making any additional payments a double penalty. They also said that the only reason they store payment card data is because they're required to by the credit card companies. In October, the [National Retail Federation](#) (NRF) asked Visa and the other card companies to [drop that requirement](#).

The NRF's request is echoed by Litan, who long has argued for fundamental changes in the card industry's payment process, via the introduction of measures such as one-time passwords and all PIN-based transactions.

### **The bad guys remain hard to catch**

For all the attention paid to the breach by TJX, and all the hired forensics experts and law enforcement authorities on the case, the perpetrators thus far haven't been tracked down. Some individuals who [allegedly used](#) card numbers stolen in the breach have been arrested. But the hackers themselves have remained frustratingly out of reach, as is the case in most breaches.

"The crooks are still at it," Litan said. "They probably will strike again. They're laughing all the way to the bank."

# Top 10 Cybersecurity Menaces For 2008 Listed

## Expect increased attacks on Web browsers, more botnets, and sophisticated cyberespionage, according to the annual SANS Institute report.

By [Thomas Claburn](#)

[InformationWeek](#)

January 15, 2008 06:30 AM

The SANS Institute on Monday released its take on the [top 10 cybersecurity threats for 2008](#). Leading the list is a rise in the number of attacks on Web browsers, the proliferation of botnets, and sophisticated cyberespionage.

Twelve noted cybersecurity experts -- Stephen Northcutt, Ed Skoudis, Marc Sachs, Johannes Ullrich, Tom Liston, Eric Cole, Eugene Schultz, Rohit Dhamankar, Amit Yoran, Howard Schmidt, Will Pelgrin, and Alan Paller -- helped compile the list. Released in conjunction with the SANS [Security](#) 2008 conference in New Orleans, the list represents a collective assessment of the online attack vectors most likely to cause damage in the year ahead.

Attacks on Web browsers, particularly plug-in components like Flash and QuickTime, represent the top threat. The reason these browser components are being targeted is that they're widely distributed and they're not automatically updated when the browser is updated, leaving a longer window of vulnerability on affected systems. Additionally, cybercriminals have been automating their attacks so that they check for a variety of possible vulnerabilities and disguising them so that each new assay is different from the last. One of the hacking kits now available to attackers, MPack, "produces a claimed 10% to 25% success rate in exploiting browsers that visit sites infected with the module," according to the SANS report. Attackers also have been more successful in placing malicious payloads on trusted sites, making reputation-based defenses less effective.

The increasing sophistication and effectiveness of botnets -- coordinated groups of compromised PCs -- takes the second spot on the SANS list. The Storm Trojan, which began spreading through e-mail in January 2007, was responsible for one out of every 12 computer virus infections only a week after its release. Both [Storm and an upcoming rival, Nugache](#), operate through encrypted peer-to-peer channels, which means there's no central server to shut down and botnet communication is difficult to block.

Third on the list is cyberespionage. "One of the biggest security stories of 2007 was disclosure in congressional hearings and by senior DoD officials of massive penetration of federal agencies and defense contractors and theft of terabytes of [data](#) by the Chinese and other nation states," the SANS report said. "In 2008, despite intense scrutiny, these nation-state attacks will expand; more targets and increased sophistication will mean many successes for attackers."

Attacks on high-value targets are often conducted through spear-phishing, in which personalized messages rely on social engineering to trick recipients into taking some action that compromises their computer -- opening a file that exploits an undisclosed Microsoft (NSDQ: [MSFT](#)) Office vulnerability, for example.

Threats to mobile phones, particularly to the iPhone, upcoming Google (NSDQ: [GOOG](#)) Android phones, and VoIP systems, rank fourth on the SANS list. "A truly open mobile platform will usher in completely unforeseen security nightmares," the SANS report said. "The developer toolkits provide easy access for hackers."

Apple CEO Steve Jobs on Tuesday is widely expected to provide additional details about the upcoming Apple iPhone software development kit (SDK), about how iPhone applications will be made available (presumably through Apple's iTunes), and about how iPhone applications will be made secure.

Insider attacks rank fifth on the list. While rogue employees and contractors have long been a concern of corporate security managers, the various experts contributing to the SANS report see the risk posed by malicious insiders rising due to the interconnectedness of systems today and the rising value of data in general. The flurry of acquisitions in the data leak prevention space over the past year suggests that security companies hear worries about this from corporate clients and are investing accordingly.

Advanced identity theft bots appear sixth on the SANS list. "A new generation of identity theft is being powered by bots that stay on machines for three to five months collecting passwords, bank account information, surfing history, frequently used e-mail addresses, and more," the SANS report said. "They'll gather enough data to enable extortion attempts (against people who surf child porn sites, for example) and advanced identity theft attempts where criminals have enough data to pass basic

[security](#) checks."

A Trojan program, Trojan.Silentbanker, described on Monday in a [Symantec blog post](#) represents one such bot. "The ability of this Trojan to perform man-in-the-middle attacks on valid transactions is what is most worrying," said Symantec (NSDQ: [SYMC](#)) researcher Liam O'Murchu. "The Trojan can intercept transactions that require two-factor authentication. It can then silently change the user-entered destination bank account details to the attacker's account details instead."

The sophistication of Trojan.Silentbanker and other malware like Storm and Nugache reflects the seventh-ranked item on the SANS list: The increasing maliciousness of malware. Malware is not only becoming more insidious, but more aggressive in its quest for self-preservation. The SANS researchers see malware increasingly taking the offensive against malware fighters and their systems. They also see malware becoming increasingly stealthy, hiding its malicious nature to strike more effectively. This also is happening at a network level, where fast-flux DNS techniques are being refined to better conceal malware server infrastructure.

Web application vulnerabilities, such as cross-site scripting and SQL injection attacks, rank eighth on the list. "Until 2007, few criminals attacked these vulnerable sites because other attack vectors were more likely to lead to economic or information access advantage," the SANS report said. "Increasingly, however, advances in XSS and other attacks have demonstrated that criminals looking for financial gain can exploit vulnerabilities resulting from Web programming errors as new ways of penetrating important organizations."

As if to prove the point, a [massive SQL attack](#) was reported last week. And the security experts who participated in this SANS report expect more such attacks in 2008.

Coming in at number nine, the SANS report anticipates a rise in blended and event-based attacks. Such attacks might rely on a provocative fake headline to entice recipients to open a malicious message. Or they might combine a phishing attack with an inducement to reveal personal information over the phone. An example of such an attack is the [phony Federal Trade Commission e-mail](#) notice sent Salesforce.com users last October that installed malware when the message was opened.

Last, the SANS report cites the rising risk of supply chain attacks affecting consumer devices. "The widespread adoption of the USB standard combined with cheap memory and consumer demand for more computer peripherals makes this vector a simple target for a sophisticated attacker," explained Marc Sachs, executive director of government affairs for national security policy at Verizon (NYSE: [VZ](#)) and director of the SANS Institute's Internet Storm Center, in an e-mail last week. "Pranksters like it, too. It's a simple matter to purchase an item at Best Buy (NYSE: [BBY](#)) or Target, bring it home, infect it as a joke, and return it. Most large stores have a 'no questions asked' return policy within a week or two of purchase. Even worse, most stores will quickly test a returned item and, if it appears to work, will reshrink-wrap it, put a price sticker on it, and return it to the shelf."

Despite recent reports of malware-infected digital picture frames and other devices, such attacks aren't likely to match the broad impact of the Storm Trojan. Nonetheless, they're well-suited for targeted attacks, and those tend to be more damaging than less discriminating attacks.

## Government urged to standardize data encryption standards

By Heather Greenfield *CongressDaily* January 11, 2008

Some people are hoping the new year brings a new level of agreement on encryption standards used by federal agencies. Vendors are awaiting a request for proposals from the Homeland Security Department on encryption standards.

Encryption is seen by many as a way federal agencies can better protect sensitive data, but the existence of so many types of encryption and services has meant that the purpose and ability to read them can easily get lost.

"It's like one hand clapping," said Jim Russell with Symantec's public-sector education department. "We need one single encryption tool that incorporates multiple vendors."

He will be both advocating and applauding any movement toward encryption standards, but it could be a slow process. Chief information officers, including Vance Hitch at the Justice Department, have said complying with directives by the White House Office of Management and Budget to encrypt all sensitive data leaving his department is a challenge because of differences among federal agencies, which currently use competing software and vendors.

At security conferences last fall, federal CIOs said the problem is that when employees see encryption or other security steps as too slow or too much of an obstacle to doing their jobs, they become more likely to break the rules.

The Government Accountability Office repeatedly has criticized federal entities, including the Internal Revenue Service in a report this week, for not following their own rules that require sensitive data to be encrypted.

GAO praised the IRS for better controlling user IDs on critical servers, building security into new applications and encrypting

data. But the watchdog also found that the agency didn't always enforce password management or encrypt sensitive data. A main reason that about 70 percent of the cyber-security upgrades remain undone is that the IRS is part way through implementing an agency-wide security program, according to the report. The fiscal 2008 budget provides \$267 million for the upgrades.

On another security front, GAO has recommended Homeland Security do a better job securing online electric-control systems and sharing vulnerabilities of the systems. Additional steps may be around the corner for that.

Because private companies control the power grid, Homeland Security has been relying on the Federal Energy Regulatory Commission to recommend how to better protect the power grid from cyber attacks. FERC in turn has relied on voluntary standards developed by the Northern American Electric Reliability Corporation.

NAERC issued a report on its latest guidelines this week and is requesting comments. But at a hearing last fall, Rep. Al Green, D-Texas, wanted something with teeth. He has asked FERC's new director, Joseph McClelland, to determine whether FERC needs Congress to grant legal authority to mandate that electric companies implement best cyber-security practices. McClelland told the House Homeland Security cyber-security panel that he does not think FERC has any enforcement authority over private companies on the matter.

## Secure E-mail standard released

By [William Jackson](#)

An international government-industry group has published specifications for a Secure E-mail standard that is intended to let governments communicate securely with each other and with their private-sector suppliers.

The specs developed by the [Transglobal Secure Collaboration Program](#) are built on a trusted public-key infrastructure model, similar to the U.S. government's Federal PKI Bridge, but also include a policies and procedures for vetting and managing identity and access controls within an organization. This would assure users not only that an e-mail message is securely encrypted, but that the senders and receivers are who they say they are and are entitled to access the contents.

TSCP was formed in 2002 by the U.K. Ministry of Defense (MOD); its members now include the U.S. Defense Department, the Dutch government and a handful of major international defense contractors, including BAE Systems, Boeing, EADS, Lockheed Martin, Northrop Grumman, Raytheon and Rolls-Royce. Both the DOD and MOD plan to implement Secure E-mail, said TSCP Director Wayne Grundy, who also works for BAE.

"When you think about this in principle, it sounds straightforward," Grundy said. "When you try to implement it, it becomes tremendously complicated. That is why nobody has done it before" on a wide scale. "It is done on a case-by-case basis."

The goal of the standard is to extend trusted relationships throughout the government supply chain, which can include thousands of suppliers as well as government entities and their prime contractors.

Paul Grant, deputy information sharing executive for the DOD chief information officer, said the standard would turn e-mail "from one of the most extensively used but least-trusted collaboration capabilities to one that can be trusted with sensitive information. This will serve as a foundation for sharing Controlled Unclassified Information with our mission partners, which certainly includes our suppliers."

The U.S. Controlled Unclassified designation includes "For Official Use Only" and "Sensitive but Unclassified Information." Across the pond, the standard will be used with information designated "U.K. Restricted."

The specifications were completed late last year. MOD has announced its intention to make Secure E-Mail standard on desktops across its enterprise this year. DOD completed testing of the specs last fall and is planning to pilot the standard this year in a large program involving most TSCP member companies, Grundy said. Details of the pilot are expected to be released soon.

"This is not about a specific technology," Grundy said. "The technology isn't necessarily unique. It's about how to get governments and other parties to agree" on who can be trusted.

The current implementation of the standard uses off-the-shelf e-mail products and open-source software, with CertiPath as the certificate authority. CertiPath is certified with the Federal PKI Bridge. The relationship between the federal bridge and CertiPath is unique because CertiPath itself is a bridge that cross-certifies certificates issued by aerospace contractors. CertiPath is a joint venture of Arinc, Exostar and SITA. VeriSign issues certificates to the CertiPath bridge for bridge-to-bridge trust.

Digital certificates act as electronic IDs, but the party or application accepting a certificate must have a way of validating it. When a foreign certificate is submitted to an application, it is passed on to the federal bridge, which verifies that it was issued by an organization whose policies have been accepted by the bridge. The bridge also can check with the issuing authority to

ensure the certificate is still valid.

But the trust established by a PKI bridge is only as reliable as the practices of the member organizations for establishing the identity of employees and contractors who receive certificates, and for managing their access privileges within the organization. The Secure E-Mail specifications are a step-by-step manual on how this must be done. The system also requires an end-user encryption certificate lookup tool for the collection of unpublished digital certificates in Microsoft Outlook or Lotus Notes e-mail clients. Boeing developed this tool for Secure E-Mail.

The end result should be that a sender's and receiver's identities are known at a common level of assurance and still are valid, and that the underlying identity management systems can be trusted. This assurance is used to grant access to sensitive information.

## IM, chat and P2P network attacks up in 2007

Posted by Miya Knights at 1:45PM, Friday 11th January 2008

**New figures reveal uncontrolled growth of greynets on enterprise networks help numbers of attacks on MSN, Yahoo! and AOL, as well as non-IM vectors rise.**

New figures released today have found they were five unique instant message (IM) and peer-to-peer (P2P) virus attacks on [enterprise](#) networks a day in 2007.

At the same time, uncontrolled use of greynets on enterprise networks has grown significantly over the past year, which include real time, always on applications including IM and web conferencing among others according to IM security specialist [FaceTime Security Labs](#).

The [GreynetsGuide](#) website, managed by FaceTime, found most organisations operate between eight and 10 greynets in their networks and, along with rising employee usage, can increase risk exposure to viruses increasingly targeting IM, chat and P2P vectors.

Frank Cabri, vice president of marketing and product management for FaceTime said that, while many greynet applications have legitimate business uses, there are also many that do not.

"IT managers need to ensure the safe use of approved applications and effectively detect and block the rogue use of unapproved applications," he said, highlighting the 1,088 incidents reported over all IM, P2P, and chat vectors during 2007.

The research found the most heavily targeted IM network was Microsoft MSN (45 per cent), followed by Yahoo! with 20 per cent and AOL with 19 per cent. The remaining 15 per cent included all other IM networks, including Jabber-based ones. And attacks on these private networks have more than doubled since 2003, rising from seven per cent of all IM attacks to 15 per cent in 2007.

It also notes a shift in the non-IM vectors also used to distribute viruses, highlighting that internet relay chat (IRC) distributed attacks were up 14 per cent during 2006-7, along with a rise in socially engineered attacks on sites like MySpace.

"Many hacks and scams are creeping into the mainstream areas of MySpace and other social networking sites, as the perpetrators become bolder and more aggressive," said Chris Boyd, FaceTime director of malware research.

In tandem, the security firm predicted the number of greynets currently in use worldwide will increase from more than 600 currently to over 1,000 by the end of 2008.

Other commonly downloaded applications classed as greynets also include newer plug in-type applications like search engine tool bars and online social networking sites, multimedia distribution portals, internet protocol television (IPTV) and web 2.0 applications that enable liberal user customisation and require continual revisiting of enterprise network usage and compliance policies.

## "Security Dominates 2008 IT Agenda"

[Network World \(01/07/08\) Vol. 25, No. 1, P. 1](#)

Security concerns are expected to dominate the network landscape in 2008, experts say. They are particularly concerned that Web sites and networks related to the 2008 Olympics in Beijing will be used to infect people's computers. Websense's Dan Hubbard says Olympics-related Web sites and networks will also be used as a lure for fraud. Another likely security problem this year are botnets with decentralized command-and-control structures that make them more difficult to shut down, says McAfee researcher Craig Schumgar. Meanwhile, experts are saying that there will not be any major security exploits against VoIP systems this year, due in part to the fact that the largest VoIP vendors are using proprietary controls, which are harder to obtain and study for possible security vulnerabilities. Nevertheless, Paul Simmonds, a member of the management board of the Jericho Forum, a user group promoting new principles for secure networking, calls VoIP a "time bomb" that is "poised for a massive exploit." Other trends to watch out for this year, experts say, are the growing prevalence of 802.11n wireless technology and the increased reliance of Web 2.0 technologies among enterprises.

## New predictive approach seeks to stay ahead of hackers

(01/11/2008 12:13 PM EST)

SAN FRANCISCO — Military and academic researchers are collaborating to protect computer networks—by figuring out what cyberspace intruders are likely to do next.

The researchers are looking at intrusion prediction, which uses mathematical models and algorithms to map out a hacker's or attacker's probable moves once they have broken into a network.

"We want to be one step ahead of them and predict what they are going to do," said Shanchieh Jay Yang, a computer engineering assistant professor at the Rochester Institute of Technology (RIT). "When they first get in, we try to observe what they are doing, and use that information to forecast their probable future actions."

Security specialists said the research is worthwhile, but may be of little use in a fast-changing network environment.

Nevertheless, researchers from RIT, the University of Buffalo, and Pennsylvania State University are working with CUBRC, a Buffalo-based nonprofit research and development organization, and the U.S. Air Force.

The goal is to provide information about how an intruder will react to particular network defenses and architectures so that administrators can reduce the damage they might do and better protect their systems.

Intrusion prediction modeling isn't meant to be the sole solution but part of a larger picture of network protection, according to Yang. It's designed to defend against the different tactics used by network intruders. One might be more interested in interrupting service, another in obtaining data, he said.

In either case, software first filters out false alarms and not-so-important alerts of anomalous activity. Then the scheme correlates different alert systems to the number of attackers. It can follow particular attackers and can work on parallel tracks for multiple attackers, Yang said.

The approach has both military and commercial applications, Yang said.

In a commercial setting such as a bank, the software could collect observations about a hacker's efforts to transfer money or interrupt online service. It could determine what kind of operating systems the hacker is familiar with, and whether he was a first-time hacker or a pro.

That information would go to the bank's intrusion detection system, which would send alert messages to its IT department.

The bad news is that there's no way to completely block cyberspace attacks, Yang said.

When they do occur, there's another cyberspace-specific issue, said Rebecca Bace, who ran an intrusion detection research program for the National Security Administration in the 1990s. Now president and CEO of [Infidel, Inc.](#) (Scotts Valley, Calif.), an information security provider, Bace said it isn't always clear whether an attack is intentional.

## The Future of Information Security: 2008 and Beyond

New complexities of information security create the need for a new type of executive: a strategist with business savvy, sound risk fundamentals and holistic technical understanding.

By Kevin Richards, Risk Advisory Services, Ernst & Young

**January 02, 2008 — CIO** — Looking into 2008, the information security agenda for executives continues to evolve. Long gone are the days where a firewall and an intrusion detection system can constitute the arsenal of information security defense. The complexities of what to protect and when, overlaid with requirements of regulation and compliance, create the need for a new type of information security executive—one with business savvy, sound risk fundamentals and holistic

technical understanding. These skills, coupled with a strong strategy, will be necessary for organizations to achieve their 2008 information security goals.

In looking to build that type of strategy and structure, the items most likely to top the list are data protection and governance, compliance and the effective integration of information security practices into key business and risk management efforts. Executives must choose carefully; how the 2008 strategy addresses these three critical items may determine the program's ultimate success in protecting the business.

## **Where did the data go?**

Data has gone rogue, and it didn't make any headlines in the process. Perhaps it should have. An event this important warrants some attention, but because it didn't happen with a big bang, no one seemed to notice. Inanimate as it is, data is causing problems because it's growing at an uncontrollable rate and it's hiding seemingly everywhere—both in the trusted confines of the data center and on the move through laptops, PDAs and e-mail. It's being disclosed (both on purpose and inadvertently) at an alarming rate and it's all but openly defying the letter of our corporate policies and standards.

The number one item on the 2008 information security agenda is data protection. The practice of protecting the confidentiality, integrity and availability of data is not new—passwords, encryption and data classification structures have been around for years. What has changed is the type of data that's now considered valuable. From the external attacker perspective, intellectual property and insider information were once the most sought-after data asset. Now, the data currency of choice is *identity*—e-mail addresses, social security numbers and credit card information. Corporate espionage is still a significant threat, but the new underground deals in volume, where success is being measured in thousands and millions of identities.

Internally, data protection is equally challenging. Executives demand that data be available to aid in decision support, albeit limited to only those team members with a "need to know." Whether through e-mail, jump drives or mobile devices, sensitive information seems to be leaving companies in droves. Add in the complexities of outsourcing and offshoring, and the data protection strategy needs to stretch beyond once-trusted walls and around the world.

Ultimately, the challenge starts with something very fundamental—knowing where critical data lives—then leads to a myriad of additional questions and potential obstacles. How should the data be protected? What's the risk to the business if it's lost, stolen or disclosed? What are the regulatory implications of a breach? Who controls the most recent version of the data? How are business partners protecting the data?

This is the world of data governance. In its simplest form, data governance is an umbrella term referring to the various views in a data protection strategy. Under this umbrella are a number of different facets: *data inventory* and *data classification*—where critical data live and what expectations there are with respect to how and by whom data can be accessed, handled, stored, transmitted, processed and disposed; *vendor risk management*—how data is shared and subsequently protected by business partners; and *data leakage*—what data is leaving the organization by unforeseen or inappropriate ways. There is also the question of *authoritativeness*, that is, where the copies or replicas of data may exist within the environment, where the most recent version resides, who controls it and how changes are propagated throughout the organization to aid in decision support. Additionally, there are the issues of *privacy* and *compliance*—whether privacy expectations and regulatory requirements around both are being met across the enterprise and with outside third parties. Last but not least, there is *e-discovery* and *litigation support*, particularly with respect to the accessibility of tools and processes for responding to ad hoc enterprisewide demands and legal or regulatory substantiation.

## **Does better information security lead to better compliance? Is the reverse true?**

While data protection may be the most difficult challenge for the information security organization in 2008, achieving internal and external compliance goals will be the most measured part of the program. According to the 10th Annual [Ernst & Young](#) Global Information Security Survey, 60 percent of respondents cited their compliance efforts as the most important activities to their organization, with over half stating that a majority of their team's time is being spent on compliance activities. Roughly 80 percent of respondents noted that tying compliance goals to their information security initiatives helped them justify and obtain resources and budgets for those initiatives. They also said that by having to address regulatory and compliance requirements, they've improved their organization's information security posture.

Whether it's a question of complying with Sarbanes-Oxley or with the regulatory requirements of the payment card (PCI) or healthcare (HIPAA) industries, compliance initiatives will continue to be a significant driver for and component of the 2008 information security agenda.

## **Protecting business from the inside out**

While data protection provides the challenge, and compliance will consume a majority of the time, the most relevant trend for 2008 is information security's emergence as a strategic business-level issue that plays an increasing role in achieving business objectives. For years, the term *IT security* has been very appropriate, since activities were focused around antivirus, firewall rules, intrusion detection and the like, with the need for specialized skills to implement and manage specific security technologies. These technologies will continue to flourish and improve, but the mysticism associated with managing them has all but gone away. The operational roles to support these tools are being integrated into the organization's infrastructure team, which is where the roles belong. Antivirus software should be a standard part of a desktop operating system build and supported by the desktop management team; firewall management should be included as part of the network management team, etc.

The role of information security in 2008 and beyond is to help a company understand the risks to, and effect on, business operations stemming from the current environment. That means incorporating risks associated with data, privacy, business resiliency and continuity, technology, third parties and, with the help of corporate counsel, even potential legal risks to enable executives to make better business decisions. Moving forward, information security concerns will begin to be integrated at a fundamental level with business initiatives as they are being developed and will become a relevant component of a company's enterprise risk picture.

## **The information security journey through 2008**

The role of information security in 2008 will be more of a journey than a destination. The ever-changing landscape of risks, regulations and threats will provide multiple diversions and distractions from the security program. However, focusing on data protection and governance, achieving compliance goals and integrating information security into the key business initiatives will lead to a more successful program for 2008 and in the journey beyond.

## Court extends injunction against NASA background checks

### Smart-card credentialing program raises serious privacy issues, says Ninth Circuit Jaikumar Vijayan

**January 17, 2008** ([Computerworld](#)) -- The Court of Appeals for the Ninth Circuit last week extended an injunction against [NASA](#) that temporarily prevents it from requiring certain contractors to submit to a new background-check process as part of a mandatory smart-card credentialing program.

In arriving at its decision, a three-judge panel for the Ninth Circuit noted that the background check process raised serious privacy issues and was far too broad in scope to meet any legitimate government need. It ruled that 28 contractors who had sued NASA in Los Angeles District Court last August over the background checks did not need to submit to those checks for the duration of the court proceedings. The latest injunction extends one that was issued by the [Ninth Circuit Court](#) in early October, after the district court hearing the case rejected the contractors' request.

The 28 contractors are all senior scientists and engineers at the [Jet Propulsion Laboratory](#) (JPL), which is staffed and managed for NASA by the [California Institute of Technology](#).

The group filed suit last year against the U.S. government, NASA and Caltech, challenging what they claimed were overly intrusive background-check requirements by NASA. The contractors [asked](#) the court to not only force NASA to permanently stop the background investigations, but also to issue a preliminary injunction to halt the checks while the case was considered.

NASA had required the checks under Homeland Security Presidential Directive 12 of August 2004, a presidentially mandated smart-card credential program. HSPD-12 requires federal agencies to issue new tamperproof smart-card identity credentials called Personal Identity Verification cards to all employees and contractors. As part of the program, all employees and contractors are required to submit to comprehensive background checks, including criminal histories. Those who did not submit to the checks faced termination.

The 28 contractors, many of whom have worked for JPL for decades, had argued that the checks were unnecessary in their case, considering the nonclassified, low-security nature of the work they were doing for NASA.

A hearing on a federal motion to dismiss the case had been scheduled for last Friday in Los Angeles District Court. The Ninth Circuit's ruling came before that scheduled hearing. "Federal defendants' motion to dismiss was superseded by the Appeals Court ruling, and the case will now go forward in the District Court," a [statement](#) posted on the plaintiffs' Web site noted.

The next hearing is scheduled for Feb. 15.

## UK Gov Policy Forbids Taking Unencrypted Laptops and Drives Away From Offices

(January 22 & 23, 2008) UK Cabinet Secretary Sir Gus O'Donnell has sent an email to top civil servants informing them of a new policy that prohibits laptops and hard drives containing sensitive data from being taken out of government buildings unless the devices are encrypted. The notification comes in the wake of revelations that a number of Ministry of Defence (MoD) laptops containing unencrypted sensitive data have been stolen. In a related story, Defence Secretary Des Brown outlined the steps his department has already taken in the wake of the laptop thefts as well as actions that are underway to prevent further data loss.

[Editor's Note (Pescatore): This is the typical type of backwards thinking that gets everyone in trouble. The Agency or IT organization should put encryption software on all laptops and portable devices, rather than buying users portable devices and then saying "we know they are portable, and we know we gave them to you in an unsafe condition, so don't carry them around" Don't give users laptops unless you are configuring them with encryption software, endpoint protection etc - would you give delivery drivers trucks made of balsa wood and issue policy that says "Don't drive in traffic"???

(Honan): The recent data losses were reportedly due to junior members of staff not abiding to policy. Simply implementing another policy without effective tools, controls and training to ensure compliance with the policy will ultimately result in the policy being ignored and another data breach occurring.]

## Widespread 'Rock Phish' Techniques Contribute to Online Fraud

---

Jan 23, 2008

Phishing and pharming attacks continue to be a major source of crime against worldwide financial institutions, according to latest RSA report

By Katherine Walsh

A new report from RSA's Anti-Fraud Command Center found increased phishing activity with characteristics similar to that of the so-called Rock Phish, the person or group of people potentially responsible for half of all phishing attacks worldwide. However, the same countries are still hosting the attacks, according to the study, which is based on phishing, pharming and Trojan attacks tracked by the Command Center during the month of December.

Highlights of the study include:

- \* Activity from the Rock Phish group or similar groups increased. An increase in phishing attacks is due to increased activity of the Rock Phish group and may also be the result of copycat groups that have adopted similar methodologies, such as the use of proxy servers and the initiation of multiple attacks from a single domain. Although the magnitude of these copycat attacks is smaller than Rock's, it is evidence that other groups are starting to use these techniques.
- \* The distribution of global attacks remains constant. Since June 2007, U.S banking brands have remained dominant, representing 62 percent of phished entities. December was the eleventh consecutive month in which banks in the United Kingdom occupied the second spot, at 11 percent.
- \* Online fraud activity increased. A total of 186 attacks on financial institutions were recorded during December, including attacks against 20 financial intuitions that had never been attacked before.
- \* Hosting countries for attacks remain fairly constant. Although the percentage of attacks hosted in the United States dropped to 44 percent in December from 60 percent in November, it remains the top hosting country. Hong Kong and China fell into the second and third spots, at 16 percent and 12 percent respectively. The Philippines, a newcomer to the list, became the fourth largest attack host this month, with 8 percent of hosted attacks originating from that country.

## First Case of 'Drive-By Pharming' Identified in the Wild

---

Jan 23, 2008

The theory is now a reality. Symantec reported Tuesday that drive-by pharming, in which a hacker changes the DNS settings on a customer's broadband router or wireless access point and directs the link to a fraudulent Web site, has been observed in the wild.

The first drive-by pharming attack has been observed against a Mexican bank: "It's associated with an e-mail pretending to be from a legitimate Spanish-language e-greeting card company, Gusanito.com," says Symantec Security Response principal researcher Zulfikar Ramzan. Inside the e-mail is an HTML image tag but instead of displaying images, it sends a request to the home router to tamper with it.

In the e-mail evidence Symantec has examined, the code seeks to change 2Wire DSL routers to point the user's Web browser to a fraudulent bank site that mimics the site of one of the largest Mexican banks. Ramzan declined to name the specific bank.

"So, whenever you'd want to go to the bank site, instead of the real one, you'd get the attacker's fake site," he says. For the home PC user, the danger is that this drive-by pharming attack is "so silent and there's only subtle telltale signs that it's occurring," he adds.

A white paper last year from Symantec and the Indiana University School of Informatics coined the term. At the time the researchers detailed the JavaScript-based security threat and said such an attack could hit up to 50% of home broadband users.

Drive-by pharming can occur because home router equipment is often left configured with default log-in and password information and never changed. "The attacks know what the defaults are," Ramzan says. The simplest defense is to make sure home routers of any type have the default password settings changed.

Corporate routers are not typically seen to be as vulnerable to drive-by pharming "because they tend to be managed better," he says.

Ramzan added he expected the drive-by pharming attack to accelerate as online attackers move beyond into newer methods than traditional e-mail phishing.

## CIA Says Hackers Pulled Plug on Power Grid

---

**Jan 22, 2008**

Criminals have been able to hack into computer systems via the Internet and cut power to several cities, a U.S. Central Intelligence Agency analyst said this week.

Speaking at a [conference](#) of security professionals on Wednesday, CIA analyst Tom Donahue disclosed the recently declassified attacks while offering few specifics on what actually went wrong.

Criminals have launched online attacks that disrupted power equipment in several regions outside of the U.S., he said, without identifying the countries affected. The goal of the attacks was extortion, he said.

"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands," he said in a [statement](#) posted to the Web on Friday by the conference's organizers, the SANS Institute. "In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

"According to Mr. Donahue, the CIA actively and thoroughly considered the benefits and risks of making this information public, and came down on the side of disclosure," SANS said in the statement.

One conference attendee said the disclosure came as news to many of the government and industry security professionals in attendance. "It appeared that there were a lot of people who didn't know this already," said the attendee, who asked not to be identified because he is not authorized to speak with the press.

He confirmed SANS' report of the talk. "There were apparently a couple of incidents where extortionists cut off power to several cities using some sort of attack on the power grid, and it does not appear to be a physical attack," he said.

Hacking the power grid made front-page headlines in September when CNN aired a video showing an Idaho National Laboratory demonstration of a software attack on the computer system used to control a power generator. In the demonstration, the smoking generator was rendered inoperable.

The U.S. is taking steps to lock down the computers that manage its power systems, however.

On Thursday, the Federal Energy Regulatory Commission (FERC) approved [new mandatory standards](#) designed to improve cybersecurity.

CIA representatives could not be reached immediately for comment.

## Most malware comes from legit sites, says researcher

### 51% of sites spreading malicious code have been hacked

**Gregg Keizer**

**January 23, 2008** ([Computerworld](#)) -- The majority of Web sites serving up attack code are legitimate domains that have been hacked by criminals, a security researcher said in a report released today. It's the first time that legitimate sites outnumber the malicious ones hackers purposefully set up to spread malware.

According to data compiled by [Websense Inc.](#), 51% of the sites it classified as malicious in the second half of 2007 had been compromised and then seeded with attack code that infected unpatched machines visiting the URLs. The remaining 49% were "intentionally built for malicious intent," the Websense report said.

Hacking legitimate sites to make them sling malware gives attackers instant advantages, added Dan Hubbard, Websense's vice president of security research. "It's a great vector because they don't need to drive users to the sites in many cases; they also get free hosting, of course, and [it's] hard to trace ownership," Hubbard said. "Additionally, if someone is allowing access based on reputation, then they may go undetected."

The win-win for hackers -- who get a crack at the built-in audience that's composed of a hacked site's usual visitors -- is a lose-lose for everyone else, a fact that's been proved by several prominent events where hacked sites spewed out malicious code.

A year ago, for example, the Web sites of [Dolphin Stadium](#) and the [Miami Dolphins NFL](#) team, host to Super Bowl XLI, were hacked so that they served visitors with malicious JavaScript that, in turn, tried to load a Trojan onto unpatched PCs.

Then in August 2007, the [Bank of India](#), one of that country's largest banks, was also found hosting attack code after being hacked. Later, criminals associated with the notorious Russian Business Network, a St. Petersburg-based malware and hacking hosting network, were implicated in the [Bank of India](#) compromise.

The trend is accelerating, said Hubbard, who noted that the last report estimated that the share of malicious sites that were actually hacked legitimate domains was in the mid-30% range. In fact, a pair of recent mass hacks -- one that compromised [upward of 90,000 sites](#) and another at [least 10,000](#) -- demonstrated the extent of the problem.

Hubbard echoed that with an estimate of the number of sites serving up attack code. "Counting sites can be a tricky game [because] there are sometimes entire domains we classify that have thousands of pages," he said. "However, it's safe to say that at any given time, we have more than 2.5 million in the malicious categories."

Sites are hacked in a variety of ways, said Hubbard, who noted that there is no one method that stands out. "[Compromises are] all over the place, unfortunately, [including] miss-configurations, no patches and so on."

A significant number of the sites, however, are compromised by the multi-exploit tool kits made infamous by Mpack and Neosploit. Websense estimates that 19%, or about one in five, of malicious sites were created or compromised using such tool kits.

"Exploit tool kits are being utilized more than ever," Hubbard said. "This can be a sign of increased sharing or increased numbers of sites that the same groups are attacking and infecting successfully."

## Endpoint Security: How to Control USB Devices

Shopping for stronger USB port control? Some criteria to consider when it's time to rein in thumb drives and other pesky critters

By Rick Cook

USB ports are a fact of life in modern IT--which means they are also a headache for every IT manager.

"You've got to live with USB ports, and you've got to secure them," says Ari Tammam, VP of alliances at Promisec, a maker of endpoint control software. "I don't think you can get away with blocking them for everyone."

The USB port control native to Windows XP and Windows Server 2003 is extremely limited. You can disable ports or render them read-only, but finer control over allowed devices or file types is lacking. However, there are a number of third-party applications that give you control over your USB ports with varying degrees of granularity.

One of the features of the USB hardware specification is that each device tells the system what kind of device it is as part of the connection process. Some manufacturers take advantage of this to let you block specific kinds of devices on specific ports. For instance, you might opt to allow a USB mouse on any port, but never allow thumb drives. But remember, the principle of least privilege applies with a vengeance to USB ports. Generally, the question shouldn't be "what do you want to block?"; it's "what do you want to allow?"

Some manufacturers go much further with the controls they allow, and let you require "a specific device with a specific serial number linked to a specific user" to use a particular port, says Gil Sever, CEO of the endpoint security tools manufacturer Safend. You might also mark certain devices as read-only or specify which kinds of files can be read and written through a given USB port. This helps prevent two security risks: someone loading rogue programs into the system through the port, or someone taking out unauthorized kinds of data. For example, a user may be authorized to download Excel (.xls) or Word (.doc) files, but not database files.

Some products also block USB ports at the OS level--that is, they become part of the connection process and won't allow specific kinds of devices to connect on any port on the network. Others will only allow certain specific devices while blocking other devices of that class. Thus the user can download files to, say, the disk drive in her laptop, but to no other USB disk drive. Alternately, you could set things up such that only a thumb drive encrypted with corporate-approved encryption and registered to a specific user could be allowed.

When shopping for a USB protector, the major things to look for are ease of management and granularity. Because a typical network will have thousands of USB ports, you probably want to be able to manage all of them in a single central location. Ideally, you'll want something that allows you to manage the ports on a Windows network through the group policy feature or something equally seamless. A few products have the ability to manage the ports on all the networks in the enterprise rather than having to manage each network separately.

Of course USB port control isn't the be-all and end-all of security, nor can you absolutely guarantee that data can't be leaked out USB ports. But then that's true of any other endpoint in the network as well. The point is to do what you can to mitigate the risks of these pesky but oftentimes useful devices.

## "IP Addresses Are Personal Data, E.U. Regulator Says"

Associated Press (01/22/08) ; White, Aoife

Internet protocol addresses are personal information, according to the head of the European Union's data privacy regulators. German data-protection commissioner Peter Scharr told the European Parliament that if an Internet user is identified by an IP address, then it must be considered personal data. This view differs from Google, which argues that an IP address identifies the location of a computer, not the identity of the user. Many people consistently use the same computer, which generates the same IP address, a factor that has resulted in the creation of many "Whois" Web sites. These sites allow users to find out the person or company who is linked to a certain IP address. If the EU decides to mandate that IP addresses be considered personal information, it would change the way search engines record data. Google stores search data for up to 18 months, taking the last two numbers off of the stored IP address. This makes the address part of a geographic group, instead of a representation of an individual user. Google stores user's search information in an effort to improve its regional search results and to prove to advertisers that they are not being deceived by "click fraud." Microsoft does not store user IP addresses, instead hoping that users will log into the Passport network that is featured on Hotmail and Windows Live Messenger. Arteni Rallo Lombarte, Spain's data protection regulator, criticized both companies for not clearly stating their privacy policies on their home pages.

## "Desktop Security Eases Into Place"

Federal Computer Week (01/21/08) ; Miller, Jason

Government officials predict most federal agencies will meet the Feb. 1 compliance deadline for new security protocols mandated by the Office of Management and Budget and the National Institute of Standards and Technology. All agencies must finish the Federal Desktop Core Configuration (FDCC) or show improvement by the deadline, and by March 31 agencies must have Secure Content Automation Protocol (SCAP) tools from NIST. Federal offices that do not use SCAP tools have a greater risk of a security breach, but experts say the configurations could still be checked manually by an IT security expert. Many agencies find FDCC less laborious than expected, and officials are pleased the new security protocols do not prevent important applications from running on desktop computers. "There is a risk for agencies that use nonvalidated tools," says Peter Mell, who leads NIST's SCAP project. "They can either accept the risk or manually check the configurations."

## Bush Grants Intelligence Agencies Authority to Monitor Government Computer Systems

January 26, 2008

A classified presidential directive signed earlier this month reportedly gives US intelligence agencies the power to monitor computer networks at all federal agencies. The move is believed to be a response to increasing attacks against government networks. A task force "will coordinate efforts to identify the source of cyber-attacks against government systems." The Department of Homeland Security (DHS) will focus on protecting networks, while the Pentagon will turn its attention toward developing counterattack strategies. The new initiative has met with some concerns. According to the chairman of the House Homeland Security Committee, Rep. Bennie Thompson (D-Miss.), "Agencies designed to gather intelligence on foreign entities should not be in charge of monitoring our computer systems here at home." Others have pointed out that the exclusion of the private sector from the program ignores an important source of cyber attack data.

## Erased' personal data on agency tapes can be retrieved, company says

(Govexec.com, 1/23/08)

Personal and sensitive government data -- including employees' personal data -- on magnetic tapes that federal agencies erase and later sell can be retrieved using simple technology, according to an investigation conducted by a storage tape manufacturer. The findings contradict a report released by the Government Accountability Office last year that concluded such data was irretrievable.

From March through August 2007, GAO investigated if data could be retrieved from used magnetic tapes that federal agencies sell to commercial tape companies in the United States. Magnetic tapes are widely used by federal agencies, particularly for backing up data stored on large systems in the event of a disaster or system failure. The sample of tapes that GAO obtained came from such agencies as the Federal Reserve Bank, the Air Force and the National Oceanic and Atmospheric Administration.

## Forgotten IT chores may have led to bank meltdown

By Jeremy Kirk

---

February 5, 2008 (IDG News Service) The huge losses reported by French bank Société Générale, apparently caused by a rogue trader with inside knowledge of the bank's procedures, don't necessarily point to an IT systems failure but rather to poor management of those systems, analysts say.

The bank has accused 31-year-old employee Jerome Kerviel of creating a fraudulent trading position in the bank's computers that ultimately caused it to lose around \$7.3 billion.

Kerviel achieved this by, among other things, misappropriating computer passwords, the bank said. It has revealed few other technical details of what caused the losses.

Management of passwords, including rescinding the old passwords of employees who move to different positions within the bank, or modifying the level of access those passwords allow, is often a task given to the lowest-level IT worker.

"It's dull and routine 99 percent of the time, but a vital backstop," said Bob McDowall, senior analyst at the [TowerGroup](#). Senior IT managers should conduct more frequent reviews of password policies, he said.

In some cases, it may not have been the security of the passwords themselves that posed a problem, but rather the access those passwords allowed, said Ian Walden, professor of information and communications law at Queen Mary, University of London.

Organizations tend to think of access as being binary in nature: you get access to it all, or you don't, Walden said. In reality, there are many more levels of access. "In modern, complicated systems, the granularity has to be much more sophisticated."

To make the best use of systems with advanced access controls, the IT department must have a thorough understanding of how the business works and where there is risk.

IT departments and business managers have yet to find a way to wrap security into business processes so it is not an impediment, Walden said.

"IT in a company is not given a sufficient status," Walden said. "What's shocking is you would have thought that the financial sector was more sophisticated than this, but it still tends to be the case that security is an add-on and a block, something you've got to live with but you don't have to like, rather than being viewed as an integral part of the business structure."

Workers should be able to do their job without having to share passwords when someone goes on holiday, and the IT department should not make it harder for people to perform their duties, Walden said.

In one extreme example at telecommunications company BT, one employee didn't have the right to use a computer at all, but he found it helped him do his job, Walden said.

"By the time he was found, he had 90 passwords of different employees," Walden said.

It's possible that financial institutions could use biometric systems, such as fingerprint scanners, to provide an added layer of security, McDowall said. Those systems, however, are expensive. Also, the sometimes-finicky fingerprint scanners may not be appropriate in a frantic trading environment, McDowall said.

Questions remain about how Kerviel's losses could be so high given his job as relatively low-level trader. But Kerviel's career progression in 2005 from the bank's back office to the front office -- where he would have had access to client accounts -- is also troubling, since he would have gained greater knowledge on the bank's inner controls, McDowall said.

As an arbitrage trader, Kerviel made money off price differences between different financial products. Société Générale said Kerviel balanced real and fake trades in order to avoid setting off internal alarms.

Kerviel has been described in some press reports as a computer genius. However, most attackers used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes and procedures, according to the 2005 "Insider Threat Study" by [Carnegie Mellon](#) Software Engineering Institute.

That report notes that sophisticated tools are also used in some attacks, which would demand that internal financial systems need to be designed on a more defensive footing.

Programmers should code under the assumption that a hacker or employee will use every means in order to break in, said Ben Rothke, senior security consultant at BT's International Network Services.

"The underlying issue is that many systems are designed to stop honest people from making mistakes, but do not take into account those with malicious intent," Rothke said.

It makes insider jobs one of the toughest to defend against. The psychological profile of an insider tends to be a disgruntled employee who feels wronged by the company, according to the Insider Threat Report.

That in turn can lead to a suspicious behavior such as staying late at work, which paradoxically might only signal a committed employee.

"It's always the insider," Rothke said. "It's often harder to steal \$10,000 from a bank than \$10 million."

## **Proposed Law in CA Clarifies Breach Notification Rules** (February 4, 2008)

A bill passed by the California State Senate details how government agencies and other organizations should notify consumers when their personal data have been compromised in a security breach. The bill requires that the notices be clear about exactly what happened, when it happened, the number of people affected by the breach, what information was exposed, and steps people can take to protect themselves from fraud.

They would also be required to provide toll-free phone numbers for credit bureaus. The state already has a breach notification law in place; this bill clarifies the responsibilities of the organization whose systems were breached.

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=206103872>

## **CA Bill Would Allow Local Prosecution for ID Fraud** (February 1, 2008)

California state legislators have passed another bill related to data theft. It allows identity theft cases to be prosecuted in the victim's county of residence; current law allows for prosecution in the county where the data were stolen or where the fraud occurred. Sponsors of the bill say the current configuration favors the criminals; the proposed change would allow a judge to decide where the trial should take place.

<http://cbs5.com/local/identity.theft.bill.2.644169.html>

