

Security Trends Report

08/08

Bill would require more privacy officers

By Michael Hardy

July 15, 2008

A bill under consideration in the House of Representatives, H.R. 5170, would require a privacy officer in each of the Homeland Security Department's components. The legislation seeks to strengthen DHS's privacy protection efforts.

The Homeland Security Committee approved the bill in late June and sent it to the full House.

DHS has nine components, and four have full-time privacy officers, according to the bill co-sponsored by Reps. Christopher Carney (D-Pa.) and Bennie Thompson (D-Miss.).

Although the department's chief privacy officer works closely with appropriate offices in DHS, the divisions of DHS that have full-time privacy officers generate more Privacy Impact Assessments, according to the text of the bill. Of the 11 components that have generated any PIAs, the three that have designated privacy officers account for 57 percent of the total.

"The presence of a full-time Component Privacy Officer would ensure that privacy considerations are integrated into the decision-making process at all of the DHS Components," the measure's authors wrote.

Hidden Endpoints: Mitigating the Threat of Non-Traditional Network Devices

SearchSecurity.com (07/03/08) ; Kadrich, Mark

The proliferation of IP-enabled devices and bridges represents a significant security threat to enterprise networks because these devices are equipped with few security safeguards and there is little awareness about the security issues surrounding them. One such device that could open up an enterprise network to attack is an IP printer. By using one of the printer's onboard interfaces, including HTTP and telnet, a hacker can set the printer's IP address to the gateway or DNS server, thereby opening the network up to a denial-of-service attack. Compounding the problem is the fact that default passwords on these printers rarely get changed because few security administrators consider IP printers to be a security risk. Another potentially risky device to have on an enterprise network is an IP-based security camera. These devices have built-in Web servers that allow anyone to access video from anywhere on the network. Unfortunately, this feature also allows criminals to see when a company's offices are empty and safe to rob. However, IT security professionals can take several steps to protect their company from the threats posed by such devices, including developing an enterprise security policy that spells out how non-IT controlled devices can and cannot use the network. In addition, IT security professionals should be sure to change the default passwords on network-enabled devices and ensure that unused protocols are disabled so that there are not several different ways to reconfigure the devices.

Hard Lesson in Google Data Breach

InternetNews.com (07/08/08) ; Patrizio, Andy

The Internet search behemoth Google suffered a major data breach because a third-party vendor it once worked with did not have adequate security protections on its computers. On May 26, the Colt Express Outsourcing Office in Walnut Creek, Calif., was robbed of several PCs containing the names, addresses, and Social Security numbers of Google employees. Even though Google ended its contract with Colt on Dec. 31, 2005, the outsource firm still had information on all employees hired before Jan. 1, 2006. Since the PCs are unencrypted, the thieves need only to plug the computers in and turn them on in order to access the files, which contain enough personal data to start a fraudulent credit card account under someone else's name. Gartner security

analyst Avivah Litan thinks the attack could have been deliberate, and this makes it more likely that the personal information will be abused. "The takeaway here is that a lot of companies think that in outsourcing their data processing or storage, you're off the hook or the scope of your security efforts is greatly reduced," says Litan in regards to Google. "What they don't do is due diligence on their outsourced service provider."

Structure of Cybercrime Gangs Unlocked

The chain-of-command of a cybercrime gang is not unlike the Mafia, an evolution that shows how online crime is becoming a broad, well-organized endeavor

By Jeremy Kirk, IDG News Service (London Bureau)

July 15, 2008 —

The chain of command of a cybercrime gang is not unlike the Mafia, an evolution that shows how online crime is becoming a broad, well-organized endeavor.

The [latest research from Web security company Finjan](#), released on Tuesday, outlines a pyramid of hackers, data sellers, managers and malicious programmers, all working in a fluid management structure in order to profit from cybercrime.

Finjan researchers joined forums where credit card details and other data is sold, known as "carding sites." They impersonated interested data buyers while collecting intelligence on the operations' management hierarchy, said [Yuval Ben-Itzhak](#), Finjan's CTO.

"We kind of had a feeling that something had changed there," Ben-Itzhak said. "There is something even more organized there."

When a person's credit card details are stolen, the details are sold on the carding Web sites, where salespeople offer a menu of available information. Those salespeople don't exploit the data they possess but rather seek to sell it to someone who does. Those salespeople also aren't responsible for the hacking.

The data is supplied by affiliate networks, or groups of hackers who get paid to infect machines with malicious software and steal data. Those networks often have a campaign manager, someone who oversees a particular set of attacks.

At the top of the hierarchy are the boss and his deputy, who handle the distribution of crimeware kits used for hacking. The boss doesn't engage in hacking and acts as an administrator for all of the activity.

Finjan's map of the cybercrime gang comes from chatting with data sellers on ICQ and asking them where the data originates, Ben-Itzhak said. ICQ was one of the first instant messaging programs. Participants are often only know by a number.

"We managed to build up trust," Ben-Itzhak said. "Of course, they don't know we are from Finjan."

Sellers offered "dumps" or batches of credit card numbers: [MasterCard](#) Standard and Visa Classic card numbers and security codes go for \$15 each, with Visa Gold or Corporate details going for up to \$90.

Data often comes with a guarantee, with many data sellers offering to replace cards that don't work or are reported as stolen. But Finjan and other security vendors have said that the price of a credit card number has been falling as the market as the amount of sensitive data on the market has increased.

Finjan broke off contact with the data sellers and hasn't reported it to the authorities, although Finjan does report if researchers come across servers where the stolen data is stored, as the company revealed last month.

The company doesn't have much of an idea where the cybercriminals are physically located. The touch-and-go game on instant messenger is one way to gain intelligence: "It's really about knowing your enemy," Ben-Itzhak said.

Momentum builds for U.S. privacy policy

But passage of a privacy law is unlikely until 2009

By Grant Gross

July 22, 2008 (IDG News Service) Privacy advocates in Washington have been busy in recent months.

Groups such as the [Center for Democracy and Technology](#) (CDT), the [Center for Digital Democracy](#) (CDD) and the Electronic Privacy Information Center (EPIC) have sounded alarms on several privacy-related issues before the U.S. Congress and federal agencies.

CDT, more recently joined by [Microsoft Corp.](#) and [Google Inc.](#), has long pushed Congress to pass comprehensive privacy legislation that would set the ground rules for businesses that handle personal information. Several lawmakers have recently called for a broad privacy law.

Rep. Joe Barton (R-Texas) complained about targeted advertising campaigns during a speech at a forum on Internet privacy earlier this month. Although there have been recent privacy complaints about a targeted ad service offered by [NebuAd Inc.](#), other online ad networks put cookies on computers without telling the owners, he said.

"Nobody in the world has a right to know anything about me unless I let them," Barton said.

No one expects Congress to pass a major privacy bill this year -- passing major legislation is difficult in the months approaching a national election, and a comprehensive privacy bill hasn't even been introduced. But several privacy advocates say momentum for a new privacy law seems to be building, with a real push likely in 2009.

"There is a perfect privacy legislation storm developing that should propel a bill in the next Congress," said Jeffrey Chester, CDD's executive director.

Among the privacy issues debated recently in Washington:

- Privacy groups, including CDD and EPIC, raised concerns about Google's late 2007 acquisition of DoubleClick Inc.'s online advertising network, and some have also questioned the privacy implications of Google's recent advertising deal with rival Yahoo Inc.
- Privacy groups and some lawmakers have protested experiments by a handful of broadband providers to use a targeted ad service from NebuAd. The NebuAd service tracks the Web habits of broadband users in an effort to deliver more relevant ads, but during the past couple of months, privacy groups have complained that NebuAd uses common Internet attacks to track users and that some broadband providers didn't notify their customers.
- Congress debated and passed an extension to a controversial National Security Agency (NSA) surveillance program that targets suspected terrorists and people communicating with them. The new surveillance law, given final approval this month, provides some additional court oversight to the NSA program, but it also will likely give legal immunity to telecommunications carriers that participated in the program while it was not under court oversight. The American Civil Liberties Union (ACLU) is [challenging the measure](#) in court.
- And several other privacy-related questions were placed before Congress: how to ensure privacy of electronic health records, whether to require private companies to report data breaches to customers whose personal information has been compromised, and how to improve the cybersecurity of government agencies.

A series of data breaches reported in early 2005 created a push for a data breach notification law, but Congress has failed to pass legislation. However, the controversy over broadband providers, including Charter Communications Inc., testing NebuAd's targeted ad service has brought privacy issues back to the forefront.

During a hearing last week, several lawmakers questioned NebuAd Chairman and CEO Robert Dykes about why the company requires broadband customers to opt out of having their Web habits tracked instead of taking an approach in which they opt in to the targeted ad service.

The NebuAd controversy has helped create a push for new privacy legislation, CDD's Chester said. In addition to the privacy issues, the NebuAd service stirred up concerns from advocates of network neutrality, who don't want broadband providers interfering with Web content.

"The bungled attempt by Charter ... to get into the online ad business has created a serious new layer of opposition to online marketing and data collection," he said. "One aspect of the online ad business -- ISP monitoring -- has helped potentially create a bipartisan coalition to pass some form of legislation. Ironically, we now may be able to set a standard for a bill where opt-in becomes the rule for all -- not just for ISPs."

During two hearings this month, Dykes defended NebuAd's service, saying it does not collect personal data that can be linked to specific users. NebuAd also anonymizes the information it collects, and not even the U.S. government could get access to that data, he said.

Dykes, [facing questions from lawmakers last week](#), wouldn't commit to changing his service to opt-in. Instead of opt-in permission, "it's much more important that the consumer is well-informed," he said.

But Dykes seemed to embrace a comprehensive privacy law when he called for a "consistent" set of laws governing how businesses should handle personal information. "I don't think one set of companies should be penalized," he said.

Representatives of Microsoft and Google repeated their calls for a broad new privacy law. Microsoft has been pushing for one since 2005, but too often, Congress has focused on narrow issues, such as spyware, breach notification or health records, said Mike Hintze, associate general counsel at Microsoft, in an interview.

"More and more companies have sort of come to the realization that there's ... a lot of regulation out there, but it's fractured and inconsistent," he said. "Traditional lines of industries are merging and converging, and that overlapping legislation, as a result, is very unclear how it applies to new business models and new technologies."

Chester suggested that Google and Microsoft may be trying to outposition each other in the privacy debate. "Google wants privacy legislation because it's a real headache for them politically," he said. "But I believe they wish to see a relatively weak bill enacted which creates an opt-out regime and forecloses on stronger state action. Microsoft sees a potential competitive advantage in being the better-privacy-than-Google company."

Pablo Chavez, senior policy counsel at Google, disputed Chester's reading of the privacy debate. Google has called for legislation that would create strong penalties for companies that violate privacy laws, he said in an interview.

"What we're looking for is a national standard that provides uniform protections for consumers across the country," Chavez said.

But when asked whether all online companies should get opt-in permission before they collect personal data, Chavez said there's a difference between the NebuAd model and many other sites or ad networks that collect personal data. While NebuAd intercepts broadband subscribers' Web surfing habits, many other sites follow generally accepted ways of collecting data, he said.

A strong, clear policy allowing Web users to opt out of data collection is "appropriate for third-party advertising," Chavez said.

Beyond the debate about opt-in versus opt-out, there are a lot of issues that need to be worked out before Congress can pass comprehensive privacy legislation, said Brock Meeks, communications director at CDT.

Several industries, including the financial sector, have raised concerns about how a new privacy law would affect them, he said in an e-mail interview.

"We still face a high hurdle," Meeks said. "Although a good group of corporations have agreed in principle that a baseline privacy bill is needed, there isn't much agreement on how that type of legislation should be crafted. It's a tremendously complex issue -- a lot of moving parts. We may have succeeded in getting all those pieces into one box, but we're a long way from putting that puzzle together."

Biggest security threats are from inside: survey

Data shows companies more confident warding off external attacks

By [Denise Dubie](#) , Network World , 07/17/2008

The 1979 film "When a Stranger Calls" portrayed the terror-filled night of a young woman fielding prank and increasingly threatening calls that climaxed when the police determined "the calls are coming from inside the house." Today [IT security](#) executives experience a similar chill down their spine when they realize the biggest threat they face comes from [internal security attacks](#) and data breaches.

A recent survey conducted by The Strategic Counsel and commissioned by management and [security software vendor CA](#) showed that a majority of CIOs, [CSOs](#), CTOs and other senior IT security executives consider security threats from within an organization a bigger threat to business than external attacks. The results revealed that 44% of respondents identified internal breaches as a key security challenge over the past 12 months, compared with 42% in 2006 and 15% in 2003. More than 34% of organizations reported a loss of confidential information as a result of [security attacks and breaches](#), an increase from 22% in the same survey conducted in 2006.

External attacks are decreasing in numbers. According to the report, virus attacks decreased from 68% to 59% in the past 12 months, network attacks went down from 50% to 40% and denial-of-service attacks declined from 40% to 26%.

"The security breaches identified by IT security executives as most concerning are those coming from inside the company," says Lina Liberti, vice president of CA Security Management. "The external threats still exist, but IT security executives feel more confident that they can be quickly addressed, stopped or controlled to some degree. They identified internal security breaches and attacks as those with the biggest severity of consequences."

Internal breaches strike fear in the heart of IT security executives because of the company image blow and customer confidence issues that accompany an attack and that could expose confidential customer data and require [public disclosure](#). Business costs associated with an internal breach include loss of productivity for 61% of survey respondents (up from 52% in 2006). Loss of trust and confidence on the part of the customer also increased to 35% in 2008 from 30% in 2006. And embarrassment on the part of the company suffering the breach grew to 33% this year from 28% in 2006.

"The implications are now tied squarely to dollars and reputation," Liberti says.

Senior IT executives have reason to worry, CA says, because the research also showed that an average of 8% of Americans feel "very confident" in the ability of U.S. retailers, government and banks to protect their personal data. Nearly 80% of the consumer group cited loss of trust and confidence, damage to reputation and reduced customer satisfaction as consequences of security and privacy breaches suffered by the businesses and government agencies with which they deal.

"It makes sense that customer confidence is not high because now more than ever consumers know more about computing, the Internet and the public breaches that companies have experienced," Liberti explains.

Consumers also feel companies could do more to protect their data. According to the survey data, 72% don't think retailers spend enough budget dollars on online security and privacy. Nearly 70% felt the same way about

government agencies and 58% said major financial institutions could do more to protect customers. About one-third of senior IT executives polled agree, saying the investment their company makes in security is inadequate.

"Consumers aren't confident transacting online, and security teams know the threat is ever-changing and that their jobs are never done," Liberti says. "Security executives know they need to continue to spend in this area to help raise consumer confidence."

For the consumer portion of the study, a total of 400 telephone surveys were conducted among a random sample of the U.S. general population aged 18 to 65.

Goodbye to Faulty Software?

ICT Results (07/15/08)

A team of European researchers believes that it will be possible to create software that is guaranteed to be free from bugs. "The software industry is still very immature compared to other branches of engineering," says Chalmers University computer scientist Bengt Nordstrom. Nordstrom believes the entire approach to software design needs to be rethought, replacing the usual approach of validating a program through a lengthy testing process with a design philosophy that guarantees from first principles that a program will act as it should. The key is a reformation of mathematics called type theory based on the notion of computation, in which the specification for a computational task is stated as a mathematical theorem. The program that performs the computation is essentially the proof of the theorem, and by proving the theorem the program is guaranteed to be correct. The European Union has funded a series of projects to develop type theory since 1989. Nordstrom was coordinator of the TYPES project, which supported cooperation on type theory between researchers at 15 European universities and research institutes and 19 associated academic and industrial organizations. TYPES has released several open source programs, including proof editors that, in type theory, are the key to guaranteeing bug-free programs. "This is a very slow process, it takes many years to get ideas from the universities into industry, but I think it's slowly taking place," Nordstrom says.

Privacy: Agencies Struggle to Redact Personal Data From Online Public Documents

Government Technology (07/09/08) Vol. 21, No. 7, P. 22 ; Opsahl, Andy

State and local governments are facing a number of challenges in their efforts to redact citizens' personal data from online public documents such as uniform commercial code (UCC) documents, tax liens, divorce decrees, and death certificates. Among the challenges state and local governments must deal with are the limitations of redaction software, which blacks out the section of the document where the personal information appears. For example, it is difficult for redaction applications--which are only about 98 percent accurate--to remove all of the Social Security numbers in a document because numbers tend to be written in many different places. In some documents, Social Security numbers are written under signatures, while in others they are written in the top right-hand corner so that they can be more easily organized in an office filing system. Another challenge making redaction efforts more difficult, particularly at the local level, is a lack of funding. In Virginia, for example, the state legislature authorized county clerks to redact Social Security numbers last year but did not provide any funding for the effort. That prompted one Virginia county clerk, Fairfax County Circuit Court clerk John Frey, to ask his county's Board of Supervisors for funding for the redaction project--a request that was denied. However, the Board of Supervisors did allow Frey to raise the charge citizens pay to access public documents and use the extra money to fund the project. Frey is planning to move forward with the project, despite his belief that redacting Social Security numbers from the state's 38 million records will do little to reduce identity theft. He notes that governments are forced to address this issue even in the absence of a significant threat because they will be blamed by the public if something does happen.

Privacy Central to New FISMA Guidance

Federal Computer Week (07/17/08) ; Mosquera, Mary

The Office of Management and Budget (OMB) recently published a handbook to help government agencies comply with the Federal Information Security Management Act (FISMA) before Oct. 1, when the reports are due. OMB deputy director for management Clay Johnson advised all agencies to be aware of the updates to security policies and privacy reporting. "It is especially important your agency's report clearly and accurately reflects the overall status of your program and not include conflicting views of, or unresolved differences among, the various parties contributing to the report," said Johnson in a memo attached to the guide. Federal agencies will be asked to detail the steps they are taking to form a breach notification policy, reduce the circulation of personally identifiable information, and curb the leakage of Social Security numbers. Agencies will not be required to include deficiencies in the report, though they must be documented and kept on file. Agencies could choose instead to use a shared service company listed under the Information Security Line of Business to record and track all security vulnerabilities in their Plans of Actions and Milestones.

Privacy group says identity-theft monitoring services may be a waste of money

Many are overpriced and offer protections that can be had for free, PRC claims

By Jaikumar Vijayan

July 29, 2008 (Computerworld) Consumers who sign up for identity-theft monitoring services may be getting a lot less protection against some common types of fraud than they assume they are, according to an [online guide](#) released yesterday by the [Privacy Rights Clearinghouse](#) (PRC).

What's more, many of the services offered by identity-theft monitoring vendors can often be obtained for free, the San Diego-based privacy advocacy group claimed.

The PRC's guide doesn't mention any vendors by name and notes that the available monitoring services "vary tremendously" in what they offer. Even so, many of them are overpriced and don't provide anything close to full protection against identity theft or credit fraud, said [Paul Stephens](#), the PRC's director of policy and advocacy and the author of the guide, which offers tips on selecting monitoring services.

"There is no correlation between the price you pay and the services you get," Stephens said. People who think they need monitoring services should first make sure that there are no free or lower-cost alternatives that they can take advantage of, he added.

Monitoring services are most useful, Stephens said, in helping individuals detect new-account fraud resulting from someone using their name, Social Security number and other personal information to open credit card, mobile phone or other accounts. Often, such fraud is hard to spot until after the fact, according to Stephens. He said that credit monitoring services can quickly alert victims, although the protections can be inadequate if vendors don't monitor credit reports at all three of the major credit reporting bureaus.

In general, monitoring services fail to protect against a variety of other kinds of fraud, Stephens said. For example, they seldom catch the misuse of existing accounts, such as making fraudulent purchases with an existing credit card. Similarly, the services aren't of much use against debit and check card fraud, or in situations where an imposter might use another individual's Social Security number to obtain employment, he claimed.

In addition, they offer no protection against the fraudulent use of personal information for purposes such as obtaining a driver's license or making false claims for medical goods or services, Stephens said.

He also noted that individuals can get some of the protections offered by monitoring services for less than the fees they charge, or for [nothing at all](#). As a case in point, consumers can place free fraud alerts on their credit reports with each of the major reporting bureaus — Equifax Inc., [Experian](#) and TransUnion LLC — for up to 90 days at a time. Stephens said that many identity-theft monitoring services charge up to \$10 per month to place such alerts on behalf of their customers.

For a \$30 fee payable to the credit reporting bureaus, he added, people can also place a lifetime freeze on their credit records — thus requiring credit providers to verify their identities whenever a new account is opened or a credit inquiry is made in their name.

It also pays to fully understand the implications of certain actions offered by identity-theft monitoring services, Stephens said. For example, while a credit freeze can provide fairly strong protections against fraud, it also makes it harder for people to quickly obtain credit.

More than a dozen companies, including each of the credit reporting bureaus, currently offer monitoring services. One of the biggest of them, [LifeLock Inc.](#), was hit earlier this year with [class-action lawsuits](#) in three states, charging the company and [CEO Todd Davis](#) with false advertising and deceptive trade practices.

Several of the issues raised in the lawsuits are similar to the ones mentioned in the PRC's guide. The legal filings basically accuse Tempe, Ariz.-based LifeLock of overstating the capabilities of its identity-theft monitoring and protection service and misleading people about the guarantees that it makes to customers.

In an interview today, Davis said that LifeLock, which charges \$110 for a one-year subscription to its service, makes no attempt to conceal the fact that some of the things it offers to do for customers can be done for free by individuals. For example, a core component of LifeLock's service consists of placing and renewing fraud alerts on behalf of consumers.

But Davis said that in addition to placing such alerts, LifeLock also monitors Internet chat rooms and underground sites for signs that personal data belonging to its customers may have been compromised. The company also works on behalf of its customers to contact credit card companies, credit bureaus, banks and other businesses in the event that their personal data is compromised.

"If you become a victim, we will use our expertise to correct the problem and do everything that the law allows us to do to restore your good name," Davis said.

GAO: Most sensitive data on government laptops still unencrypted

Watchdog agency says only 30% of such info was encrypted as of last September

By Grant Gross

July 29, 2008 (IDG News Service) Despite a series of high-profile data breaches [at federal agencies](#) in recent years, only about 30% of the sensitive information stored on laptops and mobile devices used by federal workers was encrypted as of last September, according to a report issued by the [Government Accountability Office](#).

The GAO, which released the report to the public today ([download PDF](#)), examined the use of encryption technology at 24 major agencies. The federal watchdog defined several types of data as sensitive, including medical records, other personal information, law enforcement records and information deemed to be essential for homeland security purposes.

"While all agencies have initiated efforts to deploy encryption technologies, none had documented comprehensive plans to guide encryption implementation activities," the GAO said in the report. "As a result, federal information may remain at increased risk of unauthorized disclosure, loss, and modification."

The report follows a string of security mishaps involving government-issued laptops. The biggest occurred in May 2006, when the Department of Veterans Affairs reported that a laptop and hard drive containing the personal information of 26.5 million military veterans and active-duty personnel [had been stolen](#) from the home of an agency employee. Law enforcement officers [recovered the hardware](#) the following month, and the VA [began encrypting](#) the data on all of its PCs, handheld devices and smart phones later that year.

But the VA has had plenty of company. Last year, for example, the GAO reported that 490 laptops [were lost or stolen](#) from the [Internal Revenue Service](#) between early 2003 and mid-2006. Many of those laptops likely contained the personal data of U.S. taxpayers, according to a separate report by an auditor at the IRS.

In another example, the Department of Commerce reported in September 2006 that 1,137 of its laptops had been lost or stolen since 2001, with 249 of them containing some personal data.

The GAO's new report notes that several laws, including the [Federal Information Security Management Act](#) of 2002, require agencies to protect their data. In addition, the White House Office of Management and Budget (OMB) first recommended in 2006, then required in May of last year, that agencies encrypt all sensitive data stored on mobile computers.

Following the lead of the VA, federal agencies [have been increasing](#) their encryption efforts. But two members of the House Homeland Security Committee said this week that they're disappointed with the progress being made by agencies, based on the GAO's findings.

"Encryption is not an option, it is a mandate," [Rep. Bennie Thompson \(D-Miss.\)](#) said in a statement. "Unfortunately, I'm not surprised that despite mandates by OMB, the federal government is only 30% of the way there." Thompson, the Homeland Security Committee's chairman, added that investing properly in cybersecurity now "will keep us from paying dearly in the long run."

[Rep. Zoe Lofgren \(D-Calif.\)](#) also released a statement saying that federal agencies "lag far behind the private sector" in protecting and encrypting data. "I'm concerned that our government is not moving fast enough in its efforts to secure its systems and [IT] procedures," she added.

Phil Dunkelberger, CEO of encryption and security tools vendor [PGP Corp.](#), said in an interview that the GAO report and the OMB's encryption mandate both miss the larger need for tighter information security within the federal government. Government officials should focus on broader approaches to cybersecurity, including better protection of data on federal networks, Dunkelberger contended.

"When are we going to get serious about protecting data — role-based and policy-based encryption, not just device encryption?" Dunkelberger asked. He added that the U.S. government has "very well-intentioned mandates to secure data, and yet, the way they've gone about it is kind of a fallacy."

Encrypting end user data is tough to do

By Frank Hayes

August 4, 2008 (Computerworld)

Encryption is hard. Case in point: the U.S. government, which requires its agencies to encrypt all sensitive data on laptops and mobile devices. But according to the [Government Accountability Office](#), as of last year, 70% of such devices didn't encrypt -- and the other 30% weren't in great shape either ([see story](#)).

The GAO just released a report that audited 24 agencies and departments for their mobile encryption implementations. It included trouble spots like the [Department of Veterans Affairs](#), which in 2006 lost a laptop containing the personal information of 26 million vets and military personnel, and the [Commerce Department](#), which has lost more than 1,000 laptops since 2001.

You already know the headline conclusion: At the time of the audit, June to September 2007, more than two-thirds of the mobile devices in these 24 agencies weren't using encryption at all.

But that's not the interesting part. The GAO also found that, in many cases, even the devices believed to be encrypted had problems. Sometimes the encryption wasn't actually installed. Or it wasn't configured correctly. Or

it hadn't been turned on. Often, users hadn't been trained, sensitive information hadn't been inventoried, and crypto key control procedures hadn't been established.

You can read the gory details by downloading the report (it's on the Web at www.gao.gov/new.items/d08525.pdf). The real horror stories start on page 29.

(Predownload quiz: Guess which department hadn't installed encryption on *any* laptops, even though officials insisted that it had? Guess which hotshot technical agency said it had no way of telling whether encryption software had been successfully installed on a laptop? And guess which department's employees never used encryption because no one told them it was installed?)

Even if you don't care about the dirt turned up by the audit, you should download the report. It includes a remarkably readable crib sheet on the different types of encryption for mobile device hard disks (full disk, file, folder, virtual disk), communications (VPNs, digital signatures and certificates) and handheld devices.

It also gives a good rundown of the categories of problems the agencies ran into with their encryption efforts, as well as a table listing the actual volume pricing that government agencies are getting. (One nice non-horror story from the report: The [Department of Agriculture](#) cut its own deal for 180,000 encryption licenses at \$9.63 each, way below even the best government price schedule.)

In short, it's a useful, practical overview of the ups and downs of putting encryption on laptops, portable drives and BlackBerries. And it's based on real-world experience -- even if, for most government agencies, that experience hasn't yet translated into success.

Why do you care? Because encryption is hard. And encryption is coming to portable devices near you. Whether because of regulations, lawsuits or common sense, soon or late you'll be doing this in your IT shop.

The more you learn now about someone else's foul-ups, failures and dead ends, the better you'll be able to avoid them. And as long as your tax dollars are being spent on these mistakes, you might as well get some value from the exercise.

Besides, what other report that you browse this year will tell you how the [State Department](#) dodged its audit: "Although the inventory provided by the agency indicated that the employees were assigned to the location that we visited, they were actually assigned to posts throughout the world."

Embedded Data Continues to be the Gift that Keeps on Giving

by [Michael Overly](#), [Overly on Security](#)

Wed, 2008-07-23 16:35

It seems not a week goes by that we don't hear about yet another instance in which company confidential information is compromised because someone failed to carefully review an Office document (e.g., Word, Excel, and PowerPoint) before disseminating it publicly. The most common problem is failing to remove information contained in embedded comments or available through "track changes." There are many examples. Consider a vendor who sends a pricing proposal to a potential customer. The proposal uses a vendor template. When the customer receives the proposal, it turns on the track changes functionality and is able to see not only the name of the last customer, but also the pricing the vendor proposed to that customer.

In another example, in the midst of a negotiation, a vendor sends its customer a redline of a proposed contract. Unbeknownst to the vendor, the redline also includes confidential comments from its lawyer analyzing the risks of the engagement.

While Microsoft and several third party vendors provide tools for ensuring comments, information contained in tracked changes, and other embedded data are cleansed from documents before they are distributed, few companies use them on a routine basis. Given the threat, businesses should explore deploying such tools and educating their employees on the importance of ensuring their internal/confidential comments and other information are not inadvertently made public in their documents.

Telecommuting poses security, privacy risks

Survey of 73 organizations by Ernst & Young and the Center for Democracy and Technology shows weak security practices in telecommuting

By [Ellen Messmer](#) , Network World , 07/29/2008

Allowing employees to work from home and telecommute poses security and privacy [risks](#) that are not being addressed adequately by business or [government](#), according to a study released today by consulting firm Ernst & Young in partnership with the Washington-based advocacy group [Center for Democracy and Technology](#).

The [report](#), "Risk at Home: Privacy and Security Risks in Telecommuting," surveyed 73 corporate and government organizations to find out whether they had formal telecommuting security policies implemented in practice, and whether employees working from home were trained in [protecting data](#). The report concludes this was too often not the case, putting business and government data at far higher risk than if appropriate security best practices were used in the home telecommuting environment.

"We identified some disconnects about recognizing risk areas and addressing it," said Sagi Leizerov, senior manager with Ernst & Young's advisory services group, about the findings in the report.

Ari Schwartz, vice president and COO at CDT, said the privacy-advocacy group assisted with the study to put the focus on determining what the best practices in telecommuting might actually be.

Schwartz said this question is of growing importance as the practice of telecommuting grows. He pointed out that security breaches have occurred in the context of telecommuting in the past two years, include well-publicized ones at the Department of Veterans Affairs and the National Institutes of Health, as well as at Blue Cross Blue Shield and the state of Ohio.

Neither Ernst & Young nor CDT is opposed to telecommuting, but Schwartz and Leizerov said the report's findings indicate the organizations surveyed often failed to adequately recognize the risks in telecommuting. They said telecommuting doesn't inherently pose more risk than office-based work, but it poses different risks that need to be recognized.

If setting policy is a starting point, organizations are slipping even on that. Only half of the organizations participating in the survey have even developed guidelines for telecommuting or provide guidance to their employees at all.

The survey looked at whether personal computers, portable devices and wireless networks were being used in telecommuting and which security controls were in place for them.

The study also asked how the protection of paper records containing the business information used by telecommuters was being addressed and whether there were security controls, such as file and e-mail encryption.

"About 50% of respondents indicated that telecommuting employees, both full-time and occasional, sometimes use their personally owned computers and PDAs at home for work purposes," the report states, adding that the trend is toward easing restrictions about it.

The security that corporations require for business-issued devices and laptops, however, is seldom applied to employees' personally owned computers.

Security controls regarding the paper documents containing business data that are generated by telecommuting employees working at home also is somewhat weak, the study indicated.

"One-third of the organizations surveyed said they provide telecommuters with shredders for disposal," the report notes. "Roughly the same percentage said they have telecommuters shred paper records, but the employees must arrange their own shredders. And 17% of the organizations indicated they have no disposal requirement for paper records," the report continues.

Leizerov called this unacceptable for a telecommuting environment, saying, "Organizations shouldn't expect employees to purchase their own controls."

The survey, which encompassed organizations in the United States, Canada and Europe, sought to differentiate between employees who work full-time from home and those who occasionally telecommute.

Ten industries were identified, with financial services and healthcare representing 40% of the respondents. The remainder included business and professional services, manufacturing, retail, telecommunications, hospitality, and a "miscellaneous" category for those not fitting neatly into the defined industries.

Among some organizations that responded to the survey, "nearly all employees are occasional telecommuters" and "many respondents found it difficult to estimate the number of their full-time and occasional telecommuters -- an interesting finding on its own," according to the report.

The number of full-time telecommuters, however, is significantly smaller than the number of occasional telecommuters, the study concluded.

"While occasional telecommuters exist at each of the responding organizations, 46 of the 73 respondents employ full-time telecommuters," the report states.

As far as securing hardware, the report states that 85% of organizations indicated they implement at least one of five methods for protecting hardware assets: failed-logon lockout settings on computers, privacy screens, security cables for locking down computers, periodic audits of telecommuters' physical working environments and a "clean-desk policy for telecommuters."

About 20% of the organizations said they conduct periodic inspections of telecommuter remote-work environments, with the frequency rate higher among organizations with greater numbers of telecommuters.

The study noted that stronger security controls, such as biometric authentication and thin-client terminals, have yet to take hold in the telecommuting environment.

"On a more positive note, the use of encryption, while not yet prevalent, is common on hard drives, in securing network connections and even in protecting e-mail messages," the report states.

When it comes to portable devices, wireless networks and Internet downloads, however, the survey found security practices were "often lacking and could lead to the compromise of the personal information that employees handle at home."

More than 70% of the organizations participating in the survey responded that they do some monitoring of telecommuters, most commonly by network monitoring or telecommuter e-mail and Internet use, the report states.

"Based on the results of this survey, many organizations today are not effectively managing the risks to personal information presented by the telecommuting workforce," the report concludes, adding, "Work-from-home arrangements are the next frontier for many companies, and the challenges they pose to privacy and security should be approached with appropriate rigor and resources."

'PhishMe' Tool Lets Businesses Spear-Phish Themselves

Web-based service generates self-inflicted targeted attacks to enlighten users, assess risk

JULY 22, 2008 | A new do-it-yourself phishing tool lets enterprises automatically spear-phish their own users.

The new PhishMe software-as-a-service offering is designed to help companies assess their vulnerability to

spear phishing, as well as to give their users a real-world taste of these targeted attacks.

Boutique security firm [Intrepidus Group](#), which is made up of some black hat researchers, today rolled out the new Web-based [PhishMe](#) service for helping companies find the weakest links in their targeted phishing defense.

Spear phishing attacks target specific organizations or individuals, rather than blanketing large groups of users. A recent report from iDefense Labs found that over 15,000 corporate victims in the past 15 months have been hit by spear phishing attacks.

The concept of unleashing a fake phishing campaign inside your own organization isn't new -- some companies routinely hire penetration testers or social engineering experts to do the dirty work for them. PhishMe is basically a way to roll your own internal campaign and to collect metrics on how users reacted to the messages.

Rohyt Belani, CEO of Intrepidus, says PhishMe is a spinoff of a service Intrepidus performs for its security clients. "This [PhishMe] is a more scalable solution that can be run across various clients, and it's cheaper to buy a license from us," he says. The service ranges from \$5,000 to under \$50,000 for a one-year license, and Intrepidus runs all the background Web and email servers on its end.

PhishMe is also a gentler way of catching employees falling for a phish. Rather than making them feel punk'd, like some social engineering exploits do, it gives them instant feedback: They are redirected to educational messages and information, including a PhishMe educational comic strip and links to their corporate sites for more information.

"The most important part is that as soon as an employee falls for the simulated phishing attack, they get immediate feedback, training materials... on their screen, telling them this is what it was," Belani says. "It's not just 'we did this to you, tricked you, and had fun at your expense.'"

Security experts say the hands-on attack approach is more powerful than a security policy statement or traditional user training. "I think it's one of the simplest and most effective ways at educating [users]," says Robert Hansen (aka "RSnake"), CEO of SecTheory. "I've never thought just telling them what to watch for works.

"This forces them to look at it, and pay attention," Hansen says. "It's far more real and easy to understand when it's staring you in the face in your inbox."

Setting up an attack takes just a few minutes, and PhishMe provides user behavior metrics as well as other trend information. For security reasons, Intrepidus doesn't collect its clients' user passwords on its servers. "The only thing we have is the email addresses of our clients," says Aaron Higby, CTO of Intrepidus.

PhishMe can be configured for any type of phishing exploit, even the more obviously phony ones that aren't targeted at any particular organization or person.

But spear phishing campaigns are usually the most difficult phishing attacks to detect, experts say. "They are hard to pick up because they are so close to legitimate emails out there," Belani says. "You need to train people to focus on the targeted phishing attacks."

The next version of the service will have options for including benign infected-email attachments, Belani says.

Mid-year security report: Web sites, open source, social networking at risk

IBM, Websense issue semi-annual report findings; SQL injection attacks made their mark

By [Ellen Messmer](#) , Network World , 07/29/2008

[IBM](#) and Websense are separately issuing their semiannual security trend reports this week, and the picture isn't pretty for Web sites, [open source software](#) and social networking programs.

The IBM Internet Security Systems ["Midyear Trend Statistics" report](#) tracked 3,534 disclosed vulnerabilities in software for the first half of the year, a 5% increase from the first half of 2007. When it comes to the Top Ten worst offenders in terms of vulnerabilities, big players like [IBM](#), [Microsoft](#), [Apple](#), [Sun](#), [Cisco](#) and [Oracle](#) continue to make the list. But this time they are joined by names in the open source software community: Joomla!, [Drupal](#), [WordPress](#) and Linux.

"IBM makes a lot of software, and companies that make a lot of software are subject to more disclosures," says Tom Cross, X-Force researcher at IBM ISS, by way of explaining why IBM and other software giants make the Top Ten disclosures list.

But this is the first time that community-developed open source software such as the Drupal and [Joomla!](#) content-management software packages for the Web also showed up on the list.

Drupal and Joomla! are open source packages that "have both been vulnerable to SQL injection attacks," Cross says.

The first half of this year will be remembered far and wide for SQL injection attacks. A massive series of such attacks struck [earlier this year](#) across the Internet, hitting Web sites based on Microsoft's Internet Information Server.

Vulnerabilities in both proprietary and open source software has led to a spike in SQL injection as well as cross-site scripting attacks that allow perpetrators to compromise Web servers, loading them up with malicious code for their own designs.

According to the Websense "State of Internet Security Q1-Q2" report, the situation regarding compromised Web sites is becoming dire.

"Sixty percent of the of 100 most-popular Web sites have been hosting malicious code or inadvertently distributing it," says Stephan Chenette, manager of the Websense Security Labs, adding, "75% of malicious Web sites in general are actually legitimate Web sites that are compromised." That's a huge jump from last year when Websense surmised that number stood at 51%.

Some popular Web sites inadvertently hosting malicious code during the last half include CNET.com, MSNBC.com and News.com, Chenette says. "We've seen malicious code on Yahoo.com, Excite.com and perl.com, which is popular with developers. We've seen banner ads, which can be purchased on Yahoo, used for malicious code."

Blog sites, such as [Google](#) blogspot, have become popular spots to post malware, and social-networking sites Facebook, MySpace and YouTube have been tarnished by postings of malicious content as well. This first half of 2008 saw spammers develop tools for beating the CAPTCHA Web security mechanism to prevent automated posting of content, Websense states in its report.

Another disturbing trend, according to IBM ISS, is that exploit code for vulnerable software is being publicly disclosed more frequently than it was in the past.

According to IBM, 95% of all browser-related online exploits occurred within 24 hours of official vulnerability disclosure. Though some researchers differ on the matter, IBM ISS says it does not favor publishing exploit code for discovered vulnerabilities because it can accelerate criminal activity.

Perhaps the only good news to be found in security in the first half of this year, according to both IBM and Websense, is that [image spam](#), a huge problem last year, has declined significantly and the size of spam e-mail has gone down.

"It appears the filters are working," Cross says, noting that about 90% of spam is now URL spam, forcing spammers "to go back to basics."

Gartner: Security through the cloud will triple by 2013

Analysts say revenue of messaging security tools, such as anti-malware and anti-spam services, through cloud delivery model will jump to 60 percent in five years

By Computerworld UK staff
July 16, 2008

Security applications delivered as cloud-based services will more than triple by 2013, according to Gartner.

The firm said 20 percent of the revenue of messaging security tools, such as anti-malware and anti-spam services for e-mail and instant messaging, currently comes through the cloud delivery model. But this will jump to 60 percent by 2013.

Popular on-demand enterprise applications, such as those provided by Salesforce.com, are allowing mobile workers to bypass the corporate network to access business data. Gartner said this will force security teams to put controls between mobile workers and cloud based services.

"Although perimeter security controls will be required to protect the remaining data center functions and the large portions of enterprise populations that are not mobile, new approaches will be needed to secure cloud-based IT services," John Pescatore, vice president and Gartner analyst said in a statement.

"One answer will be cloud-enabled security 'proxies' whereby all access to approved cloud-based IT services will be required to flow through cloud-based security services that enforce authentication, data loss prevention, intrusion prevention, network access control, vulnerability management and so on," he said.

Gartner defines cloud computing as a type of computing where IT-related capabilities are provided as a service using Internet technologies to multiple external customers. This delivery model is getting closer towards widespread acceptance, according to Gartner, because it allows enterprises to gain security services such as distributed denial-of-service attack (DDoS) protection without huge capital investments.

But, Pescatore warned the use of cloud computing will make organizations more vulnerable to some security risks.

"Inexpensive cloud-based processing will make it easier and cheaper to break encryption keys or find vulnerabilities in software, and financially motivated criminals will certainly seek to take advantage of that," he said. "Enterprises will need to prioritize the adoption of encryption technologies that provide easy movement to longer keys."

Five steps to protect mobile devices anywhere, anytime

Author: Tom Olzak - August 4th, 2008

It shouldn't take warnings about Chinese hackers to push users and organizations toward secure mobile computing. Cybercriminals come in all shapes, sizes, and from all ethnic backgrounds. Securing mobile systems is simply the right thing to do.

Reading current news and blog postings, you might think Chinese hackers are leading us to world's end, attacking our systems in ways before unseen in the history of computing. This is an obvious overreaction. Attacks against information assets—government, corporate, and personal—have been going on for some time. So why all the hype about the dangers of taking laptops to the Summer Olympics, using laptops in Chinese hotels, or carrying smartphones into Chinese public venues? Simple. Many users and organizations have blatantly ignored recommendations for protecting mobile devices, exposing themselves, their businesses, their customers, and often employees to harm.

Mobile devices in the hands of mobile workers are exposed to a variety of threats. Let's run down a short list.

- Hotel wired networks are often wide open to eavesdropping by cybercriminals or other guests. Jacking into a network frequently equates to sending and receiving information over a single [collision domain](#). This means all packets for a set of rooms, a floor, several floors, or even the entire hotel/motel are seen by all other systems on the network. Unprotected packets are prime targets for capture, analysis, and data extraction.
- Connecting to unencrypted hotel or other public wireless networks, sending sensitive information out into the ether, is a well-known problem. I won't beat it to death.
- Improper configuration of firewalls, or the total lack of an end-user device security perimeter, allows anyone, anytime, and anywhere to use public networks to peruse private information on laptops, smartphones, or PDAs.
- Some unencrypted stolen or lost devices are a treasure chest of information, including passwords, customer and employee information, and user identity data. In large, chaotic venues like the Olympics, it isn't difficult to lose a laptop or PDA.

Again this is not a complete list of potential attack vectors, but proper attention to these four issues reduces risk to a reasonable and appropriate level. The following steps are a good start in preventing information or system compromise:

1. **Store only what you absolutely need.** This is my first rule of data leakage protection. Why carry around customer spreadsheets, financial data, or plans for a new product/service if you don't need them while out of the office? Absent Information can't be compromised.
2. **Protect data passing over public wired or wireless networks.** The best way to prevent casual or directed packet snooping on public networks is packet or session encryption, even if encryption is limited to only traffic between the end-user device and a traffic encryption service provider on the Internet. For ultimate protection, use only SSL connections to check e-mail or access company information. When this isn't possible, online services, both free and for-fee, can fill the gap. Two examples are [MegaProxy](#) (fee-based) and [AnchorFree](#) (free).
3. **Configure devices to block external snooping.** The first step in establishing a security perimeter around a device is configuration of a firewall. Personal firewalls are free on laptops running [Windows XP](#) or [Vista](#). These solutions provide minimal protection against intruder compromise of your mobile system. More complete protection is available in security suites, like those from AVG, McAfee, or Symantec. Firewalls are also available for many handheld devices, protecting contact lists, e-mail, and other sensitive information commonly found on PDAs and smartphones. The second step is configuring Bluetooth, on laptops and handhelds, to block all unauthorized access. Bluetooth threats and secure configuration information is found in [Secure your Bluetooth wireless networks and protect your data](#). No laptop should be unnecessarily exposed because it lacks anti-malware protection.
4. **Encrypt sensitive information on the device.** I know this is like beating the proverbial dead horse for many, but laptop theft reports make it clear that many users and organizations haven't yet gotten the message. And laptop encryption doesn't have to drain your budget. Solutions like [TrueCrypt](#) provide effective, free file and full-disk encryption. If you need a more centralized approach to key management, lost data destruction, or data recovery, online services like [Beachhead](#) or more traditional systems like [PGP](#) can help.
5. **Backup critical information.** All business critical information should be copied to an alternate location. Even mobile users, who might not connect to the company network every day, can be protected against data loss with online solutions like Symantec's backup.com or with Amazon.com's [S3 service](#), supported with client software like [Jungle Disk](#).

And of course, practice standard system hardening practices—patching, shutting down all unneeded services, etc. In addition to following Microsoft's best practices, consider implementing some or all [NIST \(National Institute of Standards and Technology\) recommendations and baseline template settings](#).

It shouldn't take warnings about Chinese hackers to push users and organizations toward secure mobile computing. Cybercriminals come in all shapes, sizes, and from all ethnic backgrounds. Securing systems isn't about thwarting what some see as the great cyber-threat in the East. It's simply the right thing to do.

How to carjack a top Google exec -- according to Google

Privacy group puts together a cranky demonstration

By Andrew Hendry

August 4, 2008 (Computerworld Australia) The National Legal and Policy Center (NLPC) has turned the tables on [Google Inc.](#) by using the company's controversial Street View technology along with [Google Earth](#) to compile and make public a detailed dossier on a "top Google executive."

The dossier ([download PDF](#)) includes a photo of what appears to be the front gate and parking lot of the exec's opulent California manor, including the license plates of several luxury cars outside the home, the executive's landscaping company car and a photo showing the name of the neighbor's home-security company.

The NLPC did not state which Google executive the information pertains to, but media outlets around the world are reporting that it is the home of Google co-founder [Larry Page](#).

The photos are followed by information from Google Earth, including the distance from the street to the front door and the optimal driving route the exec would follow to arrive at Google's headquarters in Mountain View, Calif., complete with photos of every intersection, stop sign and traffic lights en route.

The NLPC describes itself as a not-for-profit organization focused on ethics and accountability in public life and private business. It said in a [statement](#) that it is publicly releasing the dossier to highlight the invasiveness of Google technologies to individual privacy.

"There is no better evidence that individual privacy simply does not exist in Google's world than by the chilling amount of detailed visual information Google now collects on all of us, information that any Internet user can now compile in a dossier in less than 30 minutes," said Ken Boehm, NLPC chairman.

The NLPC criticized Google for issuing contradictory statements on privacy after the search giant said that it takes privacy "very seriously" in response to concerns surrounding the [privacy implications](#) of its search-advertising deal with [Yahoo](#). The same day, the NLPC said, court documents from May were released in which Google "evangelist" [Vint Cerf](#) told the Washington Technology Alliance that "nothing you do ever goes away, and nothing you do ever escapes notice. ... There isn't any privacy; get over it."

Google's hypocrisy is breathtaking, said Boehm.

"Perhaps in Google's world, privacy does not exist, but in the real world, individual privacy is fundamentally important and is being chipped away bit by bit every day by companies like Google," he said.

Google's Street View technology has come under increasing scrutiny because of concerns about the privacy of the people, cars and places it photographs, with both the [European Union](#) and [Canadian](#) advocacy groups warning the technology could violate privacy laws.

The search giant has also come under fire for its [monitoring of YouTube data](#), its [online privacy policy](#) and its proposed [search deal with Yahoo Inc.](#)

The Street View tool, launched in mid-2007, has since expanded to most major U.S. cities and to Europe, where the U.K.'s consumer watchdog recently approved the technology provided it blurred personal information such as faces and car registration numbers.

Google has stated that Australia's version of Street View, expected to launch this year, will also blur faces and number plates and will only include photos taken from public property.

Skype won't say if it decrypts VoIP calls

It has reportedly taken extreme measures to prevent reverse engineering of its client software

By Tim Greene

August 5, 2008 (Network World) The encryption of [Skype](#) voice-over-IP ([VoIP](#)) phone calls might not be as secure as you think.

It's possible the company keeps keys so law enforcement authorities can decrypt encrypted VoIP phone calls, according to a report, but Skype won't say for sure one way or the other. (Compare [IP PBXs](#).)

According to an [online report](#), Austrian officials with legal authority to tap VoIP phone communications have no problem listening in on Skype calls, which are encrypted as a standard part of Skype service.

A Skype spokesman wouldn't say whether Skype keeps keys to decrypt calls. "Sorry, Skype does not comment on media speculation," said Skype vice president Chiam Haas.

It's virtually impossible to figure out for sure from independent research whether Skype keeps encryption keys or not, said David Endler, chairman of the Voice Over IP Security Alliance and senior director of security research at TippingPoint.

"No one has shown it publicly," he said. "Skype is a closed [software](#) package, essentially a black box." The company has on rare occasions allowed outside researchers to examine and verify the security of its encryption, but not whether the keys that can crack the encryption can be retrieved, he said.

To allay fears that the calls might not be [secure](#) from law enforcement, Skype should open its platform to evaluation by trusted, credible industry experts, he said.

Endler said it's equally difficult to know whether commercial VoIP vendors leave open the possibility of turning encryption keys over to law enforcement.

In the U.S., the [Communications Assistance for Law Enforcement Act](#) (CALEA) forbids requiring that vendors build in back-door decryption, said Jim Dempsey, vice president for public policy at the Center for Democracy & Technology. "CALEA expressly forbids requiring anyone to be able to decrypt anything," he said.

But that doesn't mean they don't build in key-retrieval anyway. Dempsey said there are no active proposals to force vendors to leave encryption back doors in their VoIP gear, but that could change. "Nothing in regulations is permanent," he said.

Endler said that attempts by researchers to learn more about how Skype works have been effectively blocked by measures put in place by Skype. "They've taken extreme measures to prevent reverse engineering of their client software," he said, more so than mainstream VoIP vendors.

DOJ: Credit card thefts helped by 'well designed' software

Currency counter, Glock, offshore banks and global players skated right past IT security

By Patrick Thibodeau

-
- August 5, 2008 (Computerworld) The intruders whom the [U.S. Department of Justice](#) alleges stole tens of millions of credit and debit card numbers were bold, global, skilled and making millions of dollars, according to details in the charging documents.

And despite all the focus on security since the 9/11 terrorist attacks, the people alleged to be behind [this network](#) had little difficulty taking data from some nine businesses, all major retailers. They exploited vulnerabilities in networks, servers and databases, making the information they gleaned available worldwide to the underground economy that buys and sells such data.

All of this was detailed by the DOJ, which is [charging 11 people](#) in what is certainly one of the largest and most organized credit card theft operations ever. It extends back to 2003 and includes nationals from several countries — a true world-is-flat operation.

The U.S. alleges that the group decrypted PINs, made new cards and got cash from ATMs. They sold credit card data on Web sites that specialize in trading that information, the DOJ said. And, it claims, they operated globally, using offshore banks and other methods to turn stolen data into cash. ICQ instant messaging and e-mail kept everyone in touch.

Millions of dollars were involved, and the charging documents outline proceeds that were transferred in seven-digits amounts such as \$3.8 million, \$4.9 million, \$1.9 million — to list but a few.

There was so much cash involved that among the things federal authorities seized from [Albert Gonzalez](#) of Miami, whom the U.S. alleges played a key role in the crime ring, was a currency counting machine. Gonzalez was captured in May; police also confiscated a Glock handgun and nearly \$25,000 in cash from him at that time.

The retailers known to have been targeted are [BJ's Wholesale Club](#), TJX, DSW Shoe Warehouse, OfficeMax, [Barnes & Noble](#), Boston Market, Sports Authority and Forever 21.

One means of access of the retailers' networks was through a practice dubbed wardriving — driving around in a car with a Wi-Fi-enabled laptop computer seeking access.

The first details of the methods used in this extensive operation surfaced in May. In [an indictment](#) concerning the theft of credit and debit card data from [Dave & Buster's Inc.](#), a Dallas-based restaurant chain, the U.S. analyzed the software used to steal the credit card data. That indictment gives the software designer a nod as having created an effective tool.

The feds asked the CERT Coordinating Center to give an opinion of the software it found. CERT told the U.S. investigators that the "core sniffer program" is "efficient, well designed and uses some algorithms and data structures that reflect college-level knowledge of computer programming skills. ..."

The thieves were tenacious, too. When an effort to break into a restaurant's point-of-sale server in Arundel, Md., failed, the intruders went straight to the restaurant chain's corporate network in Dallas, and from there, they installed packet sniffers at some of the 49 Dave & Buster's restaurants, including one in Islandia, N.Y. From that store alone, data from more than 5,000 credit cards was obtained. Of those cards, 675 were used to make unauthorized purchases at various retail and online stores, running up losses of \$600,000.

Gonzalez was named in the Dave & Buster's case. Others alleged to be involved in the crime ring include Aleksandr "Jonny Hell" Suvorov, of Sillamae, Estonia; Maksym "Maksik" Yastremskiy, of Kharkov, Ukraine; and Hung-Ming Chiu and Zhi Wang, both of the People's Republic of China.

Focus on the Human Factor, Security Panel Says **Computerworld Canada (07/29/08) ; Lau, Kathleen**

The human factor should be the central focus of security governance, say researchers at the University of South California's Marshall School of Business, who are preparing a new business model for information security governance. The experts argue that the best technological defenses available are useless unless employees have the mindset to govern and protect their own equipment. This theory was tested at the recent Information Systems Audit and Control Association conference in Toronto when KPMG's Rolf von Roessing accessed three Blackberries from his Bluetooth during a panel discussion between information systems professionals. "These are security experts, mind you," von Roessing pointed out, adding that while using a Blackberry is pretty simple, "it's how they use them, how they behave and the little awareness of day-to-day security that is most worrying." Von Roessing and several others are developing a business model for information security that addresses four points: Organization, people, process, and technology. The model is not yet ready for rollout and needs more

modification in order to adapt to today's interconnected business structure. However, von Roessing and his collaborators say the strategy's will help companies develop an "intentional culture" regarding technology usage.

Tackling Software Security: An Increasing Threat

CIO (07/30/08) ; Allen, Julia H.

The process of developing secure software begins in one of two ways: Either by using secure software coding and testing practices or by using secure software requirements, engineering, and architecture and design practices. Each approach offers software developers different advantages. Starting with secure software coding and testing practices--such as training software developers to use language-specific secure coding practices and performing source-code review using code-analysis tools--provides a number of benefits that can help software security efforts gain support and build momentum. However, software developers that begin the development process by using secure software requirements, engineering, and architecture and design practices can address the root causes of security vulnerabilities early in the lifecycle, before they show up in coding and testing. Regardless of which approach they use, software developers need to follow a number of standard practices, including selecting and integrating certain security practices with their existing software development lifecycle and development process and thinking like an attacker when developing software.

Security and the generational divide

Why 'Stay off my network, you rotten kids!' isn't a good coping strategy

By Joan Goodchild

- August 8, 2008 (CSO) The generation gap. It's a term that has been used for decades to describe the differences between people in various age groups. Corporations are constantly considering what makes different generations tick when it comes to recruiting and retaining employees. But security experts say companies also need to examine age-based perspectives and habits when it comes to [risk assessment](#) and policies.

Cultural analysts generally divide today's workplace personnel into three generations: baby boomers, Generation X and Generation Y, also known as millennials. The stereotypes typically go like this:

- Millennial employees, workers born after 1980, are tech-savvy and have short attention spans.
- Baby boomers, born between 1946 and 1965, are loyal and dependable, the original workaholics.
- Gen Xers, once known as the slacker generation born between 1965 and 1980, tend to be cynical and independent.

Companies need to understand all perspectives in order to effectively communicate their security policies.

Stereotypes are useless for predicting the actions and reactions of any one person. Yet these characteristics do tend to ring true in the workforce at many organizations, according to Roberta Chinsky Matuson, president of [Human Resource Solutions](#), a Massachusetts-based consultancy that regularly advises corporations on generational differences. Companies need to find ways to relate to all perspectives in order to create and communicate effective security policies as well as to defuse what Matuson calls "potentially explosive situations."

"From a security standpoint, there is a lot of opportunity for misunderstandings," said Matuson. "We need to educate people about what those are."

According to the security and HR experts *CSOnline* spoke with, each generation is prone to engage in risky behavior of different types and may not understand how habits are compromising a company's risk level. A clear example is recent research from security software maker Symantec Corp. The [survey](#), which was released earlier this year, found that IT managers are at odds with millennial workers. Among respondents, 66% of Gen Yers said they use Web 2.0 technologies, such as Facebook and YouTube, while at work. Only 13% of older workers admitted to logging onto these kinds of Web sites in the office. Meanwhile, Symantec also surveyed IT

managers, and 50% said they have policies specifically banning Web 2.0 applications such as social networking, iTunes, streaming video and gaming applications. [See "[Web 2.0 Applications and Sites \(and Security Concerns\)](#)" for specific examples of such sites and application and their attendant risks.]

"For millennials, there is more blurring of the lines between work and home," said Samir Kapuria, a managing director at Symantec Advisory Consulting Services, the organization that conducted the survey. "They tend to use what they have at home while at work, and this is really forcing corporations to [rethink IT risk management](#)."

The risk, according to Kapuria, is Web 2.0 programs are a huge target now for [phishing scams](#) and malicious code attacks. And the implications from these Gen Y habits go further than simply putting a corporate IT infrastructure at risk of attack. There are privacy issues to consider, too.

The poll found that younger workers regularly store corporate data on personal devices, such as PCs and USB drives, much more than older counterparts. This flies in the face of the 75% of corporate IT managers who have said they have policies that restrict corporate data and information on personal devices. Symantec also found that 85% of corporate IT managers have policies restricting download and installation of software on work PCs for personal use.

In Kapuria's opinion, the key to minimizing risk from younger workers is education.

"I don't think there is any kind of malicious intent or rebellion on the part of this generation," said Kapuria. "Companies should consider education programs tailored to this audience as part of their security approach."

However, educating older workers is equally important, according to Aaron Wilson, chief technology officer in the Managed Security Services division of Science Applications International Corp. Baby boomers' lack of familiarity with new technology may make them a risk, too.

"Gen X/Y/Z employees often understand the nuances of the new technologies they bring, whereas boomers may be equipped with the same technology but not as familiar with all of the functionality," said Wilson. "This can be dangerous from a security standpoint, for example when understanding the subtle difference between encrypted e-mail on a corporate RIM device versus an unencrypted e-mail on an iPhone. To the uninitiated, it's all e-mail. To the security team, it's safety versus possible unintentional exposure of sensitive data."

Access control and security habits

Security consultant Jack Dowling remembers a simpler time when it came to building access and security.

"There was a time when a new system was put in place and there was an understanding that it took time to get used to. Now, as soon as something doesn't work...." Dowling said, sounding like veteran reminiscing about the old days. "There are always going to be bugs in electronics. But now glitches are perceived as incompetence on the part of the company."

Dowling, the president of JD Security Consultants LLC in Philadelphia, has a resume in the field that dates back to the 1970s. He thinks that the combination of a high level of technical proficiency and a lot of impatience on the part of younger workers makes it difficult for organizations to smoothly integrate new security systems and policies these days.

But despite their youth, it's actually not millennials who Dowling thinks pose the biggest threat when it comes to access. Instead, their slightly older peers are the ones you might want to watch out for if you are concerned about access. While Gen Xers have matured and evolved considerably beyond their so-called rebellious earlier days, Dowling says it is still important to key an eye out for this group, which in today's workforce means workers between 28 and 43 years old.

"They like to reject the rules. They have their own way of doing things," said Dowling. "They tend to look for ways around the system, may not realize the security value and are probably less likely to comply."

On the other hand, millennials, a group whose young lives were defined by 9/11 and who are comfortable with high-security systems, are more likely to comply, said Dowling. But then there is that impatience and short attention-span thing again.

"Queuing problems for instance," said Dowling. "They may be more likely to get frustrated and less likely to comply if that is the case."

Queuing, or waiting in line, can sometimes be an issue in a security system, depending on how [entry control](#) works, said Dowling. For example, an optical turnstile or other system of control may have a line. Impatient users may view this as a waste of time and try to gain access through an exit door and bypass the security protocol for entry, he said.

And as for his own boomer generation?

"A new system comes into place, and they have an understanding that it is there for a reason. They are going to use it and use it the right away."

Spoken like a true boomer.

Can't we all just get along?

All of these different perspectives can no doubt lead to tension among workers. Workplace confrontation is a real concern when it comes to generational differences, according to Matuson.

Understanding different styles of communication is the first step to easing the frustration that many older workers may have about their youthful colleagues.

"Some of my more mature clients think younger people are from another planet and don't have any respect for their elders," said Matuson. "I think what some of the older workers need to understand is that it's not that these younger workers don't hear them. It's that they listen in a different way."

In other words, said Matuson, have patience. Understand that while a millennial is texting in a meeting, he is still listening. He just listens in a different way. If the concept seems a little hard to swallow, consider Matuson's next piece of advice.

"I often say to clients: When is the last time you successfully changed your childrens' ways?' You need to change your approach instead."

Joseph A. Kinney, a security consultant in Pinehurst, N.C., often advises clients to develop mentor programs.

"I think it's great if a 50-year-old can just go to lunch with a 20-year-old and discuss things," he said.

Hip to be secure

When implementing security policies and systems, corporations need to remember that each generation will see them differently and adhere in its own way. And in some cases, the system may be intimidating for mature employees who aren't used to technology.

Matuson points to a story she heard from an older client who was waiting in a lobby for a job interview. As they watched scores of younger workers breeze through the building's very high-tech screening system, he said he had one thought: "I'm not cool enough to work here."

How effective is a security system if it's keeping potentially valuable employees away? Organizations should remember that and make sure every group is considered in security -- and security communication plans, Matuson said.

