

Security Trends Report

07/08

DATA BREACHES MADE POSSIBLE BY INCOMPETENCE, CARELESSNESS

Still, installing software patches as soon as they're made available will significantly reduce the chance of a data breach, according to a Verizon Business Security survey.

By [Thomas Claburn](#)
[InformationWeek](#)

June 11, 2008 06:30 AM

Eighty-seven percent of data breaches could have been prevented with reasonable security precautions, according to a study of over 500 forensic investigations conducted by [Verizon Business Security Solutions](#).

Verizon's study of actual data breach investigations from 2004 through 2007 suggests that incompetence and carelessness represents the greatest threat to business information.

The study found that breaches were attributable a combination of events more frequently than a single action, including: a significant error (62%), [hacking](#) and intrusions (59%), malicious code (31%), an exploited [vulnerability](#) (22%), and physical threats (15%).

But for 90% of the known vulnerabilities exploited, patches were available for at least six months prior to the attack. This data point alone suggests that installing [software](#) patches as soon as they're made available will significantly reduce the chance of a data breach.

"We're seeing more and more examples of security breaches and compromises taking the path of least resistance," said Bryan Sartin, VP of investigative response at Verizon.

Fifty-two percent of attacks were rated as having a "low" difficulty level, according to the report. And only 15% of attacks were fully targeted. The remaining attacks were directed but opportunistic (46%) or randomly opportunistic (39%). An example of such an attack might be a [hacker](#) scanning the Web for sites running a particular vulnerable software application.

Based on the cases investigated, the type of data compromised falls into the following categories: payment card data (84%), personally identifiable information (32%), non-sensitive data (16%), [authentication](#) credentials (15%), other sensitive data (10%), intellectual property (8%), corporate financial data (5%), and medical/patient data (3%).

The study found that those responsible for data breaches were: external sources (73%), insiders (18%), business partners (39%), and multiple parties (30%). While insiders accounted for the smallest percentage of breaches, the breaches traced to them involved more than ten times as many records (375,000) as breaches traced to outsiders (30,000) and about twice as many records as breaches traced to partners (187,500).

Calculating risk by multiplying the likelihood of involvement times the number of records affected, the study concludes that business partners represent the greatest threat, followed closely by insiders.

"The most insidious breaches these days involve partial insiders, contractors, and third-parties who have ability misuse access," said Sartin.

Ignorance makes such incidents possible. Verizon's study found that 66% of the cases involved data that the victim did not know was on the system. Even more alarming, it found that 75% of the breaches were not discovered by the victim and that in 63% of cases, months or years passed between the initial breach and discovery.

"We find this statistic to be astounding," the study says and offers two likely explanations: "Firstly, and perhaps most obviously, criminals do not want to be discovered. They have great financial incentive to retain access to

corporate systems for as long as possible and will go to great lengths to ensure their activities remain under the radar. Secondly, and perhaps most importantly, organizations simply are not watching."

Verizon recommends aligning policy with actual business processes, focusing on essentials to avoid becoming low-hanging fruit for hackers, making sure security controls extend to partners, creating a data retention plan to understand what data is where, actually monitoring network event logs, creating an incident response plan, and conducting mock incident testing.

According to the [Identity Theft Resource Center](#), there were [446 data breaches publicly reported in 2007](#), 312 in 2006 and 158 in 2005. Verizon's report says that the more than 500 cases its investigators looked at include about one-third of the publicly disclosed data breaches in 2005 and a quarter of the publicly disclosed data breaches in 2006 and in 2007.

But according to Sartin, the publicly reported breaches are "just the tip of iceberg." He said that less than 5% of the more than 500 cases covered in the Verizon study involved some form of disclosure.

Though states have been passing data breach disclosure laws, he said that there are actually fewer data breaches being disclosed now than in the past. The reason, he said, is that each state has a different take on disclosure requirements and other countries often have no disclosure rules.

"Until there is a real consensus-based focus on how to do this right, you're going to see more and more companies find unique ways to sidestep their legal obligations," Sartin said.

Web Application Vulnerabilities on the Rise; Journalist Goes To Pen Testing School

(June 9, 2008) More than half of the vulnerabilities that appear in the SANS Security Alert email newsletter are web application vulnerabilities. Earlier this year, GCN Senior editor Joab Jackson attended a SANS class in which Kevin Johnson detailed some of the techniques he employs as a penetration tester and along the way, explained why web applications vulnerabilities are so plentiful. Operating systems have become more secure over recent years, so cyber criminals had to find another vector of attack. Most web applications are written by developers who lack essential training in secure programming. Johnson also stressed the importance of thinking like a hacker, particularly when it comes to gathering information prior to an attack.

<http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn&story.id=46418>

<http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn&story.id=46420>

[Editor's Note (Siles and Paller): The situation is much worse than the public statistics show. All the millions of custom web applications are even more likely to be flawed than commercial applications.

(Pescatore): Operating system vulnerabilities aren't really slowing down all that much, but patching and the use of intrusion prevention technologies have made those vulnerabilities harder to exploit. The real reason web vulnerabilities seem to be on the rise is that phishing and malware attacks have found that by compromising legitimate websites and getting users to visit those compromised links is a way to get around URL blocking that has been keeping people away from popup malicious web sites. The web security gateway companies are seeing on the order of half of all web malware downloads coming from compromised but legitimate sites these days. It means web security gateways have to improve their ability to block inbound malware - and not just simple signature based AV, either.

Exploiting Security Holes Automatically

Technology Review (06/03/08) ; Naone, Erica

Researchers led by Carnegie Mellon University professor David Brumley have found that software patches could be just as harmful as they are helpful because attackers could use the patches to automatically generate software in as little as 30 seconds that attacks the vulnerabilities the patch is supposed to fix. The malicious software could then be used to attack computers that had not received and installed the patch. Microsoft Research's Christos Gkantsidis says it takes about 24 hours to distribute a patch through Windows Update to 80 percent of the systems that need it. "The problem is that the infrastructure capacity that exists is not enough to serve all the users immediately," Gkantsidis says. "We currently don't have enough technologies that can distribute patches as fast as the worms." This distribution delay gives attackers time to receive a patch, find out what it is fixing, and create and distribute an exploit that will infect computers that have not yet received the

patch. The researchers say new methods for distributing patches are needed to make them more secure. Brumley suggests taking steps to hide the changes that a patch makes, releasing encrypted patches that cannot be decrypted until the majority of users have downloaded them, or using peer-to-peer distribution methods to release patches in a single wave.

Data thieves get focused (but buyers get sloppy)

Finjan: Commoditization of market driving more targeted attempts

By Jaikumar Vijayan

June 18, 2008 (Computerworld) When it comes to online data theft, credit card numbers and bank account data are so 2007.

Increasingly, thieves are after more-specialized information such as health care data, single sign-on credentials for remote log-in to corporate networks and FTP account data, according to a new report from security vendor [Finjan Inc.](#)

The report, which was released today, summarizes the latest trends in the cybercrime marketplace over the first six months of 2008.

One of the biggest among those trends is the growing commoditization of some kinds of stolen data, according to [Yuval Ben-Itzhak](#), chief technology officer at Finjan. Until recently, he said, credit card numbers and bank accounts with personal identification numbers (PIN) were considered valuable items in the underground market. But of late, the market has become flooded with such information, leading to its commoditization, Ben-Itzhak said.

Where valid credit card numbers and PINs used to sell for \$100 or more each, they retail today for \$10 to \$20 in the underground market, Ben-Itzhak noted. Depressing prices even more is the easy availability of such information from numerous sources, most of which are quite literally a mere [Google](#) search away from prospective buyers.

As a result, there is a trend on the part of some online thieves to go after data that can fetch them premium prices in the cybercrime market. "It's just basically the rules of supply and demand," Ben-Itzhak said.

One trend that Finjan has noticed is an increased focus on trying to steal log-in credentials for [Citrix](#) applications. Technologies from Citrix Systems Inc. are being used by an increasing number of health care organizations to enable remote network access, Ben-Itzhak said, and stealing Citrix log-in credentials often allows data thieves to gain single sign-on access to a wide range of health-related information from inside hospital networks. The stolen data is used for a variety of scams such as fraudulent insurance claims, illegal purchases of prescription drugs and medical ID theft.

It's not just health care organizations that criminals are targeting, either, Ben-Itzhak said. There's a growing focus on stealing log-in credentials that provide remote access to business networks as well.

For instance, Finjan recently discovered a Argentina-based server containing over 500MB of stolen data and another server containing over 1.4GB of similar information in Malaysia. In both cases, the systems contained not just health care information but also business-related data. For instance, one of the servers had a cache of data that included passenger reservation data and flight scheduling information stolen from a major airline.

Despite the increasingly sophisticated methods that cybercriminals use to steal data, those who are actually soliciting and using the stolen information are relative amateurs with little idea of how to secure their illegally gotten data, Ben-Itzhak said. Often, stolen data is stored in unprotected fashion on servers that can easily be accessed by anyone with a Web browser. Data on one of the crimeware servers discovered by Finjan this year had no access restrictions and allowed search-engine crawlers to index log files as they do with other public

information on the Internet. As a result, passwords, Social Security numbers and other sensitive information ended up being stored on public caching servers such as those of Google Inc.

The report is available on Finjan's Web site; registration is required.

One-third of IT admins admit snooping with privileged passwords

Power and anonymity equals risky business, says password management vendor

By Gregg Keizer

June 20, 2008 (Computerworld) One in three IT administrators say that they or one of their colleagues have used top-level admin passwords to pry into confidential or sensitive information at their workplaces, according to a survey by a password-management vendor.

Nearly half of the respondents also confessed that they have poked around systems for information not relevant to their jobs.

"We asked these questions last year, too, and we got similar results," said Adam Bosnian, vice president of product strategy and sales at Cyber-Ark Software Inc., a Newton, Mass.-based maker of password file security management software. "So on one hand, the results weren't surprising. What was surprising initially -- and this time around, too -- is that people admit to it."

Last month, Cyber-Ark polled approximately 300 senior IT professionals at a London security conference and trade show, asking them a dozen questions about their password practices. The majority of those surveyed said they work for companies with more than 1,000 employees.

The fact that one-third acknowledged they had abused an admin password to access out-of-bounds information shouldn't surprise anyone, said Bosnian. "Everyone thinks that IT administrators are the trusted ones, and it's all the rest that we need to worry about. But admin passwords not only give administrators a lot of power, they also provide a lot of anonymity."

That combination is too tempting for some to fight, and that would explain the high number of respondents who said that they had poked into places they didn't belong, Bosnian added. "People think, 'I feel a little bit safer' when they're using an admin password. There could be hundreds of people with access to that password."

Cyber-Ark's survey also asked IT workers to select three things they would try to take with them if they were told they would be fired the next day. The top two vote-getters: the customer database (35%) and a list of all privileged passwords (31%). "That's not really surprising either, is it?" said Bosnian. "The customer database is one of the company's most valuable assets."

The poll also revealed behavior that wouldn't make any security best practices lists. Almost one-third -- 28% -- of the IT professionals polled said that they had written privileged passwords on paper, while nearly one in 10 admitted that they never changed critical passwords.

Business partners are a prime attack vector

By Frank Hayes

- June 23, 2008 (Computerworld) If you're an IT security pro, you already know what this column is about. If you're not, you should download [Verizon's "2008 Data Breach Investigations Report"](#) right now. There's lots of horrifying data in there, but this is the one that shook me: Almost half of data thefts now come by way of our business partners.

That's right: Increasingly, attackers aren't trying to get through our security perimeters. Instead, they get inside the systems of suppliers, customers and contractors we trust, and from there, we're sitting ducks.

In 2003, only 8% of the attacks [Verizon](#) documented came that way. In 2007, 44% did.

And that percentage is likely to continue to rise.

Understand that this study from Verizon's security services group is based on metrics from more than 500 cases the company was hired to investigate. That's the study's strength and its weakness. It's naturally skewed to cover incidents that were worth calling in a security outfit about.

Then again, those are the ones that keep us up at night.

As you'd expect, the first few pages are a thinly veiled soft sell for Verizon's security services. Don't give up; the numbers start on page 8.

Some of what Verizon itemizes is common sense. But some of it demolishes our expectations. It turns out that only 18% of these attacks were launched by insiders (so much for the old "80% of security breaches come from the inside" myth). In 78% of the cases, fully patched systems wouldn't have stopped the breaches. And 55% of the attacks required no great technical chops -- just script-kiddie capability.

And despite all the investments we've made in security monitoring, 70% of the breaches were discovered only after outsiders tracked the source of identity theft and other problems back to people like us.

What does the report recommend? Put simply: Monitor your systems, review the logs, and put processes in place to deal swiftly with security problems when they're reported.

There's more to it than that, of course. Read the report. Don't just hand it off to your security people. If you're a CIO or an IT manager or a sysadmin, you need to know what it says.

Then you need to change the way you think about security. Especially as it relates to partners.

That 44%-and-growing number is the one that should scare you. These are organizations we have to trust enough to let them connect to our systems. But we can't choose them; business users and executives do that. We don't run their systems. We may not be able to vet their security or force them to improve it.

We have to set up their connections fast, frequently on short notice and always according to what the business guys want, not what security demands. We have to let them inside our perimeter -- but we can't secure *their* perimeters.

And the bad guys have figured out that every partner is now a potential attack vector.

What does Verizon recommend? Implement basic partner-facing security measures. Tighten up every aspect of your connections with partners, from provisioning to permissions. That's all good, practical advice.

But first you'll have to accept a new reality: Business partners aren't just an extension of your business. They're a potential threat -- and your worst enemies know it.

Then get ready to explain to your CEO why you want to treat every partner like your worst enemy.

U.S. Privacy Act outdated, hasn't kept up with technology, experts say

GAO expected to call for new privacy rules, position of chief privacy officer

By Grant Gross

June 18, 2008 (IDG News Service) WASHINGTON — Updates to a 34-year-old privacy law are needed to better protect personal information held by the U.S. government, privacy experts told a Senate panel today.

The 1974 Privacy Act, the main law governing how U.S. agencies should handle private information, hasn't kept up with new technologies and, in some cases, has huge exceptions on its restrictions for sharing personal information, witnesses told the Senate Committee on Homeland Security and Governmental Affairs.

"Technology evolves so rapidly in this day and age that we will need to be more vigilant in ensuring that the wheels of progress are not inadvertently running over our basic privacy rights," said Sen. Susan Collins (R-Maine). "We're constantly trying to catch up with the laws and the policies to the technology."

The U.S. government needs to make several improvements in its privacy policies and data collection to avoid data breaches like a 2006 incident in which a laptop containing the personal information of [26.5 million people](#) was stolen from a U.S. Department of Veterans Affairs employee. There were also reports of [490 laptops stolen](#) from the [Internal Revenue Service](#) over three years, Collins said.

The [U.S. Government Accountability Office](#) was due to release two reports today, one calling for Congress to establish new privacy rules, and a second recommending that the White House Office of Management and Budget establish a permanent chief privacy officer who could oversee privacy efforts governmentwide.

Privacy protections are not consistently applied across the U.S. government, and agencies often do not limit their collection of personal data to needed information, said Linda Koontz, the GAO's director of information management issues.

"Current laws and guidance impose only modest requirements for describing the purposes for personal information and limiting how it is used," Koontz wrote in one report.

Agencies are not required to be specific in their data-collection public notices, which "could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed," she wrote.

Privacy advocates [Ari Schwartz](#), vice president of the Center for Democracy and Technology, and Peter Swire, an Ohio State University law professor and former chief privacy counselor at OMB during the Clinton administration, also called for Congress to mandate changes in the way U.S. agencies handle personal data.

The Privacy Act doesn't address new technologies such as data mining, which can have major privacy implications, nor does it envision government agencies contracting with private data brokers, Schwartz said. Current privacy guidance from [President George W. Bush's](#) administration is "vague and simply does not provide the agencies the tools they need" to create privacy impact assessments for their use of personal data, he said.

Schwartz and Swire both called upon Congress to update the Privacy Act and close loopholes in the law, as well as to create a permanent chief privacy officer at OMB.

Swire also raised concerns that the [U.S. Department of Homeland Security](#) is increasingly relying on biometric data such as fingerprints. The DHS has promoted the infallibility of fingerprints, but it's easy to find explanation online on how to forge them, Swire said.

He called on the DHS and other agencies to encrypt fingerprint and other biometric data in nearly all circumstances. "If you lose your fingerprint, it's hard to get a new finger," Swire said.

Will gadgets make knowledge obsolete?

When everyone can find out anything, anytime, anywhere -- why learn?

By Mike Elgan

June 20, 2008 (Computerworld) In the 1984 cyberpunk novel *Neuromancer*, author [William Gibson](#) describes a future in which people can acquire knowledge by buying special chips called "microsofts" that plug into a surgically installed jack behind the ear. Once you plug in the chip, your brain can access its database and — voila! — knowledge!

It's an interesting and creepy idea, but one that we're going to have to face eventually. No, not painful implants; we're going to have to face the problem of education in a world in which nearly all knowledge is available to everyone, instantly, all the time.

A mere 20 years ago, almost no one had heard of the Internet, had ever used a cell phone or even knew what "GPS" stood for.

Today, most people I know over the age of 12 use the Internet every day, access data all day on their cell phones and use GPS gadgets to get from one place to another. Mobile broadband is rapidly getting faster. Mobile devices are getting radically better screens and user interfaces. And the whole world of data access on mobile devices is quickly bringing us to the point where we can find out just about anything from anywhere.

Where will we be 20 years from now in terms of our ability to access any information from anywhere? The mind boggles. Let's look at a few trends.

Trend No. 1: The rise of Internet-connected smart phones. Smart phone shipments are up 29%, according to market research firm [Gartner Inc.](#), and now represent 11% of the worldwide cell phone market. In many countries, they represent the majority of sales. As handset prices drop, and data plans and online services become more compelling, smart phones will largely replace "dumb" phones for just about everybody and become totally mainstream.

Trend No. 2: The increasing speed of data connections. Both the number of people upgrading to mobile broadband, and the speed of those connections, are rising very fast. Cell-phone maker [Ericsson predicts](#) that mobile broadband subscribers could reach 2.2 billion within five years. As of January, there were 204 HSDPA (3.5G) networks in 89 countries either fully operational or well on their way. This level of performance will quickly go mainstream, and users will start looking forward to 4G, or Ultra Mobile Broadband (UMB) performance on their phones, which will be capable of downloads as fast as 280Mbit/sec., two orders of magnitude faster than DSL on a desktop PC!

Trend No. 3: Improvements in user interfaces. The [Apple iPhone](#) and its ginormous, high-quality screen and intuitive user interface reset the bar for how easy and appealing grabbing online data over a phone should be. Imitators abound, and all are scrambling to produce ever better mobile-data experiences.

Trend No. 4: Advancements in voice recognition and artificial intelligence. Voice command is slowly creeping into our phones. Little by little, our phones' GPS functionality, applications and Web browsing will be controllable with the spoken word. Increasingly, our commands will be processed on remote servers that can "learn" and figure out what we're looking for, and present it in the way that's most usable. As services like [GOOG-411](#) (dial 1-800-466-4411 to try it) become more popular, people will increasingly use voice-command systems to get information anytime, anywhere.

Trend No. 5: More information online. There are more than 168 billion Web sites on the Internet, according to [an Internet services company called Netcraft](#). The total number of sites — not pages, but sites — increases by roughly 3 million each month. That's a primitive measure, but it's clear that knowledge is going online. Newly generated information increasingly shows up on public servers, and old books and other sources of knowledge are being scanned and digitized at a feverish pace. There are currently more than 2 million English-language articles on the [Wikipedia](#), a number that has doubled since 2006.

Trend No. 6: Improvements in search. The success of [Google](#), which largely leveraged high-quality search to place itself at the center of the technology universe, has focused competitors to innovate in search as well. Now Google has created a search-centric mobile platform [called Android](#) that should drive major improvements in cell-phone Internet searching.

If all these trends continue to develop over the next 10 years, what will the result be? It's impossible to predict, but you can bet we'll all be carrying phones that, with a simple voice command, instantly retrieve exactly the information we're looking for 99% of the time, and from anywhere, 24/7.

What's the difference between this cell phone of the future and Gibson's vision of "microsoft" chips? The only difference is that the microsofts seem clunky, useless and antiquated in comparison to the breathtaking knowledge machine everyone will carry in his or her pocket or purse.

When schoolchildren know with certainty that they will never be without a device that tells them any information they could ever want to know, how motivated will they be to sit there and memorize state capitals and other such trivia? How motivated will schools and teachers be to force this on kids?

The idea that knowledge could become obsolete is a creepy and objectionable one. The pursuit of knowledge is among our most cherished values. But mobile devices and the mobile Internet are already enabling us to deliberately remain ignorant on specific topics we used to have to know. Here are just a few examples.

GPS: In the past, if you wanted to drive to somewhere new, you had to gather information like maps or directions and study them. I've noticed that GPS users come to rely on things like turn-by-turn directions and stop trying to learn anything about where their destination is or how to get there. We hop into our cars in blissful ignorance, simply plugging in an address and obeying our GPS's commands.

Laptops: I do a lot of radio and have noticed that everyone on the radio these days — the hosts, the guests, etc. — is sitting in front of an Internet-connected PC or laptop while on the air. Both guests and hosts are on the radio because they're experts or they know something. Yet there's literally no downside to supplementing knowledge in real time with online resources. People outside broadcasting do this, too, on telephone conference calls and other situations where you can hear the person but not see him. They are, in effect, using their laptops as Gibsonian microsofts to augment their knowledge. Using an Internet-connected device when called upon to know something is simply what people do whenever they can.

Cell phones: Internet-connected smart phones are becoming the Mother of All Knowledge Replacement Devices. For general information, people head straight for Google or Wikipedia and to more specialized sites, which are increasingly mobile-friendly, for detailed, often job-specific information. The availability of this information is making people more relaxed about knowledge in general.

So whether the idea of knowledge obsolescence strikes you as horrible or not, it is already happening and is tied directly to the quality and availability of gadgets.

Maybe this is an opportunity

The truth is that we forget just about everything we learn in the 12 years we go to school. Yes, much of that lost knowledge served as building blocks for subsequent knowledge and intellectual abilities that enabled us to develop into who we are now. But broadly speaking, the difference between an educated 40-year-old and a 40-year-old moron is not how much they learned in school but what those people have done since graduating. A curious, active reader who uses reference materials promiscuously is going to be far better educated than someone who doesn't read and doesn't care about knowing anything.

In other words, the current educational system is deeply flawed. How many new high school graduates come across as people who just devoted the last 12 years of their lives to learning? Would we all be better off if we had spent more of our precollege education on skills, including how to find and process knowledge, than on memorizing facts that will soon be forgotten and can easily be retrieved later?

Maybe mobile devices will free us to transform our educational system into one that doesn't kill children's curiosity and sour them to the idea of reading a book. Maybe if kids don't have to spend so much time forcing themselves to memorize facts they've already got in their pockets, they can have less homework and regain their childhoods. Maybe we'll come to realize that knowledge — the storing of data in our brains just in case we might need it someday — isn't valuable to us. And if we can let the computers do that part for us, we can focus on what we do best, which is to recognize patterns, explore ideas and follow our curiosity.

Will knowledge become obsolete? I have no idea. But I do believe that carrying a hundred Libraries of Congress in our pockets changes our relationship with knowledge and will force us to rethink how we acquire it.

ADVICE+DISSENT: Managing Technology Forget Something?

By Jill R. Aitoro jaitoro@govexec.com *Government Executive* June 1, 2008

Offering security training isn't enough to curtail breaches - employees must follow through.

Most travelers know what to do at an airport security checkpoint: Pull out the quart-size, zip-top plastic bag filled with 3-ounce containers of liquids; take off shoes; place folded coat in a bin; remove laptop from its bag. It's almost second nature.

Go to any agency, however, and you likely will find many people who rarely change their passwords, who download sensitive documents to thumb drives, or who click on dubious embedded links in e-mails. Knowing what not to do when working on a computer should be just as ingrained in employees' psyches as knowing what to do at an airport security checkpoint.

But that isn't how it works. The answer, you might think, is to offer training. That can drive some changes in behavior, and agencies offer a slew of security courses. But the number of high-profile security breaches over the years proves that providing training doesn't cut down on such mishaps. "Compromises in security continuously arise where an employee is the cause," says Patrick Howard, chief information security officer for the Nuclear Regulatory Commission. He joined NRC in March, after holding the same position at the Housing and Urban Development Department. "A lot is human nature. People just don't think, or they rationalize, 'What I have to do today is more important than following security rules.'

"There has not been a culture of security established where [precautions have become] automatic, because agencies are too focused on getting the required box checked. Existing legislation is fine - it's the implementation that might be out of kilter."

The 2002 Federal Information Security Management Act requires agencies to provide training to ensure that employees are aware of their security responsibilities. The law also requires specialized training for employees whose jobs involve processing or managing sensitive information. Every year, agencies must file reports to the Office of Management and Budget on their security awareness and training programs.

The Information System Security Line of Business, part of the President's Management Agenda, directs agencies to provide by Sept. 30 security awareness training from the Defense Department, Office of Personnel Management or from a joint program developed by the State Department and the U.S. Agency for International Development. These agencies operate shared service centers that specialize in security awareness training. The line of business encourages agencies to take advantage of specialized services, which include courses tailored to particular work roles. This training is voluntary, but OMB likely will require it once the program has been established. A volunteer cross-agency workgroup is developing standards for the program.

But employees aren't lining up to enroll. A little more than 138,500 employees from large agencies - only 4 percent of the governmentwide workforce - took security awareness training at a shared service center in 2007, according to OMB.

The key to training more employees, says Robert Howard, the Veterans Affairs Department's chief information officer, isn't more legislation. What's needed, he said, is to communicate to federal managers that security training is important. "We do not lack for guidance and direction," he says. "Just putting out programs and asking people to take them is not good enough. You've got to keep beating the drum."

In May 2006, a laptop was stolen from a VA employee's home, exposing the names, dates of birth and Social Security numbers of 26.5 million veterans and their family members. In response, the department revamped its information security program, focusing on consistent and customized training. All VA employees now sign a document that details the rules of behavior for security. They must enroll in two online training programs at least once a year - one on privacy and one on security - which are customized by each VA organization and focus on individual security responsibilities.

The department mandates a series of role-based courses that IT and security professionals must take within the first 90 days of being hired. The more an employee works with sensitive information and networks, the more advanced the security course. An intern program for new information security professionals augments the Web-based training with hands-on classroom instruction. VA assigns trained mentors to employees who need

individual attention.

"You don't want everyone to become aware of information security after a VA-type of breach happens, but there needs to be a balance," says Karen Evans, OMB administrator for the Office of E-Government and Information Technology. "If an agency wants to take advantage of a particular capability, some degree of risk might be necessary. It's up to agencies to analyze backdoor vulnerabilities that exist and ask, 'Is this a risk we're willing to live with?' Then either sign off, or set the threshold higher."

Agencies should consider emerging threats that could infect their systems and incorporate lessons on how to thwart those attacks into their training programs, NRC's Howard says. Then they should test employees to see whether they retained the information and rework the content they failed to learn. "There's a temptation to say, 'That worked last year, so it's probably good this year,' but a lot changes," he says. "The bad guys, more than ever before, are taking advantage of those failures of human nature - the opening of e-mail attachments, clicking on embedded links. It's difficult to expect users to automatically not fall for that. People are basically trusting, even when they shouldn't be."

Insurer offers mobile health records

Security and privacy are top concerns

By Matt Hamblen

June 25, 2008 (Computerworld) Today, you can use your cell phone to make voice calls, send e-mail, browse the Web, make video recordings and even conduct wireless bank transactions.

But would you use your cell phone to carry your health records?

[Blue Cross](#) of Northeast Pennsylvania is betting that its customers will want to keep complex personal health records on their phones, especially when they have several doctors and medications to keep track of.

The health insurer began a slow rollout last month of a secure mobile personal health record application that is designed to give customers access to their medical information no matter where they go, said Drew Palin, chief development officer at the Blue Cross affiliate in Wilkes-Barre, Pa. He said the application may be among the first of its kind.

The application is free to members and has so far rolled out to less than 10% of the 600,000 people enrolled at the insurer.

Palin said the mobile health record application is free because the company wants to promote its use. Nationwide adoption of electronic medical record technology by hospitals and doctors has been "slow," Palin said, adding, "We figured the other way to promote electronic records is through the patients."

So far, it seems that the service is being adopted by the typical group of technology early adopters who are open to new systems and applications and have come to terms with questions about the privacy of their medical records, he said. But Palin noted that from Day One, his managers and others were primarily concerned with keeping the records secure and private. "Our No. 1 through 10 priorities were security and privacy," he said.

Blue Cross of Northeast Pennsylvania sought out AllOne Health Group Inc., a health care technology integrator in Wilkes-Barre, Pa., that has partnered with Diversinet Corp., a Toronto-based company with 10 years of mobile security expertise, Palin said. Diversinet had already offered a similar application for mobile financial services.

The AllOne Mobile application runs on almost all varieties of smart phones and the majority of cell phones on the market. It stores the data in encrypted form behind a password, said Stuart Segal, vice president of integrated operations at AllOne.

Palin said he felt confident in the security protocols because of the encryption it offers. Encryption works on the actual phone, over the air, and on the Diversinet server used to gather the patient data that is input by the

patient from a desktop computer, he said. During the desktop-input process, dual-factor authentication is used to authenticate the phone as the device the user wants to deploy; the insurer and other parties can never see the health data, Palin explained.

Palin said that parents and those caring for their elderly parents will appreciate the application because it means they can visit a doctor and quickly find names of medications that have caused allergic reactions, for example. While the application won't store actual X-rays and images yet, it can provide the results of lab tests. One user has already used a cell phone to send a medical record to a new doctor via wireless fax, he said. "Word of mouth is that people love it," he said.

Currently, users can input their own medical data, and starting next month, Blue Cross of Northeast Pennsylvania will begin populating the databases with information from its own files, Palin said. In a year or so, data from hospitals and doctors will be imported as well.

[Craig Mathias](#), an analyst at Farpoint Group in Ashland, Mass., said the Blue Cross rollout might be one of the first of its kind, although there is a growing market of technology providers that build mobile middleware to port applications of all kinds to devices. Despite concerns about personal privacy, Mathias expects that mobile health records will catch on. "All information will eventually be online and mobile," he said.

A fingerprint scanner on a phone might be the ultimate way to ensure security, although such technology is rare, Mathias said. But because any security system has some degree of vulnerability, Mathias said mobile health record users will need to figure out what would happen if their health record got into the wrong hands.

Palin said the privacy worry will always be a concern for users and the insurer alike. "If somebody puts in the record that there's a strong family history of breast cancer, we won't know that, but we know there will always be fears around that," he said. "I'm sure the privacy fear is always going to be there."

Still, he said the benefits for users and the insurer outweigh the risks. Palin expects the technology will lower costs for disputed claims and reduce the need to perform duplicate lab tests. Blue Cross of Northeast Pennsylvania eventually plans to sell the application, so if a user decides to switch health insurers, the customer could still use the application for an annual fee of around \$20, Palin said.

"We think it has tremendous value," he said of the application. "You can see what the [iPhone](#) is doing for the mobile phone, so you can easily see that the mobile device will be your mobile computer."

Phishing Attacks Becoming More Sophisticated

[NextGov.com \(06/25/08\)](#) ; [Aitoro, Jill R.](#)

Spear phishing attacks—in which cyber criminals target specific individuals with personalized emails in the hopes of capturing personal information such as bank account numbers and passwords—are becoming increasingly sophisticated. In the past, victims of spear phishing attacks had to click on a link in an email and enter personal information in a specific field for the attacker to steal the information. But in the latest wave of spear phishing attacks, victims open up their personal information to theft simply by clicking on an embedded link in the email. When the link is clicked, it launches an application that infiltrates the victim's network to capture personal information. Such attacks are one of the most significant cybersecurity problems facing government agencies today, says Deloitte's Michael Gibbons. Gibbons notes that a group of defense contractors were recently targeted with a phishing email that disguised itself as a legitimate email from a Pentagon employee. The email included a spreadsheet attachment that purportedly contained procurement requirements for several products. When the victims tried to open the attachment, they launched a keylogging application that gave the attackers access to all the information entered into their computers, including user names and passwords. Gibbons says government agencies can protect themselves against similar attacks by providing employees with education and training that helps them recognize phishing attempts.

Laptops Gone Wild

[CSO Magazine \(05/08\) P. 22](#) ; [Overly, Michael](#)

Remote erasure software, a product that allows the owner of a stolen laptop to erase or encrypt its contents from a distance, carries some security risks, writes Michael Overly. Corporate security leaders should be aware of a few trends before jumping on board with a remote erasure software security vendor. First, avoid wording in any

contract that allows a vendor to freely access the information on a laptop, aside from the IP address or other data needed to locate it. Though some contracts allow the vendor to partner with law enforcement agents when tracking a stolen notebook, the agreement should include language that binds the vendor to its confidentiality agreement even during an investigation. Also, the contract should ensure that the client is informed about every step of the tracking process, especially in regards to accessing and using stored data. Finally, agreements should hold the vendor responsible for any information destroyed without the consent of the client, regardless of whether the erasure occurred at the hands of a hacker or because of simple negligence.

Data Breaches Are Up 69% This Year, Nonprofit Says

New Laws May Have Increased Reporting

By [Brian Krebs](#)

Washingtonpost.com Staff Writer

Tuesday, July 1, 2008; Page D03

Businesses, governments and universities reported a 69 percent increase in data breaches in the first half of 2008 compared with a similar period in 2007, according to a study by a nonprofit group that works to prevent fraud.

The [Identity Theft Resource Center](#) in San Diego tracked 342 data breach reports from Jan. 1 to June 27. More than one-third of the reports came from businesses, a 27 percent increase over business breaches for all of 2007.

The center found that data breaches among health-care providers and banks also increased. They now account for 15 percent and 10 percent of the breaches, respectively. Breaches from educational institutions, government entities and the military declined for the third year in a row, the center found.

Yet Linda Foley, the center's co-founder, said it is difficult to say whether the numbers show an increase in breaches, an increase in reporting, or both. She said better state laws on data breach notification also might be encouraging more companies to audit their own security measures.

"Part of this may be that organizations are finding out about more breaches because they're really starting to look for them," Foley said. "The other part is that companies are coming forward because they want to control the flow and spin of the disclosure."

Hacking was the least-cited cause of data breaches in the first six months of this year. Instead, lost or stolen laptops and other digital storage media remain the most frequently cited cause of data breaches, accounting for more than 20 percent of all reported cases, the center found. The inadvertent posting of personal and financial data online prompted roughly 15 percent.

Although the share of breaches from laptops and other mobile media fell nearly 8 percentage points from last year, breaches caused by information stolen by someone inside the company increased from 6 percent in all of 2007 to nearly 16 percent so far this year. An additional 13.5 percent of breaches came from subcontractors who lost or stole their clients' customer data.

The breaches studied this year involved almost 17 million consumer records. Foley said the true number of records jeopardized by those breaches is probably far higher. In nearly 40 percent of the breaches, the companies have not disclosed how many consumer records were lost or stolen.

Some 44 states and the District now have laws requiring companies and organizations that experience a data loss or breach to alert affected consumers.

But Foley said that just three states -- Maryland, New Hampshire and Wisconsin -- require reporting to state officials and routinely publish that information online.

Notices filed within those three states have in many cases amounted to the first public disclosure of data breaches, but they also expose the gaps in the disclosure laws, Foley said.

On June 9, the United Transportation Union Insurance Association notified the Maryland attorney general that the loss of an employee laptop jeopardized the names and Social Security numbers of 394 Maryland residents. The group hasn't previously disclosed how many records nationwide were affected by the breach, but spokesman Frank Wilner estimated that the number exceeds 30,000.

Wilner said his organization would support one of several bills before Congress designed to create a federal breach notification law that would standardize state requirements and potentially centralize reporting of breaches.

"We had to put our law department to work for three days just to figure out what to do because of the hodgepodge of state laws," Wilner said. "More time was spent researching various state laws than trying to figure out how to remedy the problem."

Survey: More than 10,000 laptops lost each week at airports

They're most often lost at security checkpoints, the Ponemon Institute says

By Agam Shah

- June 30, 2008 (IDG News Service) Keep laptops close at airports, because they have a startling tendency to disappear in the blink of an eye, according to a new survey.

Some of the largest and medium-size U.S. airports report close to 637,000 laptops lost each year, according to a [Ponemon Institute](#) survey released today. Laptops are most commonly lost at security checkpoints, according to the survey.

Close to 10,278 laptops are reported lost every week at 36 of the largest U.S. airports, and 65% of those laptops are not reclaimed, the survey said. Around 2,000 laptops are recorded lost at the medium-size airports, and 69% are not reclaimed. The institute conducted field surveys at 106 airports in 46 states and surveyed 864 business travelers.

The five airports with the most missing laptops reported were Los Angeles International, Miami International, John F. Kennedy International, Chicago O'Hare and Newark Liberty International, the study said. Travelers seem to lack confidence that they will recover lost laptops. About 77% of people surveyed said they had no hope of recovering a lost laptop at the airport, with 16% saying they wouldn't do anything if they lost their laptop during business travel. About 53% said that laptops contain confidential company information, with 65% taking no steps to protect the information.

Airports, along with hotels and parked cars, are places where laptops can be easily stolen, the [U.S. Federal Trade Commission](#) said on its [Web site](#). The confusion of going through security checkpoints can make it easy for travelers to lose track of their laptops, making it "fertile ground for theft," the FTC said.

The FTC recommends people treat laptops "like cash." Like a wad of money, a laptop in public view, such as in the back seat of a car or at the airport, could attract unwanted attention. The FTC also recommends using tracking devices such as Absolute Software Corp.'s [LoJack](#), which can help track down a stolen laptop by reporting its location once it is connected to the Internet. Lenovo Group Ltd. last week announced that it would offer the LoJack option in its upcoming [ThinkPad](#) SL series of laptops.

Attaching bells and whistles that sound off after detecting laptop motion could also minimize the chances of theft, the FTC says.

Laptop theft is fairly prevalent in the U.S., said Mike Spinney, a spokesman for the Ponemon Institute. In a study conducted by the institute, 76% of companies surveyed reported losing one or more laptops each year, of which 22% were due to theft or other criminal mischief.

Many people are too ashamed to report lost laptops, knowing they left the computers out where they shouldn't have been, Spinney said.

The Ponemon survey was commissioned by [Dell Inc.](#), which today announced new security services to commercial customers, including tracking and recovery of lost laptops and data-theft prevention.

Dell's laptop-tracking service uses technology to locate and recover lost laptops, including GPS. The data protection services include the ability to remotely delete data on a hard drive and services to recover data from failed hard drives.

- [US Border Agents Copying Contents of Travelers' Laptops](#)

Wednesday 25 June 2008

Washington - US border agents are copying and seizing the contents of laptops, cell phones and digital cameras from US and foreign travelers entering the United States, witnesses told a Senate subcommittee Wednesday.

Washington - US border agents are copying and seizing the contents of laptops, cell phones and digital cameras from US and foreign travelers entering the United States, witnesses told a Senate subcommittee Wednesday. The extent of this practice is unknown despite requests to the Department of Homeland Security from the Senate Subcommittee on the Constitution and several nonprofit agencies.

The department also declined to send a representative to the hearing. Subcommittee Chairman Russ Feingold, D-Wis., said Homeland Security had told him that its "preferred" witness was unavailable Wednesday.

Feingold added that he'd submitted written questions about the seizures of electronic data - and of some devices - to Homeland Security Secretary Michael Chertoff in April. To date, Feingold said, he's gotten no reply.

Chertoff's department provided a written statement that said it wasn't its intention to infringe on Americans' privacy but to protect the country from terrorists and criminals, whose electronic devices can reveal incriminating materials.

During border searches of laptops, according to the statement, the department's Customs and Border Protection officers have found "jihadist material, information about cyanide and nuclear material, video clips of improvised explosive devices being exploded, pictures of various high-level al Qaida officials and other material associated with people seeking to do harm to U.S. and its citizens."

Jayson Ahern, the deputy commissioner of Customs and Border Protection, signed the statement.

Some witnesses noted that the 9th U.S. Circuit Court of Appeals in San Francisco had ruled in a recent child-pornography case that federal agents could seize a laptop computer at the border without reasonable suspicion that its owner was engaged in unlawful activities.

However, several witnesses said that the ruling, by the most liberal of U.S. appeals courts, didn't end their concerns about Homeland Security's refusal to explain the standards for its searches, how it protects privacy, how the seized material is used and who can see or use it.

Three nonprofits - the Electronic Frontier Foundation, the Asian Law Caucus and the Association of Corporate Travel Executives - filed a Freedom of Information Act request last year seeking Homeland Security's answers to those questions. They've gotten none thus far.

They and other groups consider seizures made without probable cause to be an invasion of privacy that leaves the door open to ethnic and racial profiling.

Farhana Khera, the president of Muslim Advocates, a San Francisco nonprofit, said they'd received complaints from Muslim, Arab and South Asian Americans. She said they also had been questioned about their political, religious and personal views.

Retaining confidential computer files also worries business travelers and companies, said Susan Gurley, the executive director of the Association of Corporate Travel Executives, an international group based in Alexandria, Va..

Her organization surveyed its 2,500 members in February, Gurley said. Of 100 respondents, seven said border agents had seized their laptops or their files. Four out of five, she said, were unaware that border agents could seize their electronic data and devices.

Unstructured data at risk in most firms, survey finds

Ponemon study shows dearth of corporate data ownership rules, user monitoring policies

By Brian Fonseca

July 1, 2008 (Computerworld) Corporate information stored on file servers and network attached storage (NAS) devices is in danger of compromise because IT governance policies and access rules in many companies are incapable of dealing with a massive growth of unstructured data, according to a [Ponemon Institute LLC](#) report issued today.

A Ponemon survey of 870 IT professionals found that only 23% believe unstructured data stored by their companies is properly secured and protected.

A wide majority - 84% -- of respondents said that too many workers at their companies can access critical corporate unstructured data. About 76% said their companies have no process in place to control which employees can access specific unstructured data. Such unchecked access could expose internal security gaps and increase the potential for misuse of data, the study notes.

Varonis Systems, Inc., a maker of data governance software, funded the survey.

[Larry Ponemon](#), chairman of the Traverse City, Mich.-based research firm, noted that IT managers say that it's difficult to find automated access control processes that can determine the importance of information the moment it's created.

About 61% of respondents said they cannot keep track of which users access specific unstructured data, and 91% said their organizations lack the ability to determine data ownership because of faulty governance policies and a lack of available storage tools that can remedy the problem.

While IT managers [continue to spend](#) significant sums of money on storage technology to hold rapidly increasing amounts of structured data, many admit that the complexity of unstructured data still makes it difficult to secure it, said Larry Ponemon, chairman of the Traverse City, Mich.-based research firm.

"What we find is not that they won't spend money on it, but they really don't know how to [resolve the issue] because of the complexity; it's a knowledge issue," said Ponemon.

The respondents said that without adequate controls for unstructured data, the top potential problems are insider negligence and deliberate misuse or theft of information from within an organization.

For the study, Ponemon defined unstructured data as electronic information residing on file servers and NAS devices that is not stored in a database or in a document/content management system. He said it can include: e-mail, instant messages, [Microsoft Word](#) documents; [PowerPoint](#) files; electronic spreadsheets; and source code.

Where the truth is: Logs and breach-disclosure laws

Do it right, and your notification burden could be eased

By Anton Chuvakin

July 2, 2008 (Computerworld) Stories detailing the theft of personal information from enterprise databases have filled our news for years and are reaching almost unbearable intensity and frequency. Even [back in 2005](#), it was reported that more than 55 million Americans had their personal data exposed in more than 130 major security breaches. A more recent [survey](#) found that nearly 90% of Fortune 500 companies and government agencies have experienced security breaches (that they know of!)

Consider the infamous TJX breach. The Framingham, Mass.-based retail giant discovered more than a year ago -- and much too late -- that its computer systems were compromised because of an unsecured wireless network and that sensitive customer data was stolen. It wasn't until later that the owners of [T.J. Maxx](#) publicly announced the breach, and even when they announced the breach, they were unaware of the full extent of the damage. Later, TJX made public that the number of affected customers had reached 94 million. Even today, years after the breach, [there are reports](#) of the company's security not being up to the Payment Card Industry Data Security Standard (which is not, to put it mildly, overly stringent). Similarly, another recent intrusion at [Hannaford Bros.](#) highlighted the fact that even complying with PCI does not guarantee that a damaging breach won't happen.

In the wake of each breach came public outcry about corporate responsibility for not only ensuring the security of customer data but also for proper notification of those affected. Compliance mandates such as [PCI](#) provide system and information security requirements for companies. Still, as the Hannaford example shows, a compliant firm can still be successfully compromised and have information stolen. And always, the remaining question is: What are the guidelines for breach notification, the other half of the corporate security responsibility story?

The first security breach notification law (enacted in 2003 and called the California Data Security Breach Notification Law, or CA 1386) requires companies to give individuals early warning in the event that their unencrypted personal information is "accessed by an unauthorized person" (which is nothing but an euphemism for "stolen"). The idea was that with knowledge of a breach, affected people can lessen the effects of the crime by taking steps to protect themselves against further identity theft. In reality, these laws work mostly through forcing the companies to safeguard information because of fear of public embarrassment, which essentially becomes mandatory. CA 1386 gives companies permission to delay notification only if it would impede a criminal investigation.

At that time, California was the only state with legislation requiring the disclosure of security breaches involving personal information. Since then, more than 40 states have passed data security breach disclosure laws, each with unique notification mandates, but all modeled after CA 1386. A national notification law, rather than disparate state laws, would help unify corporate reaction to and notification of security breaches; several bills currently making their way through Congress detail potential requirements. Some countries are also considering such laws, including the U.K., Australia and New Zealand.

For those of you familiar with my writing, you are probably waiting for logs to make their grand entrance. After all, what data security discussion would be complete without mentioning the topic of logs? Indeed, logging requirements are hidden in many regulatory mandates that do not mention "logs" by name. Breach-disclosure laws are a primary example.

I have always championed log data as one of the cornerstones of IT security and one of the best ways to detect unusual activity as well as audit normal user and system activities. Log data is also useful for mitigating the fallout from security breaches since it reveals who accessed confidential customer data, when access occurred and by what methods.

When it comes to information access, logs document both normal and abnormal system usage. Both are essential to identifying and investigating a data breach. But more importantly than knowing who accessed data and when (and whether they were authorized) is knowing what -- and whose -- information has been accessed.

In this way, logs define the parameters of a breach notification and become an essential component of compliance with state laws; they alone can precisely dictate who needs to be notified in the event of a breach. By extrapolating exactly what and whose information was accessed and when, logs take the guesswork out of breach investigation and notification, potentially allowing companies to notify the appropriate people while

avoiding the public relations nightmare of having to notify all their customers or facing the public at large and sheepishly admitting a lack of knowledge of the extent of the breach.

Given the importance of logs to breach-notification laws, you would expect that language about log data collection and organization would fill the pages. However, CA 1386 does not include any specific requirement for tracking log data, thus leaving companies guessing about whom to notify. Of course, that doesn't mean that references to logs can't be found by a discerning eye (the emphasis is mine):

"Notify all affected individuals whose personal information was acquired by an *unauthorized person*. If you cannot identify the specific individuals whose personal information was acquired, notify all those in the groups likely to have been affected, such as *those whose information is stored in the files involved*."

In fact, these phrases are just longer ways of saying, "Look at the logs!" since you can literally save thousands of dollars by notifying only 20,000 people "proven to be affected" as a result of a log review and not the 40 million people whose data happened to have been stored on the server but might not have been taken by the attacker. (Obviously, logs need to be collected and protected from the attackers for the above logic to be defensible.)

To conclude, logs are essential for compliance with breach-notification laws because you know who exactly to notify. Proper log-keeping will save massive amounts of money while complying with both the letter and the spirit of this law.

A final thought: as indicated by the results of some recent surveys, the notification laws might not reduce identity theft through increased consumer awareness, but "shaming people into security their systems" does seem to be working. Is legislation the answer to data breaches? Some say that software vendors whose insecure goods enable the cybercriminals are the ones to suffer the consequences.

A Tax on Buggy Software

Forbes (06/26/08) ; Greenberg, Andy

David Rice, an instructor at the SANS Institute and a former cryptographer for the National Security Agency and NASA, has published "Geekonomics: The Real Cost of Insecure Software," a new book that criticizes the software industry for its careless attitude toward security. Rice says the total economic cost of software security flaws is about \$180 billion a year. Rice suggests creating a tax on software based on the number and severity of security bugs, even if the cost gets passed on to consumers, in order to hold software manufacturers accountable. He says hackers simply use tests to discover flaws in the software, which software publishers could do before hackers have access to the programs. The software companies control how much testing they do before programs are released, Rice says, and they do not have the right incentives to do the testing necessary to create secure software. He says the tax model would solve software problems in the same way that taxes help curb pollution from manufacturing. Rather than trying to stop manufacturing or prohibiting pollution, companies are taxed for the amount of pollution they create, motivating them to reduce emissions. Rice says software vulnerabilities, like pollution, are inevitable, so instead of requiring software to be secure, tax insecurities and allow the market to determine the price it is willing to pay for vulnerabilities in software. Software manufacturers who are the most insecure will pay the most. The tax will also create a system, similar to the safety star-rating system used for cars, to help consumers know what software is the most secure.

IT Spending Ignores Biggest Security Threats

Channel Insider (06/21/08) ; Davis, Jessica

CDW's recent survey of more than 300 IT professionals has found that IT security executives generally do not spend money to deploy the resources necessary to address their biggest security concerns. For example, the survey found that while inappropriate Internet use on the company network was the biggest security concern IT professionals had, only 56 percent of companies had Internet content blocking or filtering software in place. The survey also found that 68 percent of IT executives work for organizations that do not have a distinct policy on security for remote or mobile access, despite the fact that many IT execs are concerned about mobile security issues. CDW's Peyton Engel says there are several reasons why IT executives are not spending money on measures that address their biggest security concerns. For instance, security vendors are selling products that

IT does not need, and IT organizations are buying them because users generally lack an awareness of security issues. In addition, Engel notes that IT organizations tend to be reactive in responding to security issues, spending money on security technology after a specific incident has made the news, for example. To address these problems, vendors should try to help their customers understand the big-picture view of what security issues are so that they can focus on addressing the security concerns affecting their organizations, not the security issues that are simply making headlines.

Opinion: Getting to governance

Asserting information security's place at the management table

By Jon Espenschied

July 7, 2008 (Computerworld) Looking over his glasses with a librarian's stare, an executive recently told me, "You IT people love the word *governance*, but it just seems too...." His voice trailed off as he searched for a way to tactfully convey his sense that "information governance" was a linguistic wedge designed to throw open the doors of [board](#)-level access for unkempt geeks and help desk managers. Instead of "governance," more comfortable phrases were suggested: "information policy board," "data management" or perhaps "IT steering committee."

Governance is a powerful word, and its use in an IT context implies that information is important -- which of course it is. Stripping away the trappings of applications, systems and networks, information is the core asset of most organizations. Establishing information governance is not, as some might think, the elevation of firewall administration to a board-level duty, and it doesn't mean the security controls that protect information subvert all other business processes.

Quite to the contrary, if information governance is planned and managed properly, information security controls end up being close parallels to, or integrated within, existing business processes. It is the establishment and maintenance of a connection between the organization's most valuable [assets](#) and the organization's [control](#) structure. Embracing governance concepts is the admission that we have assets we've [ignored](#) and that there needs to be some sort of structure that makes information tangible, addressable and protected.

"We've got some rules around here"

When challenged to explain information governance to executives, it's easy to digress into academic and philosophical debates over the centrality of information in a business. But that structure -- identifying information so that it's tangible and can be protected -- is the essence of governance. It's the explicit statement that there are rules about how people use processes and technology that affect or protect information.

The good news is that the concepts surrounding governance are becoming more easily understood as the professional dialogue and community body of knowledge becomes more mature and refined. A few years ago, one might have had to dig through the [ISO 20000](#) IT service management (or the IT Infrastructure Library) and [ISO 27001](#) (security management) standards to find the right words about establishment of a "management system" and to explain the desired governance framework for an information-heavy organization. Now there are numerous voices -- some better than others -- providing [definitions](#) and [discussion](#) on the topic.

More recently, respectable certifications have become available for professionals involved in the establishment or operation of information governance systems. For example, the Information Systems Audit and Control Association ([ISACA](#)) is administering its first test for the Certification in the Governance of Enterprise IT ([CGEIT](#)) this fall.

To measure is to know, as the adage goes, and as more people buy into these programs and refine the collective understanding, the closer we collectively get to [Dan Geer's](#) goal in *Measuring Security* ([download PDF](#)): "To move from a culture of fear to a culture of awareness and then a culture of measurement."

Who's in charge?

Establishing a structure is all well and good, but even when information is recognized as a high-value asset, many organizations still stuff the responsibility for its definition and protection down into low-level records and IT roles. This simply doesn't work, because those roles often don't have the authority to properly implement or manage the controls, and the new responsibilities take second place to existing job tasks.

For example, information classification ([download PDF](#)) is required in order to qualitatively categorize and determine what controls are appropriate to protect information, but does an IT director have the authority to mandate a classification scheme for an organization? Such attempts are often dismissed as data classification, when in fact the effort ought to apply across business units.

Likewise, would it be appropriate for IT to change the business rules for [access](#) to information because of a technical limitation or new feature? It's unfortunately common for organizations to become enamored with new connectivity features in a data repository or interface and to use that to open remote access or data interchange for remote partners. But just because you can doesn't mean you should. Access changes should be driven forward by business need and backward by risk. Technical capability is a secondary question for IT.

< merits. met??) be directives your (?Can policy and problem??) right the on working we (?Are goal their but involved, tech of love for not executives board-level or management senior to issues raises leader governance information An organization. given any within it advancing vision that having someone has There own. its happen doesn?t But it. all I?m then need, business coherent a serve track coordinated controls tasks multiple keep structure goals leadership overarching refers ?vision? if anyone, as effluvia meaningless averse vision. direction are needed What>

A limiting factor is that the [larger cycle](#) of information includes requirements gathering, governance, metrics, process controls, technical controls and audit -- and then a loop back to revision of requirements, governance feedback and adjustment, and so on, again and again. IT owns the [middle](#) of this sequence, but not the requirements, audit, or other beginning or end tasks. Someone needs to lead the beginning and end to ensure the middle (the IT part) connects and aligns with the rest.

This is why IT managers or directors are a poor choice for information governance leaders: One can't simultaneously be responsible for the implementation of controls and the audit of whether those controls work properly. A governance leader might be a senior manager or director who handles information in all forms (such as physical and electronic records management), or an executive responsible for compliance. But putting information governance program establishment or reform under the IT organization makes it control-focused, not asset-focused or performance-oriented.

Being serious

Information governance and effective security are emerging as equivalent to proper business process. Security nirvana is achieved when security controls asymptotically become indistinguishable from [right](#) and proper business process, and alerts from business process variances and security control breaches are one and the same.

Bruce Schneier recently espoused the idea that security has to be "[sold](#)" on one side of the balance sheet or the other; either it enhances the profit centers and adds to the bottom line, or it reduces actual loss. However, when information security controls end up being close parallels or integrated within existing business processes, it means less selling, less disconnection and fewer moments where executives perceive information governance as some kind of power grab from IT.

File-sharing breach at investment firm highlights dangers of P2P networks -- again

Supreme Court Justice among clients hit by data exposure after worker used LimeWire software

By Jaikumar Vijayan

July 9, 2008 (Computerworld) Wagner Resource Corp. recently learned the hard way what [Pfizer Inc.](#) and many other companies have similarly discovered in the past: installing peer-to-peer file-sharing software on corporate computers is [a bad idea](#).

The Alexandria, Va.-based investment firm last week had to notify about 2,000 of its clients that their names, Social Security numbers and birth dates had potentially been exposed on the [LimeWire](#) P2P network, according to a story [published](#) Wednesday by [The Washington Post](#). Among the individuals whose personal data was exposed in the Wagner compromise was Supreme Court Justice Stephen Breyer, according to the *Post*.

Wagner didn't immediately respond to a request for comment about the incident. But the *Post* reported that the compromise resulted from the use of LimeWire's file-sharing software by a Wagner employee. The employee apparently downloaded the software to his company-issued PC last year, so he could share music and other media files with fellow LimeWire users. But the software ended up exposing all of the contents on the employee's computer to other users of the [P2P network](#).

The *Post* said that the leak wasn't discovered until last month, when one of its online readers found the data about Wagner's clients while using the LimeWire network.

Breaches such as the one at Wagner highlight the continuing dangers that companies face from employees using P2P software on their work computers, said Christopher Gormley, chief operating officer at Tiversa Inc., a Cranberry Township, Pa.-based P2P network monitoring firm that Wagner has hired to try to help it mitigate the data leak.

The P2P software offered on networks such as LimeWire and [Kazaa](#) is designed to help users easily share media files, and to aid them in finding files on the computers of other users. The problem is that if P2P users aren't careful, the software can expose not just the media files they want to share but almost everything else on their computers.

Numerous organizations have suffered data leaks as a result of such carelessness. Last year, for instance, the personal data of about 17,000 Pfizer employees [was exposed](#) after an employee installed unauthorized P2P software on her laptop. And at a Senate hearing last year, lawmakers heard testimony from several witnesses [about the abundance](#) of classified government and military documents as well as corporate data freely available on P2P networks.

The data said to be available included a full diagram of the Pentagon's secret backbone network infrastructure, complete with IP addresses and password-change scripts; contractor data on radio-frequency manipulation techniques for dealing with improvised explosive devices in Iraq; the complete minutes of a board meeting held at a large financial services company; and the detailed launch plan of a start-up company, complete with growth targets and other business forecasts.

Despite such examples, and the fact that the dangers of P2P networks have been talked about for several years now, there continues to be an almost startling lack of awareness of the threat that file-sharing software can pose to corporate data, Gormley said.

"There's a lack of awareness across the board," he said. Few companies know about either the need for or the existence of controls for preventing P2P data leaks from occurring, according to Gormley. In addition, companies often have a poor idea of the amount of sensitive data that is being taken beyond their network perimeters on corporate laptops or systems belonging to contractors, service providers and business partners, he said.

Further exacerbating the problem, Gormley said, is the increased searching and scouring of P2P networks by cybercriminals looking for data they can use to commit fraud or espionage. On average, about 1.5 billion searches take place on P2P networks daily compared with 180 million on [Google](#), he claimed, adding that a growing number of the searches are being done for malicious purposes. Gormley said that Tiversa also has noticed the emergence of several data aggregators whose sole purpose seems to be collecting information on P2P networks for their own illegal uses or to resell to other miscreants.

The key to limiting P2P exposures is to have not just the proper controls in place but also policies for enforcing them, said Phil Neray, a vice president at database security software vendor Guardium Inc. in Waltham, Mass. It's hard to completely prevent employees from downloading P2P software, because some people will find a way around the controls, Neray said. So, he added, the focus should be more on monitoring and filtering the content that is traveling into and out of corporate networks, in order to stop sensitive data from leaking out.

The Mark of the Beast Is Located in Aisle Six, Adjacent to Frozen Foods

CISO Paul Raines ponders biometrics, religion and privacy in a Dutch grocery store

By [Paul Raines](#)

July 08, 2008 — I grew up in a fundamentalist Baptist church in a rural southern town. I have since moved on to drastically different positions both physically and spiritually, but I was reminded of those roots during a recent visit to--of all places--a grocery store in Holland. The national grocery chain, Albert Heijn recently decided to test a new method of checking out customers. Under a pilot program called Tip2Pay, store customers can pay for their groceries at the checkout counter by simply scanning their fingerprint. (See <http://www.ah.nl/albertheijn/persberichten/article.jsp?id=486644> —sorry, the press announcement is in Dutch, but there's an accompanying photo.)

As a security professional, I immediately recognised that the store was utilising biometric technology to authenticate frequent customers who had pre-registered their contact and payment details with the grocery chain and who had given their consent for the store to debit their bank account after proper authentication. From a customer service perspective it made perfect sense. I could go to the grocery store on the weekend without having to take my wallet or pocket book. That's very important to a nation that uses bicycles to travel—the less I have to carry the better.

However, remembering back to the days of fire-and-brimstone sermons in the heart of the Bible Belt, I immediately knew how this would be viewed in that community. You see, fundamentalists take what is written in the Bible literally and in the book of Revelation it is written:

"He (the Anti-Christ) also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead, so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name." Revelation 13:16-17 (NIV)

Hmmm, does a fingerprint qualify as a mark on the hand? Really doesn't matter because with the fundamentalist crowd would see it as the camel's nose-under-the-tent, the foot-in-the-door, the first step on the slippery slope to Hades and it must be nipped in the bud. Nipped, I tell you. Nipped-in-the-bud, period.

A second group opposing the introduction of fingerprint scanning are privacy advocates. They would say that fingerprints are too intrusive. If the local grocery store has your fingerprint, what are they doing with it? Are they selling it to interested third parties? Sharing it with the government? If someone has a copy of your fingerprint,

does that mean that you could be framed for a crime that you didn't commit? It seems like it would be pretty easy to fabricate your fingerprints at the scene of a crime and thus make it appear that you had been there.

Even if Albert Heijn is sincere and diligent in protecting the information and are sharing your fingerprint with no one else, there are still no guarantees. Suppose their database got hacked? Or suppose they were like the U.S. telecommunications companies who, when asked (coerced?) by the government, acquiesced in illegally spying on Americans? That happened and it's likely that those companies will face no legal action from having done so. If it happened with telecommunications companies and phone lines it could just as easily happen with grocery store chains and fingerprint scans.

These two groups, the religious fundamentalists and the privacy advocates, make unlikely political bedfellows. Yet, as the saying goes, the enemy of my enemy is my friend. So, they may yet make common cause against this system.

The Netherlands has a strong privacy advocate group and there is the Data Protection Act which governs how corporations use private citizen data. There is also a Bible Belt in the Netherlands, although the Christian population in the Netherlands is considerably smaller as a percentage of the overall population, has less influence in politics, and is less fundamentalist in nature than are their American counterparts.

The program is currently in a pilot phase and will stay that way for six months. After that time it will be evaluated and, if successful, it will be deployed on a nationwide basis. Who knows? If it succeeds in grocery stores, it may be introduced to other vertical markets. If it succeeds in The Netherlands, it may be introduced in other countries.

This new payment system may be quietly flying under the radar screen for now because it is only being deployed in one grocery store. However, if and when it goes national it will attract everyone's attention—including the two aforementioned groups. When that happens Albert Heijn had better be ready for the questions and the hostility that will inevitably follow. ##

Senate Grapples With Web Privacy Issues

Washington Post (07/10/08) P. D3 ; Whoriskey, Peter

Despite support from leading technology companies and frequent consumer complaints, Congress has been unable to pass Internet privacy legislation. Following a two-hour Senate committee hearing yesterday on Internet advertising and privacy, Sen. Byron L. Dorgan (D-N.D.), who led the discussion, said the hearing primarily served to emphasize how little legislators understand about the subject. The hearing was called in response to fears that the massive volume of information that Internet companies are collecting on users is violating their privacy. The practice of assembling profiles on users to determine personal preferences and activities has been going on for years, but as Web sites have increasingly been united in large ad networks, the various profiles kept by smaller sites have been combined to create more detailed and widespread user profiles. Over the past year, some Internet service providers (ISPs) have been experimenting with a practice that would provide even more detailed profiles, using a technology called deep packet inspection, which allows them to examine streams of data coming from a user's Internet connection. Critics of deep packet inspection compare the practice to wiretapping. At the hearing, representatives from companies that provide deep packet inspection services to ISPs assured the panel that they were doing their best to preserve privacy. Experts say that before Congress can pass privacy legislation it must first decide what constitutes personally identifiable information, whether a person's Internet address should be considered private, should people be informed about data collection practices, and should users be allowed to see profiles compiled about them.

Spying Has Few Legal Checks

Baltimore Sun (07/07/08) P. 1A ; Olson, Bradley

U.S. citizens' communications, travel patterns, and spending habits are being monitored and analyzed for suspicious activity by domestic surveillance programs run by federal intelligence and law enforcement agencies, and these programs have few legal restrictions. Although protecting Americans' privacy is the goal of provisions contained in pending amendments to the Foreign Intelligence Surveillance Act, there is little oversight for surveillance programs that fall outside the bounds of FISA. Critics say the safeguards are not infallible, while Congress has often held back funding for surveillance programs because it is dissatisfied with the information the administration has provided about the programs. Such was the reasoning behind the House Appropriations

Committee's recent decision to stall funding for an initiative by the National Applications Office to use American satellites for domestic purposes until August, when the Government Accountability Office will issue a report about how the program will address civil liberties and privacy concerns. Lawmakers say even in instances where Congress has received information about surveillance programs, their questions or concerns are frequently handled by the agency responsible for surveillance, which adds up to self-policing. Partially to address concerns about privacy, the Homeland Security Department has set up a privacy czar to guarantee that the technologies and programs initiated by the agency do not violate civil liberties or chip away at privacy laws, but some believe the position should be expanded to a Cabinet-level post in the executive branch. "We should have what Canada has, which is a minister of privacy, someone looking out for the privacy issues of Americans," says intelligence expert James Bamford. "We have armies of people out there trying to pick into everyone's private life, but we have nobody out there who's an advocate."

Data Leaks Emerge as Worst Security Threat

VNUNet (07/01/08) ; Jaques, Robert

End users are the second biggest threat to corporate security after viruses, concludes a Trend Micro study. The survey polled 1,600 employees in the United States, United Kingdom, Germany, and Japan, and only 6 percent admitted they had shared sensitive information, while 16 percent of respondents believed other employees were responsible for data leaks. U.S. workers are most confident in their abilities to keep a secret; about 74 percent said they understand the difference between privileged and proprietary information, compared to 68 percent in Germany, 67 percent in the United Kingdom, and 40 percent in Japan. Nearly 80 percent of mobile end users and 69 percent of desktop computer users can identify confidential data, but companies in Germany and Japan are more likely than companies in the United States and the United Kingdom to write data leak prevention policies. Across the board, large companies are more likely than smaller companies to have preventative policies, and security software is the weapon used most frequently to prevent data breaches.

Identity Problems

National Journal (07/05/08) Vol. 40, No. 27, P. 22 ; Carney, Eliza Newlin

Outfitting virtually all U.S. citizens with fraud-resistant IDs has proven to be a major challenge from a practical as well as emotional point of view, with a multitude of technical, legislative, administrative, and ethical obstacles impeding progress. Events and trends fueling the drive for more reliable IDs include the 9/11 terrorist attacks, the push to deter illegal immigration, credit-driven commerce, the threat of identity theft, and technological innovations in identity verification methods. A sore point among various parties is the Real ID Act, which has come under fire for being passed without public debate or hearings, and for receiving inadequate federal funding. Real ID sets up federal standards for issuing driver's licenses, and dictates that states must link their databases in order to enforce the law's prohibition on drivers holding licenses from multiple states, which critics warn would create an irresistible target for hackers and ID thieves. Some experts believe a national, biometric ID card is the solution. "Right now, we are proceeding in hundreds of different ways, for dozens of different IDs, at tremendous expense," says Robert Pastor, co-director of American University's Center for Democracy and Election Management. Privacy experts favor a scheme in which Americans carry multiple smart cards with different applications, arguing that a single ID would reduce Americans' security. "Uniformity in IDs across the country would create economies of scale" for snoops and could help bring about a surveillance society, warns the Cato Institute's Jim Harper.

