

Security Trends Report

03/09

A Real Dumpster Dive: Bank Tosses Personal Data, Checks, Laptops

In this new age of data protection, where most information is stored digitally and paper shredding is commonplace, you don't need to worry about private information ending up in the garbage, right? Steve Hunt shows that assumption is just plain wrong

By [Joan Goodchild](#), Senior Editor

March 18, 2009 — [CSO](#) —

Data protection is not just an IT security issue. But security industry analyst [Steve Hunt](#), who heads up Hunt Business Intelligence, believes too many people in IT security still have that false perception.

"There are so many physical security aspects to data protection it ought to never be considered merely an IT security issue," Hunt said.

Instead, noted Hunt, sensitive data is sitting on USB drives, in the garbage, in the discarded fax pile and plenty of other places, waiting to be found by criminals.

Good old-fashioned dumpster diving. It might sound like a 90s tactic, but Hunt thought it would still work as a way to garner sensitive information. With that in mind, Hunt headed to the trash bin at what he describes as "a big bank in a big city." He was in and out of the dumpster in three minutes, according to his estimate. In that short amount of time he came up with the following items

Wire transfer information

Hunt obtained the wire transfer information of many transactions. The documents he found included transfer information for transactions between US banks and banks in Jordan, Saudi Arabia, Dubai and Portugal. The documents included the account numbers and social security numbers of both the sender and the receiver, and their names.

Check copy

Hunt found a clear and easily-readable copy of a bank check with all of the important information: Bank account number and routing number and name of the account holder. The account holder's social security number and small business ID number were hand written in on the top right of the check.

Bank account transaction history

The dive also turned up the bank account numbers, balances and banking activity for the fundraising account of "a certain prominent politician in the area," according to Hunt.

Personal financial statement

Hunt found the personal financial statement of an individual he described as "very wealthy." The documents list the person's name, home address, real estate owned and values of the properties, several of the individual's bank account numbers, social security number and date of birth. Hunt Googled the name and easily found a picture of the person.

An entire, intact PC

Hunt's experiment even yielded a whole laptop with a tag on the back that says "Property of [another financial institution]". While the computer had no power and Hunt was not able to power it up, "I know how to connect to a hard drive," he noted.

Technology leaps beyond Florida public records laws

By [Cristina Silva](#), Times Staff Writer

February 17, 2009

President Barack Obama isn't the only government employee addicted to his BlackBerry.

Communication gadgets are becoming increasingly pervasive in daily government operations, from cell phones to personal computers to handheld devices.

But Sunshine Law advocates say Florida's open government laws have failed to keep pace. They worry these new devices could be creating a troubling black hole of public records.

"It's a problem," said Adria Harper, director of First Amendment Foundation in Tallahassee. "We just have to hope that our public officials are following the Sunshine Law and not trying to evade it."

State law requires that any records made in connection with official business be saved for public inspection. But it doesn't address newer technologies, including text messages, personal e-mail accounts or instant messages. Government workers say the very nature of these mediums make them nearly impossible to monitor or capture.

The state is only beginning to address these issues.

Gov. Charlie Crist's Commission on Open Government Reform released a report last month that recommended all agencies adopt policies and procedures to ensure public records created on personal computers are disclosed and retained according to law.

The nine-member commission also recommended "all agencies adopt policies that prohibit the use of text and instant messaging technologies during public meetings and/or hearings." This would prevent a government body from, say, conducting a private policy debate before a public vote.

The commission determined exchanges such as text messages and other "such messages which are transitory in nature, are analogous to the spoken word and the public records law most likely does not apply," according to the report.

Officials from the state Attorney General's office, however, say using text messages to skirt public record rules violates the law's spirit.

But because the ability to retain text messages varies so widely between cellular service providers, it is unlikely the state would be able to obtain the evidence necessary to prosecute.

"If you don't have evidence, you can't convict," said Alexis Lambert, Sunshine Law attorney for the Attorney General's Office.

AT&T, for example, removes text messages from its system once they are delivered to the intended wireless

device. Even with a subpoena, the records cannot be retrieved, said spokeswoman Kelly Starling.

No easy solutions

Government officials in the Tampa Bay area say there is little that can be done to ensure employees abide by the Sunshine Law other than to discourage certain technologies.

"We try to manage what we can control," said Muslim Gadiwalla, chief information officer for the city of St. Petersburg. "This whole area is fairly new. Five years ago no one thought about any of this."

The city removed text messaging capabilities from most city phones in October after an employee racked up excessive charges, Gadiwalla said.

Pasco County doesn't provide cell phones to its employees, and text messages are disabled on all county BlackBerry accounts. But governments can't keep tabs on what employees do with their personal communications devices.

"If there is any texting that goes on with their own private phones, you would have to think that is only for their private use and it's not county business," said county spokesman Eric Keaton. "The county does not see that as something that needs to be monitored."

Others governments have embraced text messages despite the medium's ephemeral nature.

In Tampa, employees use them to stay in touch.

"I think we are more texting each other to say, 'Hey I'm at this address, I need this thing to do this work,' like, 'I'm a water person and I need an 8-inch pipe,' " said James Buckner, the city's chief information officer. "I like to think that's what it all is, but I really don't know."

Bucnker said Tampa automatically archives all employee e-mails and department directors must approve any new cell phone lines.

Impenetrable privacy

The city, however, can't capture communication between employees who log onto public sites such as Gmail, Facebook or AOL Instant Messenger to chat and there are no records of text messages sent to or from employee BlackBerry accounts.

"It's no different than voice communication. We are sitting here talking to each other on the telephone and that's not being recorded," said Buckner. "There is just going to be an ongoing challenge to be able to capture all government communication and I don't know if we are ever going to be able to get there."

Government officials also allow employees to self select which of their records are personal or public.

For example, when the *Times* requested to review text messages sent by St. Petersburg's lobbyist — one of a handful of city employees who still have text messaging service — the city said her 865 text messages were private, and therefore not public record. She reimbursed the city for at least \$113 in charges.

Recession raises threat of data walking out the door

By Chris Parkerson

February 11, 2009 (Network World) Moving into 2009, the number of [layoffs](#) and unemployed has multiplied as a result of the falling economy. Corporate data is at risk now more than ever and companies need to be sure they have reliable protection in place.

As companies are forced to make layoffs, [disgruntled employees](#) may act maliciously and take sensitive company data with them as they leave. Out-of-work employees worried about finding a position in a bleak job market may also act out of desperation and steal confidential company information to get a leg up on the competition for hard-to-find jobs. It is also possible that companies hiring are accepting or even requesting internal data of their competitors as part of the hiring process.

Employees can [confiscate sensitive](#) company data by saving it to a memory stick, e-mailing it to a personal account, or even walking out with a laptop or BlackBerry. Companies need to be protected in all instances to ensure their information doesn't walk out the door.

It's 5 p.m. Do you know where your data is?

The first step to ensure that corporate data is protected from insider threat is to make sure laptops are encrypted. Not encrypting employee machines is a potentially fatal mistake, but it is not the only step to protection. Companies need to make sure the encryption can be revoked when an employee leaves the company. This requires having an encryption policy that is centrally managed by IT. This type of policy will keep data protected while enabling IT to lock it from unauthorized employee access at any time.

The next step is ensuring employees cannot transfer information to a USB, MP3 player or other portable device. Implementing device control allows IT to monitor and restrict data copied to removable storage devices to keep it from leaving company control. Having control over devices on the network also allows IT to understand how internal compliance is working and block any attempts to violate IT policy.

The final step to protecting data on your network is to ensure employees cannot send information outside to personal email accounts or through instant messaging. Putting network data loss prevention ([DLP](#)) in place allows IT to identify, monitor and protect endpoint and network actions in order to prevent the unauthorized use and transmission of confidential company information.

In a down economy the risk of data loss increases. Now, more than ever, companies need to ensure the integrity of their data. Putting significant protection in place should be a first priority in 2009 to ensure data theft is not a risk. Encrypting laptops with flexible encryption controls, implementing device control and putting a data loss prevention system in place will cover all bases and ensure employees don't have any way to walk out the door with company data.

Layoff backlash: Five steps to protect your business from angry ex-employees

Layoffs can spark destructive behavior. Take these steps to protect your company.

By Julia King

March 2, 2009 (Computerworld) A senior corporate executive leaves the company, taking with him his framed family photographs, his prized gold pen-and-pencil set -- and the passwords of several hundred employees.

One of your firm's most experienced sales reps hears a rumor that she is sure to be laid off. And she is, but before she gets her pink slip at the beginning of the next quarter, she manages to download to her Gmail account a long list of A-plus customers and their ordering and payment histories.

If you're thinking "Never at my company" or "Not my employees," [think again](#). Scenarios like those above are playing out every day, experts say, and [even the most trusted and skilled professionals can be driven to data theft](#) and other computer crimes in the face of crippling economic pressures and looming job layoffs.

Recent statistics bear this out. In a late 2008 [survey conducted by IT security firm Cyber-Ark Software Inc.](#), 56% of financial services workers in New York, London and Amsterdam admitted to being worried about layoffs. In preparing for the worst, more than half said they had already downloaded competitive corporate data that they planned to use to get their next jobs.

In the U.S., the percentage was slightly higher, with 58% of Wall Street workers saying they had done so. And 71% of all workers said they would definitely take data with them if they were confronted with the prospect of a layoff tomorrow.

"When people are desperate to pay for the roof over their head or put food on the table, they're capable of doing things they wouldn't normally do, which is why crime goes up when the economy suffers," says David Griffith, vice president of business line integration and reporting at RBS Citizens Bank. "That doesn't go away because you have a bachelor's degree or a master's degree. It's a common fear based on need. You have a different level of comfort with the crime you commit."

Security Tips for Good Times and Bad

Regardless of the economic conditions, IDC recommends taking these steps to ensure that systems will be secure and data will be protected when employees exit:

- Clearly and completely document each worker's access to the network, applications, servers and the physical building.
- Shut down remote connections, including pcAnywhere systems and VPNs.
- Invalidate usernames and passwords.
- If the employee worked in IT, change root access and network access.
- Shut down external access to the telephone system.
- Make sure handhelds, smartphones and cell phones are turned in along with PCs and laptops.
- Collect ID cards.
- Use monitoring software to keep an eye on network traffic.

Supply and Demand

"It makes sense that [data] theft is on the rise when demand is low and supply is high. Right now, there's a huge supply of employees, and if one person can make himself more attractive to a potential new employer, it would

be a great temptation," says Keith Jones, a digital forensics investigator and partner at Jones Dykstra & Associates, a computer security consultancy in Columbia, Md.

Meanwhile, [the legion of laid-off workers continues to grow](#). In the past few months, Citigroup, SAP, Sun Microsystems, IBM, Sprint and Microsoft have all announced layoffs, adding to the tens of thousands of already unemployed people, many of whom are technically savvy and have access to key computer systems, highly sensitive corporate data or both.

What's surprising -- and potentially lethal to corporate security -- is how many departed workers retain such access via so-called orphaned accounts long after they've been discharged. Four out of 10 companies have no clue whether user accounts remain active after employees leave, according to [a study of 850 security, IT and human resources executives by Symark International Inc.](#), a security software company.

In addition, 30% of executives reported that they have no process in place to locate and disable orphaned accounts. Another sorry statistic: 38% of them have no way of determining whether a current or former employee is using or has used an orphaned account to access information.

The most common threat is that an employee may take intellectual property, including strategic plans or customer data, before or soon after he is let go, says Jonathan Penn, an analyst at Forrester Research Inc.

And things can get even more dicey when IT staffers are laid off. Often, these are employees with "the keys to the kingdom," says Jones.

He notes that Roger Duronio, a former IT worker at UBS Paine Webber who was [convicted and sentenced to eight years in prison](#) for planting a software logic bomb, was able to do such extensive damage to company data because "he had access everywhere." (A logic bomb is software code that triggers malicious functions under certain prescribed conditions; for example, one could be set to delete all customer accounts at a particular time on a specific date.)

Systems administrators and users with privileged account access -- such as those who know root passwords -- can definitely pose a greater threat, says Sally Hudson, an analyst at market research firm IDC. "Those with access to privileged passwords possess the power to change system data, user access and configuration. They also have the power to easily sabotage the critical IT operations of any organization," she says.

Despite these vulnerabilities, there are steps that companies can take to limit potential damage, especially when conducting layoffs.

Do your homework. Exit strategies and security measures should vary depending on the employee's role. Executives and managers who are charged with laying off personnel shouldn't assume that disabling computer access is simply a matter of pulling a plug.

"Before you lay off, look closely at the classes of people," advises Jones. "If they're from sales, HR or finance or [are] senior employees, it may take longer to [disable their access] because they have greater access to systems" than other employees do.

Involve IT in layoff plans as early in the process as possible. "It's important for IT to be synchronized tightly with HR," says Ken van Wyk, an information security specialist and consultant in Alexandria, Va. "But IT people need to understand how sensitive their roles are, and there has to be zero tolerance for spreading rumors. If an IT person tells people that they're going to be laid off, that IT person also needs to be included in the exit roster."

Make sure the proper security programs and policies are in place well before the layoff, advises IDC's Hudson. Among other things, you should make sure you're using systems to secure content, prevent data loss and manage threats. Such systems include firewalls, content- and spam-filtering tools and antivirus software.

You should also have a secure identity and access management infrastructure. Also known as an IAM, this type of setup "controls the who, what, where, when and why of user activities throughout the enterprise," Hudson explains. Having the ability to monitor and evaluate how access rights are being used is critical to meeting governmental mandates and identifying system misuse.

Compartmentalize system access according to employees' roles. This is a secure system design principle that companies should implement at the beginning of any software-development effort. "Access control means tightening up a lot more on the business logic layer," explains van Wyk.

But all too often, companies forgo this step "because it requires more time and thinking through of the design of software," he says. In the absence of an initial secure design, the next best measure is to implement software that records users' access to systems and the actions they take while using various business applications, van Wyk says.

"Almost all business applications have some level of user ID and password security, and then, once you're in, you're in," he says. But with a tracking system, when a user goes into a database, everything that he does there is recorded -- and potentially reported to law enforcement, van Wyk explains.

Part on good terms, but plan for bad times. Jones recommends that even if a layoff goes smoothly with no apparent disgruntlement on the part of the employee, a company should still collect evidence of its own due diligence in case there's some sort of investigation in the future.

That's because companies that experience any kind of security breach, including the theft of data by a laid-off employee, must be able to show that they took all possible precautions and measures to protect that data.

Bill proposes ISPs, Wi-Fi keep logs for police

STORY HIGHLIGHTS

Politicians are calling for a federal law to save Internet users' records for police use

Law would apply to all Internet providers and operators of millions of Wi-Fi spots

It would require providers to keep records for two years to aid police investigations

Republican-led bill is certain to draw fire from businesses and privacy advocates

By Declan McCullagh 

(CNET) -- Republican politicians on Thursday called for a sweeping new federal law that would require all Internet providers and operators of millions of Wi-Fi access points, even hotels, local coffee shops, and home users, to keep records about users for two years to aid police investigations.

The legislation, which echoes a measure proposed by one of their Democratic colleagues three years ago, would impose unprecedented data retention requirements on a broad swath of Internet access providers and is certain to draw fire from businesses and privacy advocates.

"While the Internet has generated many positive changes in the way we communicate and do business, its limitless nature offers anonymity that has opened the door to criminals looking to harm innocent children," U.S. Sen. John Cornyn, a Texas Republican, said at a press conference on Thursday.

"Keeping our children safe requires cooperation on the local, state, federal, and family level."

Joining Cornyn was Texas Rep. Lamar Smith, the senior Republican on the House Judiciary Committee, and Texas Attorney General Greg Abbott, who said such a measure would let "law enforcement stay ahead of the criminals."

Two bills have been introduced so far--S.436 in the Senate and H.R.1076 in the House. Each of the companion bills is titled "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act," or Internet Safety Act.

Each contains the same language: "A provider of an electronic communication service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user."

Translated, the Internet Safety Act applies not just to AT&T, Comcast, Verizon, and so on--but also to the tens of millions of homes with Wi-Fi access points or wired routers that use the standard method of dynamically assigning temporary addresses. (That method is called Dynamic Host Configuration Protocol, or DHCP.)

"Everyone has to keep such information," says Albert Gidari, a partner at the Perkins Coie law firm in Seattle who specializes in this area of electronic privacy law.

The legal definition of electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." The U.S. Justice Department's position is that any service "that provides others with means of communicating electronically" qualifies.

That sweeps in not just public Wi-Fi access points, but password-protected ones too, and applies to individuals, small businesses, large corporations, libraries, schools, universities, and even government agencies. Voice over IP services may be covered too.

Under the Internet Safety Act, all of those would have to keep logs for at least two years. It "covers every employer that uses DHCP for its network," Gidari said. "It covers Aircell on airplanes-- those little pico cells will have to store a lot of data for those in-the-air Internet users."

In the Bush administration, Attorney General Alberto Gonzales had called for a very similar proposal, saying that subscriber information and network data should be logged for two years.

Until Gonzales' remarks in 2006, the Bush administration had generally opposed laws requiring data retention, saying it had "serious reservations" about them. But after the European Parliament approved such a requirement for Internet, telephone and VoIP providers, top administration officials began talking about the practice more favorably.

After Gonzales left the Justice Department, the political will for data retention legislation seemed to ebb for a time, but then FBI Director Robert Mueller resumed lobbying efforts last spring.

This tends to be a bipartisan sentiment: Attorney General Eric Holder, a Democrat, said in 1999 that "certain data must be retained by ISPs for reasonable periods of time so that it can be accessible to law enforcement." Rep. John Conyers, the Democratic chairman of the House Judiciary Committee, said that FBI proposals for data retention legislation "would be most welcome."

Smith, who sponsored the House version of the Internet Safety Act, had previously introduced a one-year requirement as part of a law-and-order agenda in 2007.

A 1996 federal law called the Electronic Communication Transactional Records Act regulates data preservation. It requires Internet providers to retain any "record" in their possession for 90 days "upon the request of a governmental entity."

Because Internet addresses remain a relatively scarce commodity, ISPs tend to allocate them to customers from a pool based on whether a computer is in use at the time. (Two standard techniques used are the Dynamic Host Configuration Protocol and Point-to-Point Protocol over Ethernet.)

In addition, Internet providers are required by another federal law to report child pornography sightings to the National Center for Missing and Exploited Children, which is in turn charged with forwarding that report to the appropriate police agency.

The Internet Safety Act is broader than just data retention. Other portions add criminal penalties to other child pornography-related offenses, increase penalties for sexual exploitation of minors, and give the FBI an extra \$30 million for the "Innocent Images National Initiative."

Starbucks Facing Lawsuit Over Laptop Theft

(February 23, 2009) A Starbucks employee has filed a class action lawsuit against the company in response to a data security breach that occurred on October 2008. A laptop containing the names, addresses and Social Security numbers (SSNs) of approximately 97,000 Starbucks employees was stolen last fall; the suit alleges fraud and negligence, and seeks an extension of the one year of credit monitoring the company offered as well as unspecified damages and assurances that Starbucks will be required to undergo regular third party security audits.

More Than Half of Former Employees Took Company Data

(February 23, 2009) The Ponemon Institute interviewed 945 US adults who had been laid-off, fired, or changed jobs within the last year and found that more than half took company information with them when they left their former positions. The rationales for taking the data included help getting another job, help starting their own business, or simple revenge. All of the participants in the survey had access to proprietary information, including customer data, employee information, financial reports, software tools and confidential business documents. The survey also found that just 15 percent of the companies examined the paper and/or electronic documents their former employees took with them when they left.

Legislator moves to limit Google Maps because of terrorist threat

California bill would cloud details in images of schools, government buildings, churches

By Sharon Gaudin

March 4, 2009 (Computerworld) A California state legislator has submitted a bill that would limit the amount of detail allowed in images available from applications such as [Google Maps](#) and Google Earth, contending that [terrorists are using](#) such online tools to plot attacks.

Assemblyman Joel Anderson submitted Bill AB 255 to the California legislature on Feb. 11. The bill, which is waiting to go to committee, would not allow online mapping tools from companies such as Google Inc. to provide aerial or [satellite images](#) of schools, places of worship, government buildings and medical facilities unless they have been blurred.

Anderson told *Computerworld* that he is looking to limit the amount of detail that Internet users can see.

"We heard from terrorists involved in the Mumbai attacks last year that they used Google Maps to select their targets and get knowledge about their targets. Hamas has said they were using Google Maps to target children's schools," said Anderson. "What my bill does is limit the level of detail [\[in Google Earth\]](#). It doesn't stop people from getting directions. We don't need to help bad people map their next target. What is the purpose of showing air ducts and elevator shafts? It does no good."

Elaine Filadelfo, a spokeswoman for Google, said they are hoping to have a sit down with Anderson and talk about his concerns.

"We are happy to speak with Assemblyman Anderson's office regarding this legislation and hope to have a productive conversation," she added. "Google Maps and Google Earth provide users with a rich, immersive experience, offering useful information and enabling greater understanding of a specific location or area."

Anderson said he's not against online mapping and has sat down with Google officials to talk about other issues in the past. "My door is open," he said, adding that he hopes Google will help him craft future drafts of the legislation.

"I'm not talking about blacking out locations but changing levels of detail," he noted. "Just because the knowledge is there, [it] doesn't mean the information is useful."

If passed, this bill would only affect California, but Anderson said he's confident that other states, as well as federal lawmakers, will introduce similar bills.

California bill spells out what companies have to say about data breaches

New legislation seeks to broaden scope of state's landmark breach-notification law

By Robert McMillan

March 9, 2009 (IDG News Service) A co-author of the landmark [data-breach notification law](#) that took effect in California six years ago is now looking to add new requirements spelling out what companies have to tell affected individuals about breaches.

The new bill, which was introduced by state Sen. Joe Simitian in December and is officially known as [S.B. 20](#), also would require companies to report any [data breaches](#) affecting more than 500 California residents to the state's attorney general.

Speaking at a symposium on breach notification issues that was held last Friday at the University of California's Berkeley campus, Simitian contended that S.B. 20 would give "greater clarity and specificity as to the content of security breach notices, which I think is long past due."

While some breach notification letters do a good job of telling users what happened to their data, a "substantial number" do not, Simitian said, adding that the lack of information leaves consumers "more confused than informed."

California's [S.B. 1386](#) breach-notification law was the nation's first. It requires that consumers be notified when unencrypted financial data is lost or stolen from systems and is credited with shining a light on the issue of data privacy and inspiring [similar legislation in 43 other states](#).

In fact, Simitian said that one of his goals in helping to write the 2003 bill was to help people outside of California. "This goal has been more fully realized than we could have ever anticipated at the time," he added.

But lawyers working on data breach cases estimate that perhaps only one in 10 breaches are ever made public, according to Fred Cate, a law professor at Indiana University. "We actually have very poor data on data breaches," he told the attendees at the symposium.

Part of the problem, according to Cate, is that while consumers must be notified of breaches, most states don't require that any notifications be made to a central authority.

That would change in California if S.B. 20 is signed into law. And by requiring the attorney general's office or another government agency to keep track of breaches, state residents and officials would get "a better understanding of the nature and scope of the problem," Simitian said.

Some states already require that breach notification letters be sent to a designated state agency, but Simitian's bill would centralize that information in the most populous state in the U.S., potentially creating the country's largest repository of breach data.

Simitian said he hopes to see California Gov. Arnold Schwarzenegger sign S.B. 20 by year's end. "That would make a good law, a groundbreaking law, even better," he said.

The California law was just expanded in January to cover breaches of medical and insurance data.

Virus Creators, ID Thieves, Spam Senders Hit Social Networks

Investor's Business Daily (03/05/09) P. A4 ; Deagon, Brian

Cybercriminals are increasingly targeting users of social networking sites in an effort to steal their personal data and the passwords to their accounts. One of the tactics cybercriminals use to gain access to this information involves sending social networking users emails that appear to come from their online "friends." For instance, some Facebook users have been receiving emails from their social networking friends that claim to contain a video of them but actually downloads a virus that goes through their hard drives and installs malicious programs. The virus, known as the Koobface virus, then sends itself to all of the friends on the victim's Facebook profile. A new version of the virus also is affecting users of MySpace and other social networking sites. In addition, cybercriminals are tricking social networking users into downloading malicious software to their machines by creating fake profiles of friends, celebrities, and business associates. Security experts say that such attacks, which became widespread last year, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites. Security experts warn that users need to be careful about what information they post because the data can be used to steal their identities or even claim money that the government owes them.

Fed agencies push new security audits

By [Ellen Messmer](#) , Network World , 02/23/2009

Dissatisfied with the current way Congress mandates their networks be [evaluated for security](#), some federal agencies, including the Department of Defense, are proposing a new approach unveiled Monday that would encourage investment in automated defensive measures.

The proposed Consensus Audit Guidelines (CAG) are 20 security controls that begin with the concept of automated inventory-taking of authorized and unauthorized hardware and software for the purpose of assessing network security. Strongly oriented toward specific technical measures that could be automated, CAG is an effort to gradually shift the federal agencies off the annual security compliance effort known as [Federal Information Security Management Act](#) (FISMA), which Congress made law in 2003.

"The federal government FISMA legislation that federal agencies comply with has only proven to be partially successful," says John Gilligan, head consultancy Gilligan Group.

A former Air Force CIO, Gilligan has become a strong [backer of CAG](#), kicked off last autumn among some in the federal agencies, including the CIO Council, with help from Alan Paller, director of SANS Institute.

Conforming with FISMA requires the inspector general of each agency to lead an evaluation of agency IT systems based on hundreds of pages of guidelines from the National Institute of Standards and Technology (NIST), tasked by Congress to come up with FISMA standards. These confidential FISMA reports are sent to Congress, which each year publicly hands down grades like a school report card to each agency.

As CIO of the Air Force, Gilligan says he found FISMA certainly focuses on security, though much of it was simply paperwork, and "it didn't help you narrow down, what should I do first?"

Gilligan said he got a handle on what to do first when the "NSA would annually do an assessment of DoD systems with their penetration analysis and call together the CIOs, and every time it was the same story: We broke in, it was easy."

He says he's convinced the government would benefit from a new approach requiring very technical steps, perhaps akin to the [secure-software configuration effort](#) of the Air Force five years ago.

CAG's list of 20 controls is published for a month's worth of public comment, and it features a broad list of both automated and non-automated practices that include continuous vulnerability testing remediation and secure configurations of hardware, software and network devices.

Security expert Ed Skoudis is the technical editor on the project.

The CAG recommendation is being funneled through the Center for Strategic and International Studies in Washington, D.C., as part of a cybersecurity report to the White House. The CAG concept Monday garnered backing from the National Security Agency, the Department of Homeland Security, various divisions with the Defense Department, the Department of Energy, the Department of Transportation, the Government Accountability office, MITRE Corp. and the SANS Institute.

Though agencies are [restive about FISMA](#), Gilligan says they are intent on bringing agency inspector generals — as well as NIST and Congress — on board to prove CAG will work. To that end, agencies are working to set up "pilot sites" in their production networks where they can demonstrate how CAG controls would work in practice. "We want real-world examination of this for feedback," Gilligan notes.

The CAG alliance wants feedback on how its guidelines mesh with other government and industry security-compliance efforts, such as the Health Insurance Portability and Accountability Act (HIPAA) guidelines from the Department of Health and Human Services or the Payment Card Industry data standards.

Physical security and cybersecurity go hand in hand

Los Alamos thefts show that you can't separate physical security from cybersecurity

By [William Jackson](#)

Feb 17, 2009

The National Nuclear Security Administration recently dressed down Los Alamos National Security LLC (LANS), the contractor responsible for security at the Los Alamos National Laboratory, for its apparent mishandling of computer thefts from the weapons lab.

NNSA noted that the lab "had made great strides in improving the robustness of cyber security implementation," in a Feb. 3 [memo](#) released by the Project on Government Oversight, a private watchdog organization. But cyber security is not a standalone effort. "For example, on January 16, 2009, three computers were stolen from a LANS employee's residence in Santa Fe," the memo noted. "This incident has revealed several property management, accountability, incident reporting and cyber security concerns."

The problem was that the theft was treated as a property management issue rather than a cyber security incident. And that was just the tip of the iceberg. "LANS has reported that 13 computers have been stolen or lost in the past 12 months, and that 67 computers are currently 'missing.' The magnitude of exposure and risk to the laboratory is at best unclear as little data on these losses has been collected or pursued given their treatment as property management issues as well."

In the early days of computing physical and cyber security were one and the same. Mainframe computers were locked in computer rooms and accessed by hardwired dumb terminals. But as computers became smaller, smarter and more ubiquitous, property and data were dealt with separately and there traditionally has been little reintegration of physical and cyber security. Today, data in any form can be the most valuable asset in any organization, government or private, and the proliferation of devices on which it resides means that physical security is becoming as critical to protecting it as cyber security.

True, breaches caused by hackers can generate huge losses and big headlines. The recent hacking of Heartland Payment Systems Inc. potentially exposed data from hundreds of millions of online transactions a month for an untold number of compromised persons. But don't ignore the physical risks. One of the largest government data breaches occurred with the 2006 theft of a Veterans Affairs laptop containing records of more than 26 million persons. That incident has cost the VA \$20 million in a settling a class action suit.

Of the 31 publicly disclosed data breaches [listed](#) by the Privacy Rights Clearinghouse for January, 10 involved stolen or missing laptops, PCs or storage devices. There also were incidents of theft or improper disposal or paper records, including documents found in a filing cabinet sold by the U.S. Consulate in Jerusalem. And a New Zealand man bought a used MP3 player in Oklahoma that contained, among other things, 60 files containing records on U.S. soldiers.

If an organization, be it government or private sector, wants to protect itself, it not only needs good cyber security and good physical security, it needs to integrate the two. Ideally, the systems implementing controls and doing the monitoring should communicate with each other. This could be a challenge because it often means integrating legacy systems that might not work and play well together. In the absence of integrated systems, the staff and management of the two shops need to communicate with each other. A physical breach or loss should be examined for possible information security consequences, and vice versa.

Los Alamos National Security had this reality thrust upon it by the NNSA, which directed the contractor to treat any loss of computer equipment with data storage capacity as a cyber security concern. Adopting this policy before a theft occurs could help an agency avoid another type of unwanted data leak; the kind in which embarrassing incidents show up in newspapers and on Web sites.

DOE seeks new approach to cybersecurity

By [William Jackson](#)

Feb 12, 2009

Reactive approaches to information security have not kept pace with the rapidly evolving information technology environment, and a panel of experts examining the state of security at the Energy Department has recommended a fundamentally different approach.

The traditional layered wall-and-moat approach to physical security is not well suited to complex information systems whose development and use are unpredictable, the panel concluded in its [report](#), “A Scientific Research and Development Approach to Cyber Security.”

“Today’s cybersecurity methods, policies and tools have proved to be increasingly inadequate when applied to the exponentially growing scope, scale and complexity of information systems and the Internet,” the report states. For instance, the availability of small, powerful USB drives easily circumvents many security measures. “Innovation is needed in many areas — ranging from better authentication protocols to stronger encryption to better understanding of social and human factors.”

The report recommends a program to apply scientific research to the problem, which could enable security to take a leap ahead of emerging threats and vulnerabilities instead of being condemned to a continual game of catch-up.

“Peer-review processes must be used to identify the best research ideas,” the report states. “Opportunities for dissemination of research results — through workshops, conferences, traditional publications or online journals — will be an important consideration in engaging the open science community. Involvement of postdoctoral researchers and students in this effort will help build the pipeline of trained cyber professionals.”

DOE undertook the study because of its heavy reliance on IT and its mission to protect the nation’s energy systems and nuclear stockpiles.

“Despite ubiquitous dependence on electronic information and on networked computing infrastructure, cybersecurity practice and policy [are] largely heuristic, reactive and increasingly cumbersome, struggling to keep pace with rapidly evolving threats,” the report states. “Advancing beyond this reactive posture will require transformation in information system architecture and new capabilities that do not merely solve today’s security challenges — they must render them obsolete.”

A community of cybersecurity professionals and researchers from DOE laboratories, the private sector, academia and other agencies conducted a series of workshops to assess the state of cybersecurity in general and at DOE specifically. “The conclusion reached is that the department should develop a long-term strategy that applies science and mathematics to develop information system architectures and protective measures that go beyond stopping traditional threats to rendering both traditional and new threats harmless,” the report states.

The department sees itself as uniquely qualified to play a leading role in the cybersecurity research and development area because of its reliance on IT infrastructure for a mission that includes classified and unclassified work and basic scientific research.

The panel identified the following three focus areas for research.

- Mathematics: Predictive Awareness for Secure Systems. The goal is to examine system and network behavior to anticipate failures or attacks, including real-time detection of anomalous activity.
- Information: Self-Protective Data and Software. DOE should create active data systems and protocols to enable self-protective and self-healing system.
- Platforms: Creating Trustworthy Systems from Untrusted Components. DOE should develop techniques for maintaining the integrity and confidentiality of a system comprising components for which there are varying degrees of trust.

Smartphone Threats Intensify

Dark Reading (02/17/09) ; Higgins, Kelly Jackson

Experts' warnings that iPhones, Windows Mobiles, and other smart phones were not secure enough to handle potential security threats are borne out by a McAfee study estimating that more than 50 percent of smart phone manufacturers said their products received malware, voice, or text spam attacks in 2008. These devices are conspicuous targets because they are frequently used for checking business email, browsing the Internet, and other applications. "[Users] want to do everything on them," says consultant Stewart Allen. "But they are [typically] completely bypassing the IT infrastructure." McAfee's survey of more than 30 mobile device manufacturers worldwide found that vendors are spending more money to recover from the rising number of attacks. More than half of the respondents to the survey said that data was stolen from as many as 1 million of their handsets in 2008.

RFID's Security Problem

Technology Review (02/09) Vol. 112, No. 1, P. 72 ; Naone, Erica

New U.S. passport cards and driver's licenses issued by Washington and New York state are designed to enable U.S. citizens to cross international borders more efficiently through the use of radio frequency identification (RFID) tags containing identity data that can be scanned by readers. But RFID technology has generated controversy because of its potential for privacy infringement, and studies of the new cards indicate that they can be exploited by ID thieves as well as by governments for the purpose of tracking people. Both the federal passport cards and the Washington driver's licenses boast electronic product code (EPC) tags that earned a passing grade from the U.S. Homeland Security Department, and which are inexpensive as well as capable of being read from an unusually long way off. Researchers from the University of Washington and RSA Laboratories see the latter capability as a means to facilitate invasive tracking, and also perceive a privacy issue in the tags' ability to store a unique number. The researchers also conclude that border security would be threatened by unauthorized reading, since the cards' ID numbers can be easily retrieved and therefore easily counterfeited. In addition, the Washington cards' EPC tags can be disabled by a "kill" command that is supposed to come from authorized users, and the state's failure to set the PIN on the cards it distributed means that anyone with RFID readers can set it themselves and issue kill orders. Some of the weaknesses in the federal passport cards and the Washington licenses are not apparent in New York's enhanced driver's licenses, which contain chips with serial numbers to guard against counterfeiting. Their memory banks are locked to shield them against unauthorized use of commands, but the New York licenses also raise the same privacy concerns the other cards do.

Social Elements of Security Policy and Messaging

End users tuning you out? Here's a three-step process for taking human factors into account in your security program (and even using them to your advantage).

By Christopher Burgess, Senior Security Advisor, Cisco

March 07, 2009 — [CSO](#) —

Let us begin with the premise that security policies exist to protect an entity's assets as it pursues the normal conduct of business. To ensure that those policies are effective, security professionals must first understand the social elements, including cultural and generational variances, that affect employee behavior and perceptions about security. With the implementation of a **three-step process of discussion, creation and messaging**, security policy can be successfully crafted—with consideration given to geographical, cultural and generational factors—while assuring resonance and understanding throughout the organization.

A recent Cisco white paper, [Data Leakage Worldwide: The Effectiveness of Security Policies](#), illustrates the apparent disparity between the perceptions of end users and IT professionals surrounding the existence, relevance, updating and communication of security policies. Just as businesses strive to understand their marketplace, they should also conduct internal market research to identify the key characteristics of their employee demographics.

To protect your employees, it is necessary to answer a number of rudimentary questions:

-
- What are the business's goals? -
- Who is responsible and accountable for the business's success? -
- Which individuals or business units are most affected by a certain policy? -
- Who and what functions are you trying to protect? -
- What social differences exist?
 - Cultural?
 - Geographic?
 - Generational?
 - Functional?

So let's look at some of these demographic challenges that an enterprise may face. In the geographic domain, a policy written for one audience may fail elsewhere if not fine-tuned for relevance. After all, cultural differences affect methods and styles of communication. For example, a message crafted for a highly technical audience in Asia may not have much success with a less technical group of employees in the U.S. who are used to a different communication style, and indeed one risks putting them to sleep or having them intellectually check out.

Generationally, how do we deal with individuals who are entering the workforce having collaborated and communicated openly using social media and other collaborative tools? Truly, this is an unprecedented challenge.

The key to success is in the early transfer of responsibility to those engaged in making the business successful. Take steps to assist those who believe that "there are no secrets" and help them comprehend why their personal livelihood depends on protecting the corporate intellectual property and infrastructure. Clearly communicate, that, in fact, there are secrets. Once employees understand that they have a responsibility to protect the enterprise, the chasm between the security professional and the

rest of the staff not only shrinks but disappears. Through this process, the enterprise will acknowledge security as forethought, not an afterthought.

Far too often, security policies arrive as a reactive action as opposed to a proactive management of risk. Unfortunately, many policies are created without any discussion or consideration of business needs. When challenged, an IT department expects automatic adherence. Managers frequently expect subordinates to comply with a policy even if they don't understand why adherence is expected; it is simply "because I said so" compliance.

To have security policies arrive as an overlay to an existing procedure is like placing a patch over a hole on a sweater. The patch may be effective, but if applied incorrectly, it can leave a noticeable flaw.

An upfront investment and a mandatory engagement by those crafting security policy need to occur at the point of strategic discussion within the business unit. This strategic interaction exponentially raises the odds of having a security policy that makes sense and factors in the data from demographic and functional research. A policy created in this way is a tool that each member of the business unit can use in a manner consistent with the agreed-upon security protocol.

This early alignment in the creation and implementation of policies is thus analogous to security being one of the integral threads woven into the fiber of the aforementioned patch, thus making it stronger and less likely to develop new holes. This way, policy isn't based on disconnected silos of knowledge, and your employees aren't being placed in the position of having to choose between business success and policy adherence.

So how do you go about engaging your employees and communicating your policies? Think globally, but act locally. You may have a global workforce message, but you must tailor that message for comprehension and relevance at a local level based on cultural, linguistic and other social factors.

Now let's discuss existing policies that were created in the overlay fashion. First, review these policies with the affected business units to assure they don't handicap or stifle business direction. Recommend that a review of adherence be completed prior to the discussion, as it may provide some measurable clues to a policy's effectiveness. Then recraft these policies to align with the reality of actual business objectives and goals.

Ultimately, the key is to ensure that your colleagues understand both the "why" of the policy and their share of ownership in the policy's existence. The empowerment of the ownership of any security policy by those most affected will increase adherence and address the risk that the policy is designed to mitigate. The exercise of the what of the policy follows with understanding, if not enthusiasm.

Ideally, security professionals will use this three-step process of discussion, creation and messaging. Each step reflects a consideration of geographical, cultural and generational diversity, but also positions the arrival of policy in a manner designed to assure resonance and understanding, as well as applicability.

Layoffs leave behind orphaned hardware, unused software licenses

The fate of sensitive corporate data is also a worry

By Lucas Mearian

March 11, 2009 (Computerworld) Pat Beemer, IT director for [Seattle Lighting](#), has a lot of orphaned computer hardware and unused software licenses on his hands -- the result of what he calls "serious" layoffs at the company.

"We're scratching our heads with what to do with them. Some of these PCs had sensitive data on them," he said. "Most of the PCs are old, so they can either be resold or destroyed, but how do we warehouse the others?"

Seattle Lighting is not alone. The question of what to do with unused IT equipment is a rapidly growing problem for many companies hit by the recession and the accompanying layoffs. Countless desktops, laptops, servers and handheld devices are lying around -- often with sensitive data on them -- gathering dust in cubicles, in stockrooms or on vacant desks. At the same time, software licenses, notoriously easy to lose track of, are also piling up.

From the beginning of the recession in December 2007 through February 2009, 4.4 million people had lost their jobs, [according to the U.S. Bureau of Labor Statistics](#). In the fourth quarter of 2008 alone [there were 3,140 mass layoffs](#) around the country resulting in 508,859 lost jobs. In January, another 2,227 mass layoffs occurred involving 237,902 workers.

"Let's say half of those [laid off] are knowledge workers," said Forrester Research Inc. analyst Peter O'Neill. "A knowledge worker usually has a copy of Microsoft Office, so you can make a direct correlation" between unused software and laid-off workers.

More than one in five businesses that have had software audits are holding on to unused software, also called shelfware, according to a soon-to-be released software budget survey from Forrester. And, only 35% of the 776 U.S., European and Asian companies that Forrester surveyed between December of 2008 and February 2009 had even been audited by a third-party provider, O'Neill said. That means the percentage of companies with shelfware is likely higher than the survey results indicate.

O'Neill added that on average, 15% of a company's IT budget is dedicated to software expenses, including new licenses, which can be expensed, and maintenance. Companies pay 10% of their software maintenance payments for shelfware. So, a company with an IT budget of \$1 million, would waste about \$15,000 on shelfware, O'Neill said.

"At the end of the day, I'd say almost every company... finds shelfware," said O'Neill, who works in Germany. "I've seen it in Europe even more dramatically."

Many companies have no comprehensive, well-documented end-of-life program for hardware and software -- a business oversight now coming to light as the recession deepens. "That isn't a standard business practice yet," O'Neill said. "It definitely should be."

Unused software isn't the only problem. Hardware recycling firms are often working overtime to keep up with incoming hardware, the majority of which comes through the door with hard drives -- and sensitive data -- intact.

"Trucks are booked. Account managers are running around like chickens with their heads cut off. Schedules are tight," said Angie Keating, vice president of compliance and security at [Reclamere Inc.](#) a Pennsylvania-based data forensics company that specializes in data recovery, data destruction, computer recycling and hardware disposal.

Keating said that while business is booming, she's concerned that eight out of 10 computers coming in still contain hard drives, even though they were supposed to have been removed. Many times, sensitive data is still on those drives because corporate budgets have been slashed, reducing or eliminating the trained employees needed to recycle computers properly.

"In some cases, those companies have gone bankrupt; the data is literally just sitting out there, probably sitting on eBay," said Keating, whose company serves the northeastern U.S., West Virginia and Ohio. "It is very frightening to me as a consumer, a mom, a health care patient. Everybody's data is out there."

In fact, [a New York computer forensics company recently reported](#) that 40% of the hard disk drives that it recently bought in bulk orders on eBay contained personal, private and sensitive information.

Besides sending hardware to a reputable recycling firm, Keating said companies that want to dispose of their hardware in-house must have three things in place to ensure that data is properly destroyed: a thoroughly documented process, a good quality-control program and solid follow-up documentation about what was done and who did it.

"If you have, let's say, 500 machines -- and that's a small number -- coming out of service and you've got them stacked up, how do you know which ones have been processed and which haven't if you don't have a quality control program?" she said.

Simson Garfinkel, an associate professor in the department of computer science at the Naval Postgraduate School in Monterey, Calif. agreed, emphasizing that an end-of-life program must include documentation. But it doesn't have to be expensive.

"A lot of people say that it's technically difficult or even impossible to overwrite the contents of a hard drive," Garfinkel said. "This is not true. There is freely available software which does a great job. But you need to run it, and then you need to track which drives you have erased and which you have not." One example of free software to handle the task of erasing drives is [Darik's Boot and Nuke, or DBAN](#).

Still easier, Garfinkel said, is "to just [punch a hole through each hard drive](#) and be done with it."

Laura DeBois, an analyst at research firm IDC in Framingham, Mass., said that besides physically shredding hard drives and mobile devices, companies can simply encrypt a drive and throw away the encryption key. They can also electronically "shred" the data by overwriting it using hard-drive-wiping software approved by the U.S. Department of Defense or the [National Institute of Standards and Technology](#).

Using a [degaussing machine](#) to eliminate a hard drive's magnetism, and thereby destroy its ability to store electronic data, is another method. But Keating said companies often use tape drive degaussers on hard drives, and that doesn't guarantee erasure.

"It doesn't have near the power necessary to get to the inner workings of a computer hard drive. And, with no quality control program, how do you know? A degaussed hard drive looks exactly like one that hasn't been degaussed," Keating said.

The other option is to simply keep the hardware and warehouse it until better economic times roll around, DeBois said.

"Overall, IT is facing strains and pressures. I think one thing that could happen as budgets compress is that extending maintenance contracts for the more expensive systems will become more popular. An administrator of a large disk storage system with a [three-to-five-year] refresh cycle might err more toward the five-year than three-year end."

Seattle Lighting, which has stores in nine locations in the Northwest, has just begun to look at how it will implement an end-of-life policy for hardware, according to Beemer. Most of the company's sensitive data resides on centralized servers, and for hardware without a home, "most likely we'll run an eraser tool on hard drives," he said.

A bigger problem for Beemer are the hundreds of software licenses orphaned by the layoffs. "We're aggressively asking our vendors for renegotiations," he said. "In some cases they do, but others won't. That goes across the board for the enterprise in general, including lease negotiations."

Garfinkel said companies in that situation should simply begin migrating to open-source software, "rendering this issue moot."

According to Forrester's O'Neill, vendors that would never have considered renegotiating a software contract two years ago have softened and are likely to rework deals to keep their customers.

"This year especially [software vendors] are highly dependent on maintenance... and that's dependent on the relationship with customers," he said. "Even Microsoft these days probably doesn't feel that safe. The threats building up for Microsoft Office around the cloud and service offerings are very apparent. While the last 12 months of thousands of layoffs... translates into additional shelfware being created. I'm not sure companies have even reacted to it yet."

People Search Engines: They Know Your Dark Secrets

By JR Raphael

March 11, 2009 (PC World) [Editor's note: While researching this story, JR Raphael discovered the Coldplay radio station I created on [Pandora](#) on August 13, 2006; found that I had looked into purchasing a 4-foot iPod-compatible 3.5mm audio cable in October of 2007; and sleuthed out what my [StumbleUpon](#) user name is. Though only my musical taste was mildly incriminating, it was freaky to see what details popped up. (Do I want my hipster friends to know that I like Chris Martin and his melodic cohorts?) Read on to find out how deep these searches can go.]

I know things about my lawyer I absolutely should not know. He's 55 years old, listens to the music of [the band Creed](#), and screams like a little girl when riding roller coasters. He also relaxes with New Age spa treatments and is thinking about getting an electronic nose hair trimmer. And that's just the start.

Now, let me be clear: I've never spent a single moment outside the office with this guy (and for what it's worth, I'd just as soon not be privy to his personal grooming habits). I learned all of these details by tracking his social footprint across the Web--and he probably has no idea that he has left such a vivid trail behind.

In our age of social sharing, we expect some of our thoughts to be public. But as we slowly put more and more pieces of ourselves online, specialized search engines are making it easier than ever to pull them together into a highly detailed (and potentially invasive) profile of our virtual lives.

I'll let you in on a little secret: The picture isn't always pretty. And even no rap sheet turns up, do you really want the world to know that you look at bad breath cures online or post awful Star Trek fan fiction?

The Depths of the Deep Web

You hear a lot of terms bounced around when you talk about this growing breed of search engines. Some services like to be called "social search" utilities, while others prefer the phrase "people search." Many boast of their ability to delve through the "[Deep Web](#)" that even Google doesn't touch.

"Even though most people think the size of the Web is basically the Google crawl index, there's actually a lot of information that Google doesn't crawl," says Harrison Tang, founder and CEO of [Spokeo](#)--which, taking a mash-up approach to its identification, describes itself as a "social people search engine" service.

Spokeo, like its competitors [Pipl](#) and [CVGadget](#), is designed to let you dig up information on friends, foes, and anyone in between. Spokeo goes a step farther than many of the other services, though, by importing your entire e-mail address book.

Then, for a few bucks a month, it continually monitors your contacts and lets you know whenever anyone has done anything new, anywhere online. (The site's home page promises to help you "uncover personal photos, videos, and secrets," including "juicy" and "mouth-watering news about friends and coworkers.") [Editor's note: Pipl reports that my former boss donated \$500 during the 2004 presidential election--candidate not named.]

Each individual bit of information may seem insignificant, but the cumulative effect of seeing it assembled in a neatly packaged portfolio is enough to give almost anyone pause. [Editor's note: According to CVGadget's quick search, my college roommate researched the game of bocce ball recently for a children's book she's writing. And a former boyfriend I haven't spoken to since the 1980s appears to be an actor in Santa Barbara. Who knew?]

"Aggregated identity is actually a new type of identity," Tang says, theorizing about why so many people seem to use the word "spooky" when describing his service. "A lot of people know that they have a public MySpace page, a lot of people know that they have a public Twitter album. But, when combined together, it's not one plus one equals two--you actually create a new identity."

How Spokeo Works

Spokeo's system uses your contacts' e-mail addresses to track their activity on a few dozen services, ranging from basic blogs and social networks to a slew of photo- and video-sharing sites. That means the random photos

of your kids you shared on Flickr two years ago (or perhaps those less innocent images from your spring break trip a decade earlier) will pop up right under your name, seconds after someone searches for you.

Less obvious sources such as Amazon Wish Lists, Pandora playlists, and movie rating sites fill in the colorful details that you may not have realized were out there at all--things like (in my lawyer's case) an affinity for New Age jams and nasal maintenance.

I found Mr. Attorney's age on an old MySpace profile and his roller coaster behavior on a personal YouTube video, but Pandora divulged his cravings for Creed and his suggested usages for the "Spa Radio" station he had created. As for the nose hair trimmer, he can thank his Amazon Wish List for sending that factoid my way.

For Sale: Your Information

Other services access the same data and then sell the information under the banner of marketing research. One highly visible example is [Rapleaf](#), a company that describes its services as "data and people lookup." Clients pay thousands of dollars to have [detailed social profiles](#) compiled of individuals in their own customer databases. As is the case with the data that Spokeo assembles, the information is all publicly available--Rapleaf just brings it together. "Things that people have posted are out there for anyone to come and see," says Joel Jewitt, Rapleaf's vice president of business development. "As long as you're not going beyond that, that's within the privacy norms today."

Most of Rapleaf's clients, Jewitt says, are simply trying to understand how to use social media more effectively for marketing. An auto manufacturer, for example, might want to know which car models its customers are checking out and discussing on social Internet services. Armed with the company's list of customer e-mail addresses, Rapleaf would crawl the Web and track down the information, person by person.

"It's pretty standard Web spidering," Jewitt says. "We re-create in an automatic way what someone from the general public would be able to do if they were looking."

Electronic Exposure

Whether they target businesses or individuals, the services have one thing in common: Unlike the [public record-driven search tools of the past](#), the new people-tracking utilities build a highly detailed dossier about you solely from information that you yourself published--a circumstance that may give you a distinct feeling of discomfort.

"What it does is make the ubiquity of the Internet and the sheer openness of the world tangible," says Internet privacy expert Kevin B. McDonald, executive vice president of Alvaka Networks, a network management firm. "It makes the whole concept of the world sharing of information and the 'no-walls' approach that the Internet was designed for very real to people."

The reality can be chilling if the information is going to certain interested individuals: a curious client, a boss big on background checks, or an obsessive ex, say. A recent study reported that half of all British Internet users surveyed admitted to having used the Internet to [look up information on a former flame](#). The ease with which someone can arrange to monitor your every electronic move certainly adds a new dimension to the idea of fixation.

"It is a little 'stalkery,'" says Marc Rotenberg, executive director of the Electronic Privacy Information Center. "If the information is distributed, that's actually a form of privacy. When it's gathered up in one place, it creates some new risks."

Rotenberg is no fan of companies that assemble nuggets of personal but public information to turn a profit. "The fact that someone's made something public doesn't mean that someone else can sell it," he contends. "I would say even with affirmative consent, if there's going to be a market for personal data, the user should get some percentage of whatever value the data has."

Taking Control

The thing to remember, of course, is that these services aren't doing anything illegal. The information they gather is information that anyone who knew where to look--and had the time to do it--could find. So rather than ignoring

the king-size file that may have been collected on you, McDonald suggests, you should try to use it as a tool to understand and control your online identity.

"I've come to the point where rather than be driven by the Internet, I intend to drive it to the degree that I can," he says.

"All you can do is learn to live with it," McDonald says. "That's the confines of the world that we live in."

Google Voice: Press "1" to invade your privacy

Lost in all the hooplah about [the release of Google Voice](#) is this disturbing fact: The service will give Google enormous amounts of information about the intimate details of your everyday life, including recordings of your voice mail and possibly your phone calls. Combined with what Google already knows about you, it could mean your privacy is at an end.

Google Voice, by all accounts, may be the best tool ever for managing your telephone communications. It routes all of your calls through a single number, and can then ring all of your phones simultaneously. You can manage your voice mail with it, including getting free transcripts of your calls. It includes free voice conferencing, inexpensive overseas calls, and plenty more. You'll also be able to record and store your calls online.

But all that information about your calls will be routed through Google. Google will know everyone who called you and when they called. They'll have records of your voice mail, and because they offer free transcription, it means they'll have not just the voice, but text of your calls as well. They'll have recordings of your phone calls --- and I would expect them to offer transcriptions of them as well, which means they'll have the transcriptions as well as your calls.

Google Voice will be offered for free. Google, though, will certainly be looking for ways to make money from it. One of the most obvious ways is via targeted advertising, particularly because the company recently announced that it's going to figure out new ways to target ads based on your interests. It already does this with Gmail. So don't be surprised to see ad targeted based on who calls you.

Doing that means that Google will be mining data from your calls, possibly including what is being said on the calls themselves. It already does the equivalent of this in Gmail, looking for key words, and then displaying ads based on those words.

Privacy advocates are already worried. Marc Rotenberg, executive director of the Electronic Privacy Information Center, when interviewed by the New York Times, [has this warning about the service](#): "In the privacy world, it is increased profiling and tracking of users without safeguards."

Google already has a profile about your interests and surfing habits. If you use Gmail, it examines the content of your mail as a way to target ads. With Google Voice, it will know who you're talking to, and when you're talking to them --- and will have records of your voice mail, and possibly recordings of your actual calls themselves.

Given that, will there anything about your personal life that Google won't know?

Researchers sniff PC keyboard strokes from thin air

By Robert McMillan

March 12, 2009 (IDG News Service) That PC keyboard you're using may be giving away your passwords. Researchers say they've discovered new ways to read what you're typing by aiming special wireless or laser equipment at the keyboard or by simply plugging into a nearby electrical socket.

Two separate research teams, from the [Ecole Polytechnique Federale de Lausanne](#) and security consultancy [Inverse Path](#), have taken a close look at the electromagnetic radiation that is generated every time a computer keyboard is tapped. It turns out that this keystroke radiation is actually pretty easy to capture and decode -- if you're a computer hacker-type, that is.

The Ecole Polytechnique team did its work over the air. Using an oscilloscope and an inexpensive wireless antenna, the team was able to pick up keystrokes from virtually any keyboard, including laptops. "We discovered four different ways to recover the keystroke of a keyboard," said Matin Vuagnoux, a Ph.D. student at the university. With the keyboard's cabling and nearby power wires acting as antennas for these electromagnetic signals, the researchers were able to read keystrokes with 95% accuracy over a distance of up to 20 meters (22 yards), in ideal conditions.

Laptops were the hardest to read, because the cable between the keyboard and the PC is so short, making for a tiny antenna. The researchers found a way to sniff USB keyboards, but older PS/2 keyboards, which have ground wires that connect right into the electric grid, were the best.

Even [encrypted wireless keyboards are not safe](#) from this attack. That's because they use a special algorithm to check which key is pressed, and when that algorithm is run, the [keyboard gives off a distinctive electromagnetic signal](#), which can be picked up via wireless.

Vuagnoux and co-researcher Sylvain Pasini were able to pick up the signals using an antenna, an oscilloscope, an analog-digital converter and a PC, running some custom code they've created. Total cost: about \$5,000.

Spies have long known about the risk of data leaking via electromagnetic radiation for about 50 years now. After the U.S. National Security Agency found strange surveillance equipment in a U.S. Department of State communications room in 1962, the agency began looking into ways that radiation from communications equipment could be tapped. Some of this research, known as [Tempest](#), has now been declassified, but public work in this area didn't kick off until the mid-1980s.

The idea of someone sniffing out keystrokes with a wireless antenna may seem ripped from the pages of a spy thriller, but criminals have already used sneaky techniques such as wireless video cameras placed near automated teller machines and Wi-Fi sniffers to steal credit-card numbers and passwords.

"If you are a company using highly confidential data, you have to know that the keyboard is a problem," Vuagnoux said.

If pulling keystrokes out of thin air isn't bad enough, another team has found a way to get the same kind of information out of a power socket. Using similar techniques, Inverse Path researchers Andrea Barisani and Daniele Bianco said they get accurate results, picking out keyboard signals from keyboard ground cables.

Their work only applies to older, PS/2 keyboards, but the data they get is "pretty good," they said. On these keyboards, "the data cable is so close to the ground cable, the emanations from the data cable leak onto the ground cable, which acts as an antenna," Barisani said.

That ground wire passes through the PC and into the building's power wires, where the researchers can pick up the signals using a computer, an oscilloscope and about \$500 worth of other equipment. They believe they could pick up signals from a distance of up to 50 meters by simply plugging a keystroke-sniffing device into the power grid somewhere close to the PC they want to snoop on.

Because PS/2 keyboards emanate radiation at a standard, very specific frequency, the researchers can pick up a keyboard's signal even on a crowded power grid. They tried out their experiment at a local university's physics department, and even with particle detectors, oscilloscopes and other computers on the network were still able to get good data.

Barisani and Bianco will present their findings at the [CanSecWest](#) hacking conference next week in Vancouver. They will also show how they've been able to read keystrokes by pointing a laser microphone at reflective surfaces on a laptop, such as the screen. Using the laser's very precise measurements of the vibrations on the screen's surface caused by typing, they can figure out what is being typed.

Previously, researchers had shown how the sound of keystrokes could be analyzed to figure out what is being typed, but using the laser microphone to pick up mechanical vibrations rather than sound makes this technique much more effective, Barisani said. "We extend the range because with the laser microphone, you can be hundreds of meters away," he added.

The Ecole Polytechnique team has submitted its research for peer review and hopes to publish it very soon.

Effects of corporate social media on network security

By Howard Price

March 12, 2009 (*Network World*) In today's increasingly communicative world, businesses face a dilemma. They have to find ways to be more engaging and communicate more directly to their customers and the public, while retaining close control of sensitive information.

The most convenient way for both business users and their customers to share information has been through blogs. Over the last three years blogs have sprung up everywhere. It's hard to find a major corporation that doesn't have a host of blogs on different subjects all aimed at getting more relevant content out to the marketplace faster and more effectively.

The popularity of blogs has been closely followed by a wave of Web-based social networks, such as LinkedIn, Facebook and Twitter. According to Nielsen Online's article "Social Networking's New Global Footprint," time spent in "member communities" now accounts for one of every eleven minutes online.

But the distinction that used to exist between blog posting and updating your status on LinkedIn is fading. Each status update to your Twitter account becomes the latest entry in a rolling blog of your life. This interconnection is important because it is this aspect of social networks that can be cause for concern to IT departments.

If, for instance, you have linked your LinkedIn account to your Facebook account to Twitter and beyond, anything you post to any one of the services will immediately be federated or syndicated to the others. This replication and distribution of data makes it difficult if not impossible to take things back.

For the most part, the interconnected aspect of social networking is a benefit (who wants to update 10 networks with their latest status?), but it's a double-edged sword in the hands of the careless. As status updates and notes get quickly exchanged from a network intended for personal use to your business social network, it's easy to see how the mixing of the groups could cause problems. "Friends" that we once had at company X might now be the competition at company Y. When the relationships you have in your online communities get tangled you need to exercise caution in what you share or the consequences might hurt your company and/or your career.

The knee-jerk reaction to these kinds of problems from most IT departments is to implement URL filtering and block access to sites such as LinkedIn and Twitter. While this feels like it's solving the immediate problem, it is not. The thing that needs protecting is your data, not your Web access. Data protection has many forms, but all good data protection starts with solid and repetitive user education. The computer security industry is responding to this need by delivering tools for IT to help learn about important and sensitive data. By learning where data is stored, how it is handled and who has access, IT can build more effective policies to protect it more quickly.

Solutions that help support business rather than cripple it with overwhelming false positives are essential to success. Being able to look at historic data patterns will give IT the ability to prevent future data leaks. Once the patterns of use are identified it becomes easy to implement effective user education programs to start to change behavior and perceptions. That education coupled with systems that constantly monitor data as it moves around your network and provide immediate feedback to users and efficient tools to handle incidents quickly make the recipe for success.

The most effective way to prevent casual data mishandling is to raise awareness of safe data handling practices with your users rather than locking down your business by cutting off its essential access to the world which its customers live in.

